VIR-AC5000xx

Lecteur biométrique de Virdi

Manuel d'utilisation VIR-AC5000xx

Table des matières

1 HISTORIQUE DES REVISIONS

Version	Date	Description	Version Firmware
1.00	2011-01-10	Première version	10.51.00-000.00

2 LISTE DE MOTS

- Admin (Administrator)
  - Si un utilisateur a accès au menu du terminal (appareil), il possède les droits pour enregistrer/adapter/supprimer les utilisateurs et changer l'environnement de travail en adaptant les paramètres.
  - Si aucun administrateur n'est enregistré sur le terminal, alors n'importe qui peut entrer dans le menu et modifier les paramètres. Par conséquent, il est recommandé d'enregistrer au moins un administrateur.
  - Prenez garde lors de l'enregistrement et de l'exploitation car un administrateur a le droit de modifier les paramètres d'environnement essentiels du lecteur biométrique.

- Authentification 1:1 (Vérification 1 à 1,)
  - Il s'agit d'une méthode qui authentifie les empreintes digitales via l'ID utilisateur ou la carte
  - Cette méthode est appelée vérification 1:1 parce que seule l'empreinte digitale enregistrée est utilisée pour la comparaison avec un ID utilisateur ou la carte.

- Authentification 1:N (1 à N, Identification)
  - Il s'agit d'une méthode de recherche d'un utilisateur uniquement sur base de l'empreinte digitale.
  - Cette méthode est appelée vérification 1:N car on recherche une empreinte identique aux empreintes digitales enregistrées sans ID utilisateur ni carte.

- Niveau de protection
  - C'est le niveau utilisé pour la vérification d'empreintes digitales. Le niveau de 1 à 9 indique le degré de similitude entre deux empreintes digitales. L'authentification sera réussie uniquement si la similitude entre les deux empreintes digitales est plus élevée que le niveau prédéfini.
  - Plus le niveau de vérification est élevé, plus la sécurité est importante. Néanmoins, comme la similitude doit être relativement élevée, il se peut que l'auto authentification échoue.
  - Niveau 1:1 : Niveau d'authentification utilisé pour vérification 1:1.
  - Niveau 1:N : Niveau d'authentification utilisé pour identification 1:N.

- Méthode d'authentification
  - Cela représente différents types de méthodes d'authentification y compris l'authentification EP (empreintes digitales), l'authentification RF (carte) ou une combinaison de ces méthodes.
  - Ex : Carte ou EP: Authentification avec Carte ou empreinte digitale.

- Touches de fonction
  - Touches [F1], [F2], [F3], [F4], et [ENT] sont disponibles. Ces touches permettent à l'utilisateur d'entrer dans le menu et de changer de modes tels qu'arriver/quitter bureau.

- LFD (Live Finger Detection)
  - Cette fonction permet d'enregistrer uniquement de véritables empreintes digitales et bloque l'introduction de fausses empreintes digitales (imitation) faites de caoutchouc, de papier, de films et de silicone.

3 AVANT L'UTILISATION

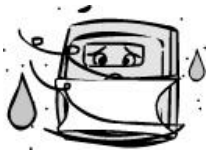
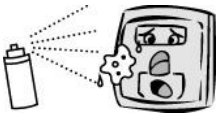
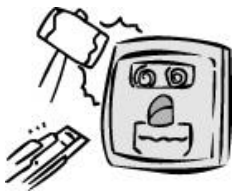
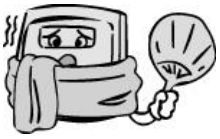
3.1 PRECAUTIONS DE SECURITE

- Avertissement

Ne manipulez pas l'appareil avec des mains humides et ne laissez pénétrer aucun liquide -> Cela peut provoquer un choc électrique ou des dommages. 	Ne placez pas de source de feu à proximité de l'appareil. -> Cela peut provoquer un incendie. 
Ne démontez pas, ne réparez pas, ne modifiez pas l'appareil. -> Cela peut conduire à un choc électrique, un incendie ou des dommages. 	Tenez l'appareil hors de portée des enfants. -> Cela peut entraîner des dommages ou d'un accident. 

- Si les avertissements ci-dessus sont ignorés, cela peut entraîner des blessures graves ou la mort.

- Attention

Gardez l'appareil hors de la lumière directe du soleil -> Cela peut conduire à un mauvais fonctionnement, déformation ou changement de couleur de l'appareil. 	Evitez la poussière ou un taux d'humidité élevé ->Cela peut provoquer une défectuosité de l'appareil. 
Evitez d'employer de l'eau, du benzène, du diluant ou de l'alcool pour nettoyer l'appareil. -> Cela peut entraîner un choc électrique ou un incendie. 	Ne placez pas d'aimant à proximité de l'appareil. -> L'appareil peut arrêter de fonctionner ou mal fonctionner. 
Evitez que la zone empreinte digitale soit encrassée. ->Cela peut mener à une non-reconnaissance de l'empreinte digitale. 	Evitez d'utiliser un insecticide ou un spray inflammable vers l'appareil. -> Il peut en résulter une déformation ou un changement de couleur de l'appareil. 
Evitez les chocs ou l'utilisation d'objets pointus sur l'appareil. -> L'appareil peut être endommagé ou cassé. 	Evitez l'installation de l'appareil dans des pièces à fortes variations de température. ->Cela peut mener à un mauvais fonctionnement de l'appareil. 

- Si les avertissements ci-dessus sont ignorés, cela peut conduire à la perte de propriété ou des blessures humaines.

※ En aucune circonstance, nous ne pouvons être tenus responsables en cas d'accident ou de dommages provoqués par une utilisation non autorisée du produit ou si les précautions mentionnées dans ce manuel ont été ignorées.

3.2 DESCRIPTION DE L'APPAREIL

LED d'état

Ecran LCD

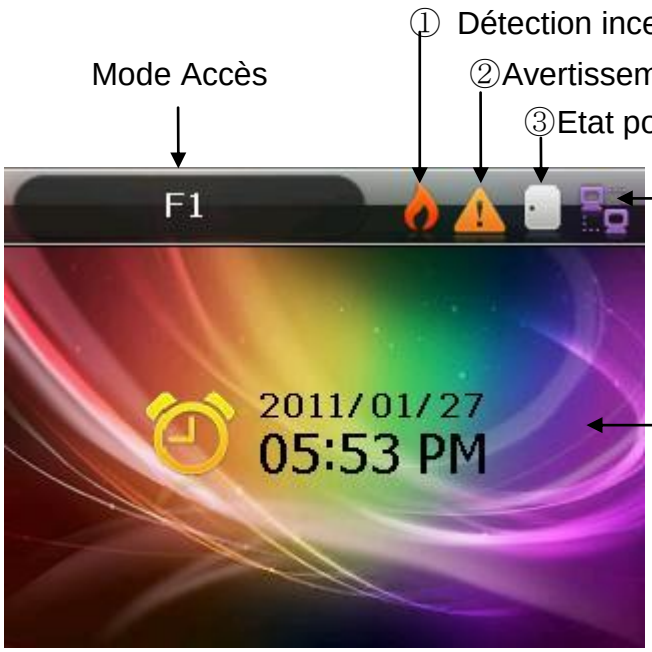
Senseur d'empreintes digitales

Touches tactiles

Normalement, les chiffres sont invisibles si la LED est éteinte. Quand la LED est allumée, les chiffres apparaissent lorsque l'utilisateur touche légèrement cette zone.

Zone de lecture de cartes

3.3 DESCRIPTION DE L'ECRAN (PENDANT LE FONCTIONNEMENT)



① Détection incendie

Mode Accès

②Avertissement sabotage, etc.

③Etat porte

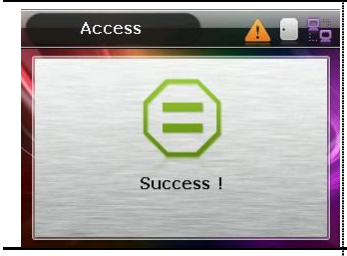
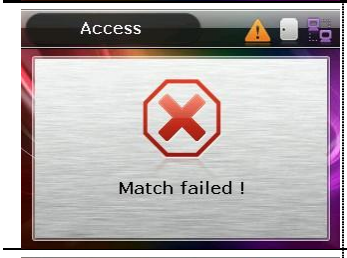
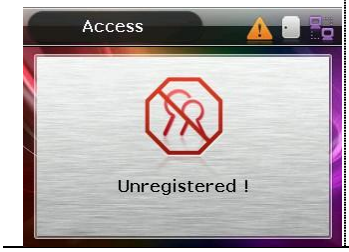
④Connexion avec Serveur

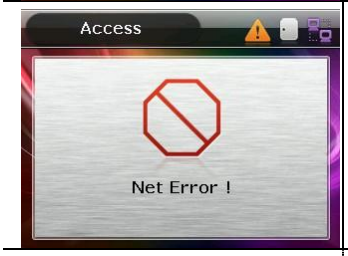
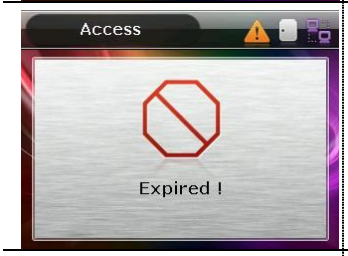
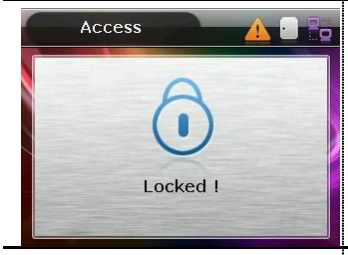
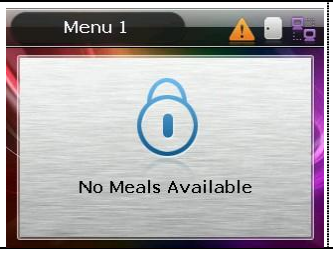
Heure actuelle

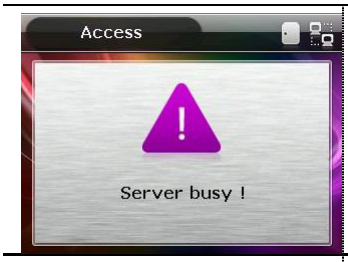
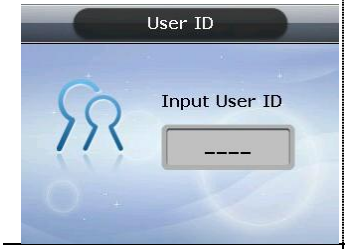
3.3.1 ICONES AFFICHES PENDANT LE FONCTIONNEMENT

① Détection incendie	Aucun	: Normal
		: Un incendie a été détecté par le senseur d'incendie (Si un détecteur incendie est connecté)
② Avertissement	Aucun	: Normal
		: Etat anormal, il y a un sabotage sur le terminal ou la porte a rencontré un problème.
③ Etat Porte		: L'état de la porte est inconnu
		: La porte est fermée
		: La porte est ouverte
④ Connexion au Serveur	Aucun	: Le câble LAN n'est pas raccordé
		: Le câble LAN est connecté, mais pas encore au serveur
		: Connecté avec le programme serveur

3.3.2 MESSAGES AFFICHES DURANT LE FONCTIONNEMENT

	- Ecran initial de l'AC5000
	- Lorsque la vérification est réussie
	- Lorsque la vérification a échoué
	- Quand un utilisateur non enregistré se présente - Lors d'une tentative de vérification d'empreintes digitales dans le cas où le serveur n'est pas connecté et qu'aucune empreinte digitale enregistrée n'est présente dans le terminal.

	- Lorsqu'une carte non enregistrée est présentée.
	- Lorsque l'analyse de l'empreinte digitale échoue. - Lorsque l'utilisateur retire trop rapidement le doigt après le scan.
	- Lorsque l'Anti-pass back donne un défaut (dans le cas où l'utilisateur utilise la fonction Anti-pass back)
	- Si l'utilisateur fait deux tentatives ou plus au cours de la même zone horaire repas (si utilisé pour une cafétéria)
	- Si aucune réponse ne vient du serveur lors d'une tentative de vérification vers celui-ci. - Si le réseau est interrompu lors d'une tentative d'authentification vers le serveur.
	- Si l'utilisateur n'est pas autorisé pour l'authentification, même s'il est enregistré ou quand l'utilisateur tente une authentification à un moment où l'accès n'est pas autorisé.
	- Quand l'appareil est défini comme Verrouillé.
	- Quand il n'y a pas d'horaire de repas (dans le cas où il est défini sur Cafétéria).

	- Si l'authentification ne peut pas être traitée parce qu'il y a trop de requêtes d'authentification du terminal durant l'authentification serveur.
	- Pendant l'état d'attente pour l'introduction d'un ID utilisateur.
	- Pendant l'état d'attente pour l'introduction du mot de passe de l'utilisateur.
	- Pendant l'état d'attente pour l'introduction de l'empreinte digitale de l'utilisateur.
	- Pendant l'état d'attente pour la présentation de la carte de l'utilisateur.
	- Au moment de l'authentification par carte, indique que la carte lit les données d'empreintes digitales. L'utilisateur doit présenter sa carte pendant 1 ~ 2 secondes jusqu'à ce que le message disparaisse.
	- En attendant une réponse du serveur après une tentative d'authentification de l'utilisateur vers le serveur.
	- Lors de la mise à niveau du programme du terminal (Assurez-vous que la tension NE soit PAS enlevée pendant l'affichage de ce message).

3.4 INDICATIONS LED PENDANT LE FONCTIONNEMENT

●	Alimentation	Rouge	Allumée: Normal Clignote: Si le couvercle est ouvert ou s'il y a un problème de communication lors de la connexion avec le LC010.
●	Porte	Verte	Allumée : Porte ouverte Eteinte: Porte fermée

3.5 TOUCHES UTILISEES PENDANT LE FONCTIONNEMENT.

[0]~[9]	- Touches utilisées pour introduction numérique
[F1]~[F3]	- Touches utilisées pour changer le mode d'authentification
[F4] ou [←]	- Utilisée pour modifier le mode d'authentification - Utilisée comme touche SUPPR pour corriger une mauvaise introduction de chiffres - Utilisée pour effacer les données saisies et retourner au menu parent du mode menu
[F4(←)~]	- Signifie presser la touche [F4(←)] pendant 2 secondes ou plus. - Si le point d'entrée est situé dans la zone de saisie, vous pouvez annuler l'entrée et retourner au menu principal en appuyant sur ce bouton pendant 2 secondes ou plus.
ENT [ou MENU]	- Utilisée pour modifier le mode - Est utilisée pour stocker une valeur dans le mode menu ou aller à la configuration dans l'écran.
[ENT~]	- Signifie presser la touche [ENT] pendant 2 secondes ou plus. - Utilisée pour accéder au menu si pressée dans l'écran de base. - Si le point d'entrée est situé dans la zone de saisie, alors l'utilisateur peut retourner au menu parent tout en sauvegardant la valeur actuelle en pressant sur ce bouton pendant 2 secondes ou plus. - Utilisée pour actualiser la configuration de l'écran actuel en mode menu et ensuite revenir au menu parent.

3.6 MESSAGES VOCAUX UTILISES PENDANT LE FONCTIONNEMENT

Type d'opérations	Message vocal
Lors de l'introduction d'une empreinte digitale	Please enter your Fingerprint
En cas de vérification réussie	You are authorized.
Si échec de la vérification	Please try again.

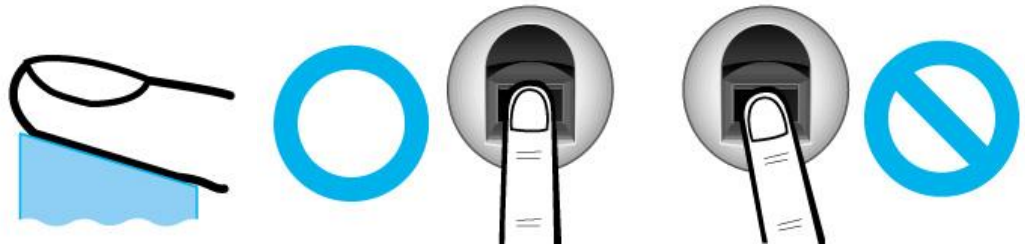
3.7 TONALITES AUDIBLES PENDANT LE FONCTIONNEMENT

Beep	Tonalité générée quand une touche est pressée ou quand une carte est manipulée.	Quand une touche est enfoncée ou une carte est lue. Lorsque la lecture du doigt est terminée et que l'utilisateur est autorisé à ôter son doigt.
Be peep	Tonalité d'échec de lecture	Quand l'authentification échoue ou quand l'empreinte digitale a été mal introduite.
Brrrrrrp	Attente d'introduction	En cas d'affichage de l'état d'attente de la saisie d'une empreinte digitale d'utilisateur ou d'un mot de passe.
Beeeep	Succès	En cas d'une authentification réussie ou quand la configuration est terminée.

3.8 COMMENT ENREGISTRER ET INTRODUIRE UNE EMPREINTE DIGITALE ?

- Comment introduire une empreinte digitale?

  Introduisez votre empreinte digitale comme si vous scelliez un document avec votre index.
  Evitez la saisie/l'enregistrement d'une empreinte digitale en ne touchant que légèrement du bout du doigt la zone de scan.
  Assurez-vous que le centre de l'empreinte digitale touche correctement la zone de saisie.



- Saisissez si possible l'empreinte digitale de votre index.

  Cela facilitera la saisie exacte et stable de l'empreinte digitale.

- Vérifiez que l'empreinte digitale soit nette et ne porte aucune cicatrice.
  Une empreinte digitale trop sèche ou trop humide, ambiguë, avec une cicatrice, etc… peut ne pas être reconnue. Utilisez/Enregistrez dans ce cas l'empreinte d'un autre doigt.

- Précautions liées à l'état de l'empreinte digitale des utilisateurs

Si l'état de l'empreinte digitale n'est pas satisfaisant, il est préférable qu'elle ne soit pas utilisée par l'utilisateur autrement des problèmes pourront survenir.

- Ce produit est un système de reconnaissance d'empreintes digitales. Les empreintes digitales endommagées ou imprécises ne peuvent être utilisées. Dans ce cas, l'utilisateur doit utiliser un mot de passe.

- Si le doigt est trop sec, il est recommandé à l'utilisateur de respirer sur le bout doigt pour permettre une authentification correcte.

- Dans le cas d'un enfant, de par la petite taille ou des propriétés tendres du doigt, il peut être difficile ou même impossible de l'utiliser. Il est donc nécessaire de relever les empreintes digitales tous les 6 mois.

- Dans le cas de personnes âgées, les abondantes petites stries présentes sur les empreintes digitales peuvent empêcher un enregistrement approprié.

- Il est recommandé de saisir au moins 2 empreintes digitales par utilisateur, si possible.

4 INTRODUCTION PRODUIT

4.1 CARACTERISTIQUES

- **Application pour POE et bloc terminal – Simple à installer**

- POE étant pris en charge, il peut être facilement installé sans câble d'alimentation séparé.

- **Conçu avec spécification d'étanchéité IP65** – Installation extérieure possible.

- **Design mince et élégant**

- Facile à installer du fait même de sa conception. **Design mince et élégant qui utilise** un LCD de couleur et un clavier tactile.

- **Télécharger fonction du Server – Offre la possibilité de modifier l'image de fond et les messages vocaux**
  - Offre une variété de messages informatifs via le LCD couleur et les messages vocaux. L'utilisateur peut télécharger des images d'arrière-plan et des messages vocaux du serveur selon ses préférences. Le rétro-éclairage LCD intégré et le clavier tactile assurent une lecture aisée de l'écran et une excellente visibilité des touches même dans un endroit sombre.

- **Fonction de détection automatique facile**
  - Permet d'effectuer facilement l'opération de vérification par la saisie de l'empreinte digitale sans devoir présenter un badge.

- **Auto vérification aisée via empreintes digitales**
  - Évite le risque de mots de passe oubliés, de cartes/badges perdus ou volés grâce à la technologie de reconnaissance d'empreintes digitales biométrique. Cette technologie renforce la sécurité de l'authentification par l'utilisation de propres empreintes digitales.

- **Système de Gestion d'Accès via le réseau (LAN)**
  - La communication entre le lecteur biométrique et le serveur d'authentification utilise le protocole TCP/IP ; Ceci permet de placer facilement des extensions sur le réseau. L'appareil détecte automatiquement 10/100 Mbps, ce qui assure un fonctionnement à haute vitesse permettant ainsi une gestion aisée via le réseau.

- **Offre une gestion d'accès diversifiée et flexible**
  - Offre une fonction de contrôle parfait en attribuant des droits d'accès par groupe d'utilisateurs.

- **Applicable à plusieurs méthodes de travail telles qu'accès, enregistrement horaire, cafétéria, etc.**
  - Donne la possibilité de différentes méthodes de travail selon les paramètres dans le menu de l'appareil.

- **Capacité étendue pour le traitement du serveur.**
  - Gestion d'un nombre presque illimité de personnes qui entrent via le serveur.

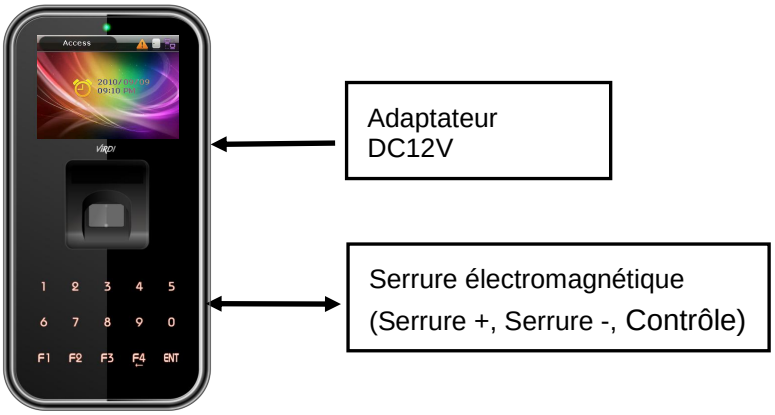
- **Offre une variété de méthodes d'enregistrement et d'authentification**

  Pour un utilisateur général, il y a 12 méthodes d'enregistrement et d'authentification. Il est donc nécessaire déterminer la méthode d'enregistrement et d'authentification avant que l'utilisateur ou l'administrateur ne soit enregistré.

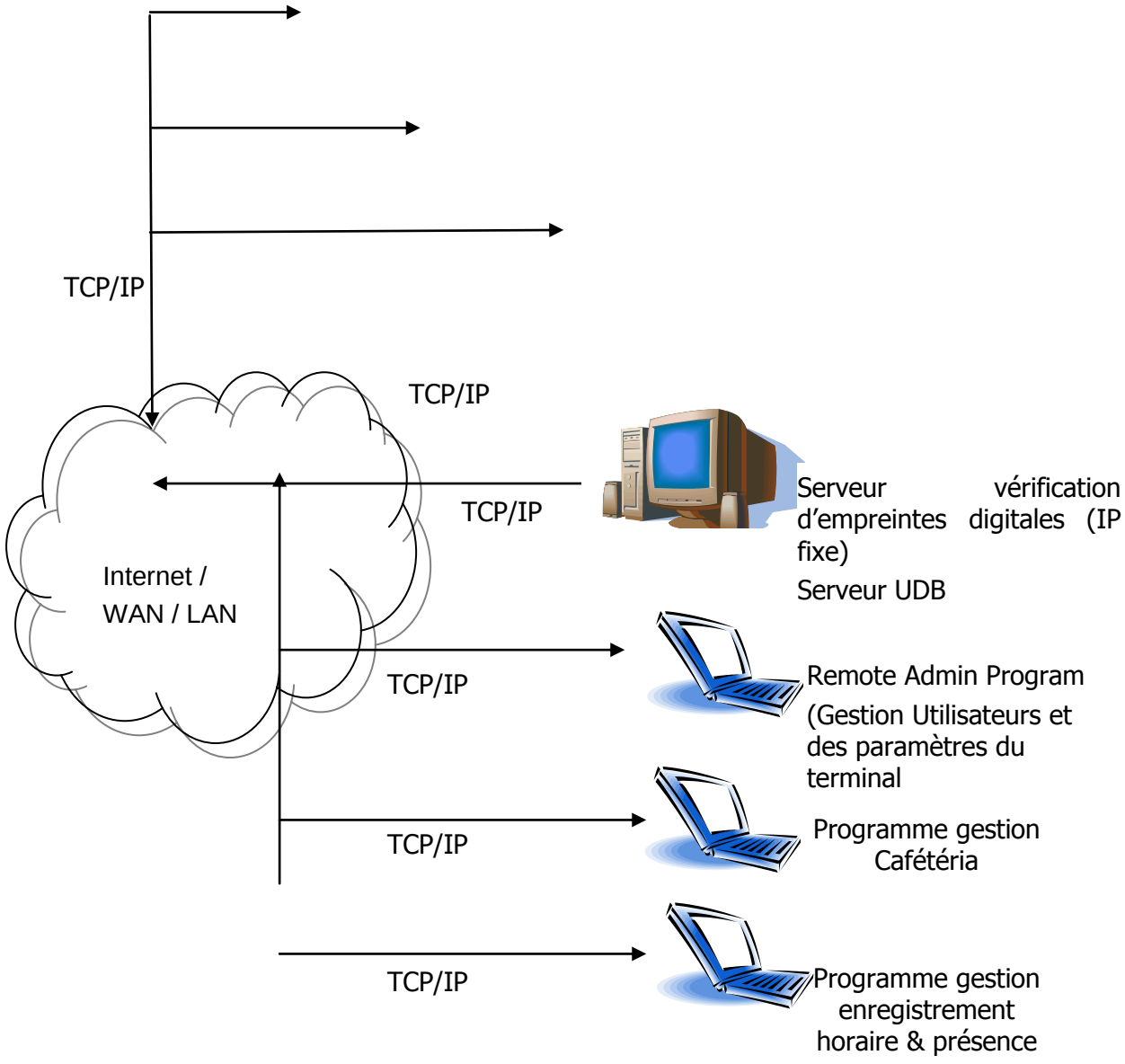
FP	Enregistrement d'empreintes digitales Vérification d'empreintes digitales
PW	Enregistrement mot de passe Vérification mot de passe
FP ou PW	Enregistrement d'empreintes digitales et mot de passe Vérification mot de passe lorsque la vérification d'empreinte échoue
FP & PW	Enregistrement d'empreintes digitales et mot de passe Vérification d'empreinte et ensuite vérification mot de passe
Card	Enregistrement carte Vérification carte
Card ou FP	Enregistrement carte et empreinte digitale Vérification carte ou empreinte digitale
Card & FP	Enregistrement carte et empreinte digitale Vérification carte et ensuite vérification empreinte digitale
Card ou PW	Enregistrement carte et mot de passe Vérification carte ou mot de passe
Card et PW	Enregistrement carte et mot de passe Vérification carte et ensuite vérification mot de passe
(ID ou Card) & FP	Enregistrement carte et empreinte digitale Saisir ID et ensuite vérification empreinte digitale ou vérification carte et ensuite vérification empreinte digitale
(ID ou Card) & PW	Enregistrement carte et mot de passe Saisir ID et ensuite vérification mot de passe, ou vérification carte et ensuite vérification mot de passe
Card & PW & FP	Enregistrement carte, mot de passe et empreinte digitale Vérification carte et ensuite vérification empreinte digitale & mot de passe

4.2 CONFIGURATION

4.2.1 AUTONOME (ACCES)



4.2.2 CONNEXION VIA LE SERVER PC (ACCES, ENREGISTREMENT HORAIRE, CAFETERIA)



4.3 SPECIFICATIONS

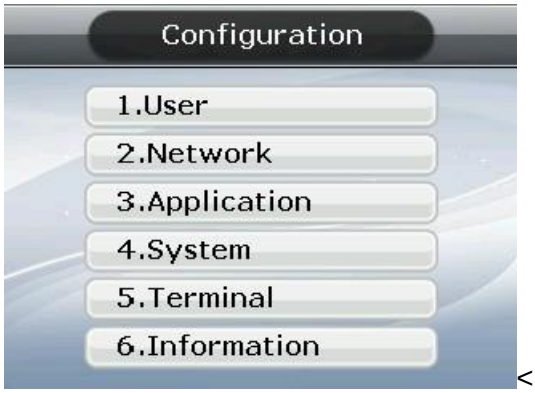
Division	SPEC	REMARQUE
CPU	32Bit RISC CPU (400MHz)	
Etanchéité	**IP65**	
LCD	**TFT 2.8" Couleur (320*240)**	
Touches tactiles	15 touches (0~9, F1~F4, Enter)	
Mémoire	32M SDRAM	
	32M FLASH	20,016 Utilisateurs 20,016 doigts 61,439 Log
Senseur Empreinte digitale	Optique	
Vitesse de vérification	Endéans 1 seconde	
Zone de Scan / Résolution	15 * 17mm / 500 DPI	
FRR / FAR	0.1% / 0.001%	
Température / Humidité	-20 ~ 50 / Inférieure à 90% RH	
POE	**Supporte 13W POE**	
Adaptateur AC / DC	Entrée : Universelle AC 100 ~ 250V	
	Sortie : DC 12V (Option : DC 24V)	
	Agréé UL, CSA, CE	
Contrôle serrure	EM, Strike, Serrure motorisée, Porte automatique	
I/O	3 Entrées (1 Exit, 2 Monitor) 2 Sorties (Contrôle serrure)	
Port de Communication	TCP/IP (10/100Mbps)	Communication Serveur Vérification
	RS-232	Imprimante ticket repas
	RS-485	Communication avec dispositif externe
	Wiegand In/Out	Lecteur carte ou comm. avec dispositif externe
Lecteur de carte	125KHz RF ou 13.56MHz Smart (1 SAM Socket)	Option
Dimensions	88.0mm * 175.0mm * 43.4mm	

5 PARAMETRES D'ENVIRONNEMENT

5.1 ELEMENTS A CONTROLER POUR LES PARAMETRES D'ENVIRONNEMENT

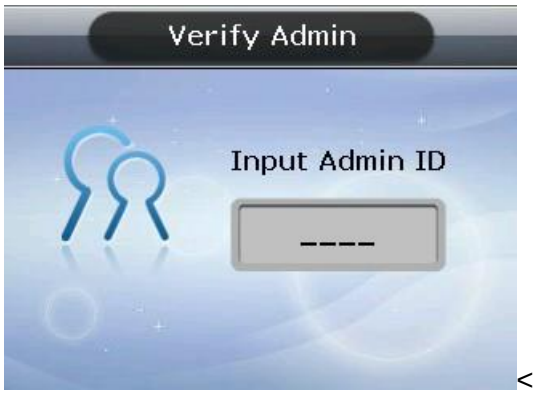
5.1.1 OUVRIR LE MENU

Appuyez pendant 2 secondes ou plus longtemps sur la touche [ENT], alors l'utilisateur peut consulter l'écran comme suit pour la sélection du menu.



<Figure 3-1>

L'utilisateur peut accéder à chaque sous-menu en cliquant sur la touche numérique correspondante. Si l'Admin est déjà enregistré, l'écran Verify Admin apparaît comme ci-dessous ;



<Figure 3-2>

Selon les méthodes de vérification enregistrées telles que Carte, Empreinte digitale ou Mot de passe, l'utilisateur peut accéder à chaque menu sujet à une identification réussie après que la vérification de l'Admin est terminée.

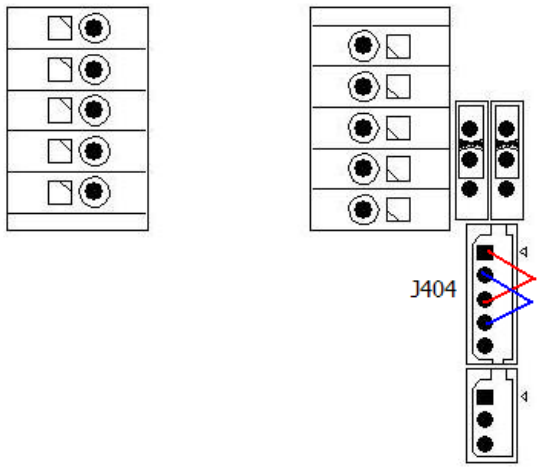
- Verify Admin apparaît uniquement si un Admin est enregistré. Une fois identifié dans le mode menu, l'utilisateur peut accéder à tous les menus jusqu'à ce qu'il quitte complètement le menu principal.

5.1.2 COMMENT ACCEDER AU MENU SANS LA VERIFICATION ADMIN.

Cette façon d'accéder au menu est inévitablement utilisée quand la vérification d'empreintes digitales est impossible parce que l'utilisateur a oublié le mot de passe Admin ou si on a perdu la carte enregistrée sur le terminal ou s'il n'y a aucun Admin.

① Enlevez le support à l'arrière du terminal pour ouvrir le couvercle

② Le couvercle ouvert, connectez comme illustré ci-dessous, la broche n°1 avec broche n°3 et la broche n°2 avec la n°4 du connecteur J404.



<Figure 3-3>

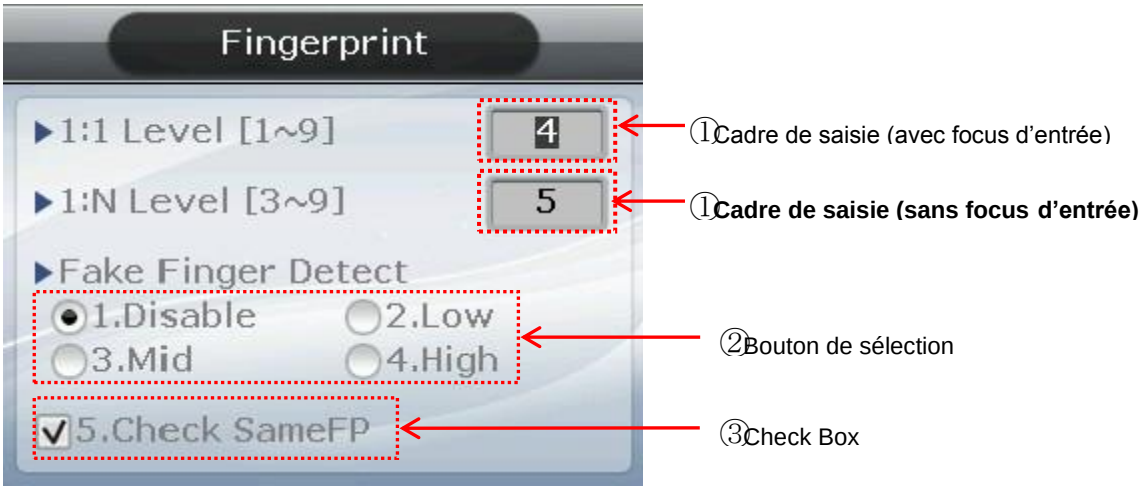
③ Accédez au menu en pressant la touche [F4 (←)] pendant 2 secondes ou plus, remplissez l'ID Admin avec '0' dans l'écran Verify Admin <Figure 3-2> et appuyez sur la touche [ENT]. L'utilisateur a alors accès au menu et le ronfleur émet un son ''Brrrrrrp''.

▸ N'oubliez pas après l'adaptation de la configuration de retirer les ponts sur les broches du connecteur J404.

5.1.3 MODIFIER LES VALEURS DEFINIES

Le nom et la méthode de saisie par élément.

<Figure 3-4>



▸ ① Cadre de saisie

Dans le cas où une valeur d'un élément doit directement être introduite comme ‘1:1 Level’, l'utilisateur doit supprimer la valeur existante avec la touche [F4 (←)]. Quand le focus se trouve dans le cadre de l'élément, entrez la nouvelle valeur via les touches [0] ~ [9].

▸ ② Bouton de sélection

Dans le cas où des éléments proposés comme ‘Fake Finger Detect’ (détection faux doigt) doivent être sélectionnés, l'utilisateur peut personnaliser la sélection ( ) en appuyant sur la touche numérique correspondante. Attention, l'utilisateur doit s'assurer que le focus se trouve sur les cases de sélection et non sur le cadre de saisie comme le montre la <Figure 3-5>. Vous pouvez déplacer le focus en appuyant sur la touche [ENT].

<Figure 3-5> Déplacer le Focus (Utiliser la touche [ENT])

Comme montré dans la figure gauche, les lettres affichées en blanc indiquent que le focus se trouve dans le cadre de saisie. Dans la figure de droite, vous voyez que si le focus est déplacé du cadre de saisie vers l'option ‘’Détection faux doigt’’, les lettres de cette option deviennent noires au lieu de grises

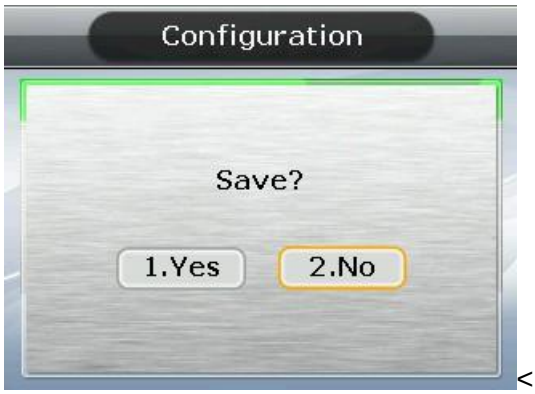
▸ ③ Check Box

Dans le cas où l'utilisateur doit faire un choix tel qu’activer ou non une option par ex. ‘Check Same FP’ (Vérifier ED identique), ce dernier peut sélectionner ( ) ou ( ) en cliquant sur la touche [5] appropriée. S’il n'est pas possible de sélectionner l'élément pertinent, il est affiché ( ).

Appuyez sur la touche [F4 (←)] pour annuler les paramètres adaptés et revenir au menu parent. Si le focus est mis sur le cadre de saisie, la touche [F4 (←)] fonctionne comme la touche [DEL] et efface les caractères un par un. Dans ce cas, pressez pendant 2 secondes ou plus la touche [F4 (←)] pour annuler la saisie et retourner au menu parent. Appuyez pendant 2 secondes ou plus sur la touche [ENT] pour enregistrer la configuration actuelle et pour retourner au menu parent.

5.1.4 SAUVEGARDER LES PARAMETRES D'ENVIRONNEMENT

Appuyez sur la touche [F4 (←)] dans l'écran de menu principal <Figure 3-1> pour enregistrer les paramètres personnalisés, l'écran suivant apparaît :



<Figure 3-6>

Sélectionnez [1. Yes] pour enregistrer le contenu personnalisé ou sur [2. No] pour annuler, puis appuyez sur [ENT]. Si pendant un certain temps aucune saisie n'est effectuée, le système revient à l'écran initial.

- S'il n'y a aucun contenu révisé, vous quittez le menu environnement sans passer la procédure de sauvegarde susmentionnée.

- Si des paramètres ont été modifiés dans le menu, et qu'il n'y a pas de saisie pendant un temps donné, alors le système quitte le menu environnement. Dans ce cas, puisqu'un menu a été modifié, vous passez par la procédure de sauvegarde. Sinon, le terminal retourne à l'écran initial sans enregistrer les paramètres adaptés.

5.2 MENU CONFIGURATION

1. User (Utilisateur) 	1. Add (Ajouter) 2. Delete (Effacer) 3. Modify (Modifier) 4. Delete All (Effacer tout)	
2. Network (Réseau) 	1. IP	1. Static IP (IP Statique) / 2. DHCP ▸IP Address (Adresse IP) ▸Subnet Mask (Masque de sous réseau) ▸Gateway (Passerelle)
	2. IP Server (Serveur IP)	▸IP Server (Serveur IP) ▸Server Port (Port Serveur)
	3. ID Terminal	▸ Terminal ID (ID du Terminal) ▸Authentification (Vérification)
3. Application 	1. Application	▸Application 1. Access (Accès) 2. Time & Attendance (Horaire & présence) 3. Cafeteria (Cafétéria)
	2. Time Schedule (Schéma horaire)	▸F1 Time (Temps F1) ▸ F2 Time (Temps F2) ▸ F3 Time (Temps F3) ▸ F1 Time (Temps F4) ▸Access Time (Temps d'accès) □NO Limit (En cas de paramètres pour gestion service traiteur (catering))
	3. Function Key (Touche de Fonction)	□F1 Enabled (F1 Actif) □F2 Enabled (F2 Actif) □F3 Enabled (F3 Actif) □F4 Enabled (F4 Actif) □Ent Enabled (Ent Actif) □Auto Sensing
	4. Extended Key (Touches étendues)	□ Extended Key (Touches étendues) ▸ou Extended Key (Touches étendues)
	5. Display (Affichage)	▸Background (Arrière plan) ▸Clock Position (Position horloge) □User Voive (Voix Utilisateur) □User Text (Texte Utilisateur)

4. System (Système) 	1. System Setting (Paramètres Système)	▸UserID Length (Longueur ID Utilisateur) ▸Display Option (Option affichage)
	2. Authentification (Vérification)	▸User GroupID (Utilisateur Groupe ID) ▸Enable 1:N (Actif 1:N) ▸Card Only (Carte uniquement) ▸Template on Card (Modèle sur Carte) ▸Verify Multi-FP (Vérifier Multi-ED) ▸Blocking Time (Temps de blocage) (sec.)
	3. Fingerprint (Empreinte digitale)	▸1:1 Level [1~9] (Niveau [1~9]) ▸1:N Level [3~9] (Niveau [3~9]) ▸Fake Finger Detect (Détection faux doigt) □Check SameFP (Contrôler ED identique)
	4. Language (Langue)	
	5. Data Time (Heure)	▸Time Sync (Sync temps) ▸Display Time (Afficher heure) ▸Set Current Time (Définir heure actuelle)
	6. Database	1. Init Config (Init Config) 2. Delete All Users (Effacer tous les utilisateurs) 3. Clear Log Data (Effacer Journal Data) 4. Initialize Terminal (Initialiser Terminal)
5. Terminal 	1. Terminal Option (Option du Terminal)	□Terminal Alarm (Alarme Terminal) □Lock Terminal (Serrure Terminal) □KeyLed ON (Touche Led ON)
	2. Volume Control (Contrôle Volume)	▸Voice Volume (Volume Voix) ▸Beeper Volume (Volume Ronfleur)
	3. Door (Porte)	▸Lock Type (Type serrure) ▸Door Monitor (Contrôle Porte) ▸Open Duration (Temps ouverture porte) ▸Warn Door Open (Avertissement porte ouverte)
	4. Wiegand	□Bypass (Exclure) ▸Wiegand Out (Sortie Wiegand) ▸Site Code (Code Site)
	5. Card Reader (Lecteur de Carte)	▸Card Format (Format carte) ▸Read Card NO (Lire n° carte)
	6. External Device (Appareil externe)	▸Printer (Imprimante) ▸Lock Controller (Contrôleur serrure)
6. Information	1. System Info (Info Système) 2. Network Info (Info Réseau) 3. Database Info (Info Database)	

	4. View Log (Visualiser Journal) 5. Version Info (Info Version)

5.3 UTILISATEUR

Sélectionnez “1. User” dans le menu principal, l’écran suivant apparait.

Appuyez sur la touche:
[1] pour ajouter un nouvel utilisateur,
[2] pour effacer un utilisateur,
[3] pour modifier un utilisateur
[4] pour effacer tous les utilisateurs.

5.3.1 AJOUTER

◆ Sélectionnez [ENT~] → [1.User] → [1.Add] ◆ dans l’écran de base, l’écran suivant s’affiche :

Introduisez l’ID utilisateur à enregistrer et appuyez sur [ENT].

Dans ce cas, l'ID utilisateur libre est automatiquement affiché de sorte que l'utilisateur puisse facilement être enregistré. Pour adapter l'ID, appuyez sur [F4 (←)], supprimez la valeur actuelle et entrez une nouvelle valeur.

Si l'utilisateur saisit un ID déjà existant, un message d'erreur apparaît. L'écran suivant s'affiche si l'ID n'a pas encore été enregistré.

Les icones à gauche ont la signification suivante;

: Type de Vérification

: Nombre d’ED enregistrées (0~10)

: Nombre de cartes enregistrées (0~10)

: Si oui ou non un mot de passe est enregistré? (: Enregistré / : Non enregistré)

Comme vous pouvez voir sur la capture d'écran ci-dessus, l'utilisateur peut enregistrer une empreinte en appuyant sur [2], sur [3] pour encoder une carte et sur [4] pour créer un mot de passe. En principe, cela est enregistré dans nom de l'utilisateur. Utilisez les touches [7] et [8] pour définir l’utilisateur comme utilisateur et Admin. Une fois l'enregistrement terminé, l'utilisateur peut appuyer sur [ENT] pour sauvegarder. L'utilisateur peut aussi cliquer sur [F4 (←)] pour annuler l'enregistrement et quitter le menu.

※ Seul l'utilisateur défini en tant qu'Admin peut changer l'environnement de travail du terminal et Ajouter/Modifier/Effacer les données de tous les utilisateurs stockés dans le terminal. Vous devez donc être prudent lors de l'enregistrement d'un Admin.

5.3.1.1 TYPE DE VERIFICATION

Effacez la valeur existante en appuyant sur [F4 (←)], sélectionnez un des 12 types de vérification affichés à l'écran et appuyez sur [ENT].

5.3.1.2 ENREGISTRER ED

① Place finger on sensor (Placez le doigt sur le senseur voir 1.8). Vous devez saisir et enregistrer l'empreinte digitale. L'empreinte digitale doit être saisie deux fois comme demandé à l'écran

Quand le senseur d'empreintes digitales est éclairé et que le message 'Placez votre doigt sur le senseur' s'affiche, placez le doigt sur le capteur pendant 2 ~ 3 secondes jusqu'à ce que la lumière s'éteigne.

②Si le message 'Place same finger on sensor' (Placez le même doigt sur le senseur) s'affiche, placez à nouveau le même doigt sur le capteur comme ci-dessus.

※À la 2ème présentation du doigt, ceci est à nouveau proposé après que l'utilisateur ait enlevé le doigt du capteur.

③ Lorsque la saisie est faite, le message ci-contre apparaît. L'image s'accompagne d'un niveau de qualité de 0 ~ 100.

Si l'impression n'est pas suffisamment claire et que la valeur affichée est de 30 ou moins, l'utilisateur est avisé d'effectuer une nouvelle saisie.

Pour une nouvelle saisie, relancez le processus à partir de ① en appuyant sur [F4 (←)]. Après achèvement, l'appareil retourne au menu précédent.

※ L'enregistrement d'empreintes digitales est disponible jusqu'à 10 par ID. Un message d'erreur apparaîtra lorsque la tentative d'enregistrement dépasse 10.

Dans le cas où l'enregistrement échoue malgré plusieurs tentatives (2 ~ 3 fois) en utilisant la méthode d'enregistrement correcte d'empreintes digitales, il est alors recommandé à l'utilisateur d'utiliser une carte ou un mot de passe.

5.3.1.3 ENREGISTRER CARTE

Lorsque l'écran d'enregistrement carte apparaît, présentez la carte au lecteur. Si vous voulez quitter le menu sans enregistrer, appuyez sur [F4 (←)].

5.3.1.4 ENREGISTRER MOT DE PASSE

Introduisez un mot de passe de 1~8 chiffres sur l'écran de saisie mot de passe et appuyez sur [ENT].

L'écran 'Confirm Password' (Confirmer mot de passe) s'affiche. Introduisez à nouveau le même mot de passe et appuyez sur [ENT].

Appuyez sur [F4(←)] pendant 2 secondes ou plus pour annuler et quitter le menu.

5.3.1.5 OPTION ED

Cette option étant liée à l'empreinte digitale, elle peut être modifiée après l'enregistrement de l'empreinte. Si l'utilisateur la sélectionne avec une empreinte digitale déjà enregistrée, il en résultera uniquement une tonalité de défaut.

▶'1:1 Level' (Valeur par défaut: '0')

C'est l'élément qui enregistre le niveau de vérification pour chaque utilisateur. En modifiant cette valeur, il est possible de déterminer le niveau de vérification des utilisateurs enregistrés.

Si défini sur '0', la vérification se fait via le niveau de vérification 1:1 du terminal.

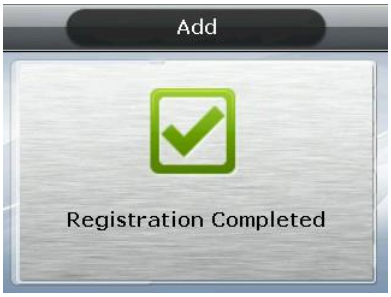
▶'Enable 1:N (Valeur par défaut: 'v')

Si cette option est cochée, une vérification réussie est possible par le biais d'empreinte digitale sans carte ni ID utilisateur.

5.3.1.6 SAUVER

Si le processus d'enregistrement est terminé, appuyez sur [6] pour sauvegarder. Si vous pressez sur [F4 (←)] (et pas sur [6]), vous quittez le menu sans sauvegarder l'utilisateur.

Le message suivant indique que l'utilisateur peut quitter le processus d'enregistrement.

	Si l'enregistrement s'est effectué normalement en appuyant sur la touche [6. Save].
	Si l'enregistrement a échoué en appuyant sur la touche [6. Save]. Si le mode d'enregistrement ne correspond pas à la méthode de vérification. Par exemple : l'utilisateur n'a pas enregistré d'empreinte digitale après avoir défini l'empreinte comme moyen de vérification, n'a pas enregistré de carte après avoir sélectionné ce mode d'authentification.
	Dans le cas de [2. FP Register] Si l'empreinte digitale n'est pas de bonne qualité ou s'il n'y a aucune empreinte digitale saisie pendant les 10 secondes qui suivent l'activation de la lampe de capteur d'empreintes digitales. Au moment de l'enregistrement des empreintes digitales, si l'utilisateur ne présente pas la même empreinte digitale mais une autre.
	Dans le cas de [4. PW Register] Si l'utilisateur saisit un autre numéro lors de la vérification avoir l'introduction d'un mot de passe.
	Dans le cas de [3. Card Register] Si l'utilisateur tente d'enregistrer une carte qui est déjà encodée.

Dans le cas de [2. FP Register]

Si l'utilisateur tente d'enregistrer une empreinte déjà existante.

※Si l'utilisateur souhaite enregistrer une même empreinte avec un autre ID, alors il doit désactiver l'option suivante '4. System → 3. Fingerprint → Check SameFP'. Ceci ne convient pas à l'application enregistrement horaire, etc. parce que les mêmes empreintes digitales peuvent être vérifiées avec différents ID au moment de l'authentification.

Dans le cas de [2. FP Register] ou [3. Card Register]

Si l'utilisateur essaye d'enregistrer plus que le nombre maximal autorisé (Max 10).

5.3.2 EFFACER

Si l'utilisateur sélectionne [ENT~] → [1. User] → [2. Delete] dans le menu principal, l'écran suivant apparait:

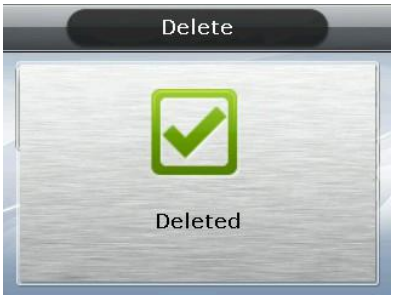
Introduisez l'ID utilisateur à effacer et appuyez sur [ENT].

En cas de saisie d'un ID non enregistré, un message d'erreur s'affichera. Un message de succès apparait lors de l'introduction d'un ID enregistré.

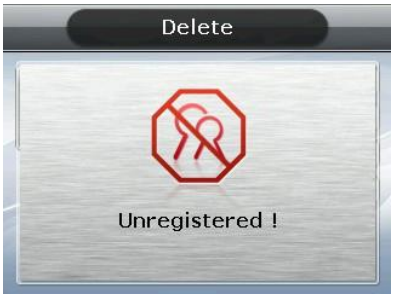
Effacer un utilisateur du terminal ne signifie pas que cet utilisateur est supprimé du serveur. Il est donc nécessaire d'effacer l'utilisateur du serveur pour qu'il soit complètement supprimé.

Attention : Effacer est possible par l'utilisateur ou un Admin. Un utilisateur enregistré dans le terminal ne peut plus être rétabli à moins qu'il soit également enregistré sur le serveur de réseau.

Le message suivant apparait durant le processus d'effacement:

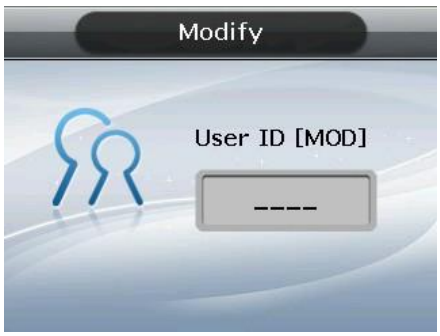


Lorsque l'effacement est OK.

	Si l'utilisateur entre un ID non enregistré

5.3.3 MODIFIER

Si l'utilisateur sélectionne [ENT~] → [1. User] → [3. Modify] dans le menu principal, l'écran suivant apparait :



Appuyez sur [ENT] après avoir introduit l'ID que vous souhaitez modifier.

Lors de l'introduction d'un ID non enregistré, un message d'erreur apparait.
Lors de l'introduction d'un ID enregistré, l'écran suivant apparait :

Les icones à gauche sont décrites respectivement par la signification de droite.

: Type de Vérification (ED)

: Nbre d'empreintes digitales enregistrées (1)

: Nombre de cartes enregistrées (0)

: Si oui ou non un mot de passe est enregistré (: non enregistré)

Pour les modifications, voir le chapitre ' 5.3.1. Add '. C'est exactement la même chose qu'illustré dans la méthode d'enregistrement.

5.3.4 TOUT EFFACER

Si l'utilisateur sélectionne [ENT~] → [1. User] → [4. Delete All] dans le menu principal, l'écran suivant apparait :

Si l'utilisateur est certain que tous les utilisateurs peuvent être effacés, alors appuyez sur [1.Yes] → [ENT]. Sélectionnez [2.No] → [ENT] pour annuler.

※Si l'utilisateur choisit [1.Yes], aussi bien l'utilisateur que l'Admin sont supprimés. Soyez prudent, car si l'utilisateur/Admin est supprimé, il ne peut plus être restauré.

5.4 RESEAU

Lorsque l'utilisateur sélectionne "2. Network" dans le menu principal, l'écran suivant apparaît.

Appuyez sur la touche correspondant au numéro de l'item à modifier.

5.4.1 IP

Si l'utilisateur sélectionne [ENT~] → [2. Network] → [1. IP] dans l'écran initial, l'écran suivant apparaît.

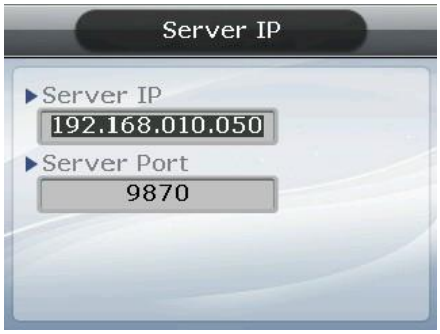
Lors d'un changement d'adresse IP, effacez tout d'abord la valeur existante via [F4 (←)] et entrez la nouvelle valeur. Le '.' entre la séquence chiffrée est généré automatiquement. P.ex. introduisez 192 168 010 50 pour obtenir '192.168.10.50'.

Sélectionnez [1] dans le cas où vous travaillez avec une adresse IP fixe du réseau connecté. Sélectionnez l'option [2] dans le cas où un serveur DHCP est présent sur le réseau connecté à partir duquel l'appareil reçoit son adresse IP. Définissez l'adresse IP, le masque de sous-réseau et la passerelle si vous travaillez avec une adresse IP fixe. Il n'est pas nécessaire de faire cela, si l'utilisateur a sélectionné une adresse IP variable.

L'utilisateur peut revenir au menu supérieur via la touche [ENT~] pour valider les modifications lorsque la configuration est effectuée. Il peut aussi utiliser la touche [F4 (←)] pour annuler le paramètre pendant la configuration. Dans ce cas, l'utilisateur peut quitter le menu en appuyant sur le bouton pendant 2 secondes ou plus si une valeur est introduite dans le cadre d'introduction.

5.4.2 SERVEUR IP

Si l'utilisateur sélectionne [ENT~] → [2. Network] → [1. Server IP] dans l'écran initial, l'écran suivant apparaît :



Définissez le Serveur IP et le numéro de Port.

Pour modifier le numéro de port, déplacez-vous d'abord sur 'Server Port' et appuyez sur [ENT].

▸Paramètre par défaut

Server Port: '9870'

Le port de base pour le serveur d'authentification est '9870' pour le serveur UNIS et '2201 ' le serveur Acces. Soyez prudent lorsque vous changez les numéros de port parce que ces valeurs doivent être aussi modifiées dans le programme du serveur.

L'utilisateur peut quitter le menu supérieur en appuyant sur la touche [ENT~] et enregistrer les valeurs modifiées ou en appuyant sur [F4(←)~] et annuler la modification.

5.4.3 ID TERMINAL

Si l'utilisateur sélectionne [ENT~] → [2. Network] → [3. Terminal ID] dans l'écran initial, l'écran suivant apparaît.

Définissez l'ID du Terminal et la Vérification.

▸Configuration par défaut

Terminal ID: '1'

Authentication: '2. terminal/server'

Terminal ID est un ID unique utilisé par le serveur d'authentification pour identifier le terminal. Par défaut, l'ID de chaque terminal est '1'. Ceci doit correspondre à l'ID de la porte d'entrée/sortie défini dans le programme serveur, il peut comporter un maximum de 8 chiffres.

▸ Authentication

Cet item détermine la priorité pour l'authentification entre le terminal et le serveur réseau. Si '2. Terminal/Server' est défini comme valeur standard, voici le fonctionnement dans chaque mode :

1.Server/Terminal	L'authentification s'effectue par le serveur quand le terminal est connecté au serveur. Si c'est n'est plus connecté suite à des défaillances du réseau, etc., la vérification est réalisée par le terminal lui-même.
2.Terminal/Server	L'authentification effectuée par le terminal même si le serveur est connecté et le résultat de l'authentification est transféré sur base temps réel vers le serveur. Mais, l'authentification est bien exécutée par le serveur lorsque l'ID utilisateur ou la carte n'est pas enregistré dans que le terminal. (Dans le cas de l'authentification d'empreintes digitales 1:N aucune vérification serveur n'est faite).
3. Server Only	Même si l'utilisateur est enregistré dans le terminal, l'authentification est effectuée par le serveur. Par conséquent, il n'y a aucune vérification si le serveur n'est pas connecté.
4. Terminal Only	Seul l'utilisateur qui est enregistré dans le terminal est vérifié. Si le serveur est connecté, le résultat de cette vérification est envoyé en temps réel vers le serveur

Une désignation flexible est autorisée selon les circonstances, telles que le nombre de terminaux connectés au serveur, le nombre d'utilisateurs authentifié ou un dérangement du réseau, etc. Il est conseillé d'utiliser '2 Terminal/Server' de sorte que les vérifications puissent s'effectuer simultanément s'il y a au moins 10 terminaux connectés au serveur ou lorsqu'il y a de fréquentes pannes de réseau en général.

5.5 APPLICATION

Quand l'utilisateur sélectionne '3. Application' dans le menu principal, l'écran suivant apparaît :

Appuyez sur le chiffre associé à l'élément que vous souhaitez adapter.

5.5.1 APPLICATION

Quand l'utilisateur sélectionne [ENT~] → [3. Application] → [1. Application] dans l'écran initial, l'écran suivant apparaît :

Sélectionnez le type de fonctionnement du terminal en pressant le chiffre correspondant.

Appuyez sur [ENT] pour adapter la configuration ou [F4(←)] pour annuler.

5.5.2 SCHEMA HORAIRE

5.5.2.1 DEFINIR ACCES / TEMPS & PRESENCE

Quand l'utilisateur sélectionne [ENT~] → [3. Application] → [2. Time Schedule] dans l'écran initial, l'écran suivant apparaît:

►Paramètre par défaut: Identique à l'écran à ci-contre.

L'utilisateur peut définir des zones de temps par mode de vérification, autrement définissez '00:00-00:00'.

Après avoir effacé la valeur existante avec [F4(←)], introduisez la nouvelle valeur en format HHMM (Heure/Minute) de 00:00 à 23:59

Dans la zone horaire prédéfinie, cela est toujours indiqué dans le mode prédéfini sauf si l'utilisateur presse une autre touche de fonction. Lorsqu'un utilisateur appuie sur une touche de fonction à laquelle aucun schéma horaire n'est couplé, l'écran du terminal passera automatiquement au mode d'authentification adapté pour la gestion du Temps & Présence.

Comme illustré dans l'exemple ci-dessous, chaque zone horaire doit être définie sans chevauchement, mais le mode est déterminé comme F1→F2→F3→F4→Accès séquentiel si elles se chevauchent.

(Par ex.) Arriver Bureau=06:00~09:59, Quitter Bureau=17:00~22:00

Quittez le menu parent en appuyant sur [ENT~] et enregistrer les valeurs adaptées. Appuyez sur [F4(←)~] pour annuler les adaptations.

5.5.2.2 DEFINIR COMME CAFETERIA

▸ Paramètre par défaut: Identique à l'écran à ci-contre.

L'utilisateur peut définir des zones horaires par type de repas, autrement laisser '00:00-00:00'.

▸No Limit

Si la case (☐) n'est pas active, chaque utilisateur peut être authentifié une fois par repas, mais si la case (☑) est activé, il est permis d'effectuer plusieurs vérifications malgré la vérification déjà faite.

5.5.3 TOUCHE DE FONCTION

Si l'utilisateur sélectionne [ENT~] → [3.Application] → [3. Function Key] dans l'écran initial, l'écran suivant apparaît :

▸ Paramètre par défaut: Identique à l'écran à ci-contre.

Touche de fonction signifie les touches [F1]~[F4], [ENT] qui sont utilisées pour changer le mode d'authentification tel qu'Arriver Bureau / Quitter Bureau, etc.. Si l'utilisateur appuie sur la touche de fonction, le mode d'authentification passe vers le mode approprié. Si celui-ci n'est pas actif, le mode d'authentification ne change pas même lorsqu'on presse la touche de fonction. C'est pourquoi, cela peut être utilisé avec l'autre touche de fonction contrôlée dans le cas où le terminal est utilisé exclusivement pour Bureau début ou Bureau fin.

Dans le cas où la case '6. Auto Sensing' est désactivée, le capteur d'empreintes digitales ne réagira pas même si l'utilisateur met son doigt sur le capteur. Dans ce cas, vous devez certainement introduire, pour l'utilisateur, un ID ou une Carte ou une Empreinte.

5.5.4 TOUCHE ETENDUE

Si l'utilisateur sélectionne [ENT~] → [3.Application] → [4. Extended Key] dans l'écran initial, l'écran suivant apparaît :

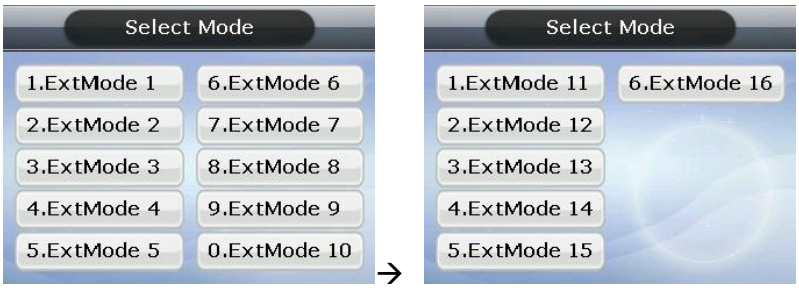
▸ Paramètre par défaut: Identique à l'écran à ci-contre.

Pour utiliser Touche Etendue, appuyez sur [1] et activez la case '1. Extended Key'. Le nombre de touches étendues peut être défini dans une plage de 1~40.

Touche Etendue est la fonction qui élargit le numéro tel qu'exigé jusqu'à 40 si plusieurs modes d'authentification sont nécessaires en plus des touches de fonction de base ([F1]~[F4], [ENT]). Dans ce cas vous obtenez l'écran comme vous le voyez sur les screenshots ci-dessous dans lesquels vous pouvez sélectionner les touches étendues en appuyant sur la touche F4. Sélectionnez le mode qui est d'application avec les touches [0]~[9].

Si le nombre de touches étendues est supérieur à 10, sélectionnez cela en changeant de page via les touches [F1]~[F4]

(Par ex.) Dans le cas où le nombre de touches étendues est de 16, appuyez sur [F4] dans l'écran initial et l'écran suivant apparaîtra :



Si l'utilisateur doit sélectionner Mode Etendu 12, allez à la page suivante avec la touche [F2] et appuyez sur [2].

Appuyez sur [ENT] pour quitter ce menu sans sélectionner de Mode Etendu.

L'utilisateur peut quitter le menu parent en appuyant sur [ENT~] et enregistrer les données modifiées ou appuyez sur la touche [F4 (←)] pour annuler l'introduction.

5.5.5 ECRAN

Si l'utilisateur sélectionne [ENT~] → [3.Application] → [5. Display] dans l'écran initial, l'écran suivant apparaît :

▸ Paramètre par défaut: Identique à l'écran à ci-contre

▸Image de fond

L'utilisateur peut changer l'image d'arrière-plan de l'écran principal en pressant les touches [1] et [2]. L'utilisateur peut aussi définir un cycle de 5 secondes ou plus pour afficher séquentiellement les images d'arrière-plan.

▸Position Horloge

Modifie l'emplacement de l'horloge sur l'écran initial.

Selon le besoin/préférence de l'utilisateur, celui-ci peut télécharger un fichier audio WAV (16bit/8kHz) pour modifier le message vocal en cas d'authentification réussie ou échouée. En outre, l'utilisateur peut télécharger le texte de l'image dans un formulaire personnalisé, tel que Bureau début ou Bureau en utilisant pour cela le fichier source spécialement fait pour cela (fichier Excel). Dans ce cas, l'utilisateur peut appliquer le contenu personnalisé uniquement lorsque les cases '6. Voix de l'utilisateur', et '7. Texte de l'utilisateur' sont cochées. Pour la méthode de téléchargement, voir chapitre '3.9. Télécharger fichier personnalisé'.

L'utilisateur peut quitter le menu parent et sauvegarder les valeurs adaptées en appuyant sur [ENT~]. Il peut aussi appuyer sur [F4 (←)] pour annuler la configuration.

5.6 SYSTEME

En cas de sélection de l'option '4. System' dans le menu principal, l'écran suivant apparaît :

Appuyez sur la touche associée à l'élément que vous souhaitez adapter.

5.6.1 CONFIGURATION SYSTEME

Si l'utilisateur sélectionne [ENT~] → [4. Système] → [1. System Setting] dans l'écran initial, l'écran suivant apparaît :

▸ Paramètre par défaut: Identique à l'écran à ci-contre

▸ UserID Length (Longueur ID Utilisateur)

Ce champ définit la longueur de l'ID utilisateur, celui-ci peut être modifié dans une plage de 1 à 9 chiffres. Il doit être identique à la longueur de l'ID enregistré dans le programme serveur. Par exemple, l'utilisateur doit définir la longueur de l'ID sur 6 si l'ID enregistré dans le programme serveur est 000075 qui comprend 6 chiffres.

▸ Display Option (Option Ecran)

Si défini sur '1. Aucun', le message résultat de l'authentification s'affiche uniquement en cas de réussite de l'authentification réussie. Si défini sur '2', l'ID Utilisateur est affiché. Si défini sur '3', '4' et '5', le nom d'utilisateur, la clé utilisateur et le message s'affiche successivement sur l'écran LCD. Cependant, l'ID est affiché dans le cas où il n'y a aucune information pertinente de l'utilisateur stockée dans le terminal.

L'utilisateur peut quitter le menu parent et sauvegarder les valeurs adaptées en appuyant sur [ENT~]. Il peut aussi appuyer sur [F4 (←)] pour annuler la configuration.

5.6.2 VERIFICATION

Si l'utilisateur sélectionne [ENT~] → [4. System] → [2. Authentication] dans l'écran initial, l'écran suivant apparaît :

▸ Paramètre par défaut: Identique à l'écran à ci-contre

▸User GroupID (Utilisateur Groupe ID)

Si la méthode d'authentification du chiffre initial de l'ID a le même groupe, la vérification 1:N est effectuée beaucoup plus vite s'il y a au moins 5000 utilisateurs enregistrés

Si cette méthode est cochée, cela authentifie l'empreinte digitale de l'utilisateur dont l'ID commence par la lettre donnée. Si cette méthode n'est pas cochée alors la figure importée est considéré comme l'ID utilisateur et une vérification 1:1 de l'empreinte digitale de l'utilisateur est effectuée avec l'ID appliqué.

Ex : Si l'utilisateur introduit '12' pour effectuer l'authentification quand l'ID utilisateur est une valeur de 4 chiffres

Si actif (☑) alors une vérification 1:N s'effectue parmi les utilisateurs ayant un ID '1200'~'1299',

Si non actif (☐), alors une vérification 1:1 est effectuée avec l'empreinte digitale de l'utilisateur dont l'ID est '12'.

▸ Enable 1 :N (1:N Actif)

Si cochée (☑), cette option donne la possibilité de vérifier simplement une empreinte sans introduire un ID utilisateur ou une carte. Si cette option n'est pas cochée dans le terminal, seule la vérification 1:1 peut se produire même si l'utilisateur est enregistré avec la vérification 1:N.

▸Card Only (Carte uniquement)

Si cochée (☑), cette option permet d'authentifier uniquement avec carte sans présenter une empreinte digitale. Même si l'utilisateur est enregistré avec (Carte & ED) ou (Carte & MP), l'authentification avec carte est la seule autorisée sur le terminal où cette option est cochée.

▸Template on Card (Modèle sur Carte)

Si cochée (☑), cette option permet l'authentification avec l'information utilisateur et empreinte stockées dans la carte sans télécharger l'utilisateur dans le terminal. Pour utiliser cette option, le lecteur carte SC doit absolument être monté et le serveur doit définir le terminal qui utilise Carte Empreintes digitales.

▸ Verify Multi-FP (Vérifier Multi ED)

Si cochée (☑), cette fonctionnalité garantit que toutes les empreintes enregistrées doivent être authentifiés après que l'utilisateur ait introduit un ID ou présenté une carte. Si cet élément est défini pour être contrôlé, l'utilisateur doit toujours entrer un ID utilisateur ou présenter une carte. Dans ce cas, l'option Actif 1:N est automatiquement désactivée (☐).

Cette fonction est utilisée pour le contrôle d'accès strict d'une zone spéciale. Par exemple, si l'utilisateur avec l'ID '0001' est enregistré avec 3 empreintes, il doit introduire l'ID et effectuer l'authentification complète des 3 empreintes. Dans ce cas l'ordre d'authentification des 3 empreintes n'est pas important, mais les empreintes doivent être présentées à plusieurs reprises jusqu'à ce que l'authentification soit réussie. L'authentification faillira en cas d'échec d'une seule vérification pendant l'introduction des différentes empreintes digitales.

▸ Blocking Time (Blocage Horaire) (sec)

Cette fonction prévient la double authentification du même utilisateur dans une zone horaire prédéfinie. Si la valeur est 0, alors il n'y aucune restriction. En revanche, si la valeur est supérieure à 0, alors l'utilisateur peut seulement être revérifié avec succès si le temps prédéfini s'est écoulé après une précédente authentification réussie.

L'utilisateur peut quitter le menu parent et sauvegarder les valeurs adaptées en appuyant sur [ENT~]. Il peut aussi appuyer sur [F4 (←)] pour annuler la configuration.

5.6.3 EMPREINTE DIGITALE

Si l'utilisateur sélectionne [ENT~] → [4. System] → [3. Fingerprint] dans l'écran initial, l'écran suivant apparaît :

▸ Paramètre par défaut: Identique à l'écran à ci-contre

▸1:1 Level (Niveau 1:1)

Niveau de vérification utilisé pour l'Authentification d'empreintes digitales 1:1, à condition que le niveau d'authentification 1:1 de l'utilisateur pertinent s'applique à l'utilisateur dont le niveau d'authentification 1:1 ne soit pas défini sur '0' (en utilisant le niveau d'authentification du terminal)

▸1:N Level (Niveau 1:N)

Niveau d'authentification utilisé pour Authentification d'empreintes digitales 1:N. Dans le cas d'une authentification 1:N, le niveau de vérification pour les utilisateurs n'est pas défini et donc est toujours basé sur le niveau d'authentification du terminal.

▸ Fake Finger Detect (Détection faux doigt)

Il définit le niveau LFD qui neutralise l'utilisation d'imitations d'empreintes digitales. Lorsque la valeur du niveau LFD est élevée, cela a tendance à renforcer la fonction qui empêche l'introduction d'imitations d'empreintes faites en caoutchouc, papier, film, silicone, etc.. Mais même lorsque vous présentez une vraie empreinte digitale, il se peut que cette dernière ne soit pas lue correctement celle-ci est trop sèche.

▸ Check SameFP (Vérifier ED identique)

Si coché (☑), cette fonction vérifie, pendant l'enregistrement, si une empreinte a déjà été enregistrée ou non, ceci afin d'éviter que la même empreinte digitale soit allouée à un autre ID utilisateur.

L'utilisateur peut quitter le menu parent et sauvegarder les valeurs adaptées en appuyant sur [ENT~]. Il peut aussi appuyer sur [F4 (←)] pour annuler la configuration.

5.6.4 LANGUE

Si l'utilisateur sélectionne [ENT~] → [4. Système] → [4. Language] dans l'écran initial, l'écran suivant apparaît :

▸Paramètre par défaut : '1. English'

En cas de modification du paramètre de langue, les messages vocaux et les messages à l'écran sont aussi changés dans l'écran vers la langue sélectionnée.

L'utilisateur peut quitter le menu parent et sauvegarder les valeurs adaptées en appuyant sur [ENT~]. Il peut aussi appuyer sur [F4 (←)] pour annuler la configuration.

5.6.5 DATA HEURE

Si l'utilisateur sélectionne [ENT~] → [4. System] → [5. Data Time] dans l'écran initial, l'écran suivant apparaît :

- Paramètre par défaut: Identique à l'écran à ci-contre

- Time Sync (Synchronisation de l'Heure)

  Ici vous définissez la méthode de synchronisation de l'heure actuelle du terminal avec le serveur. Pour synchroniser automatiquement l'heure du terminal avec l'heure du serveur, sélectionnez '1. Auto', si vous voulez le faire manuellement sélectionner '2. Manual'.

- Display Time (Affichage de l'heure)

  Méthodes pour afficher l'heure actuelle sur le terminal. '1' pour système 24 heures et '2' pour système AM/PM

- Set Current Time (Définir l'heure actuelle)

  Ceci change l'heure actuelle du terminal. Aucun changement n'est nécessaire car la synchronisation est réalisée avec l'heure du serveur si le serveur est en ligne et la synchronisation de l'heure définie sur '1. Auto'.

L'utilisateur peut quitter le menu parent et sauvegarder les valeurs adaptées en appuyant sur [ENT~]. Il peut aussi appuyer sur [F4 (←)] pour annuler la configuration.

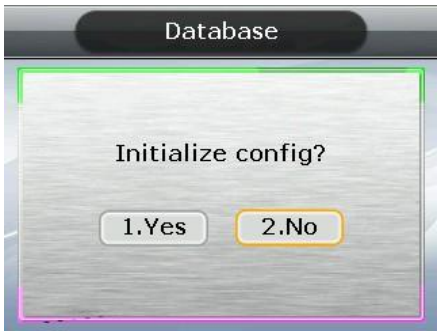
5.6.6 DATABASE

Si l'utilisateur sélectionne [ENT~] → [4. System] → [6. Database] dans l'écran initial, l'écran suivant apparaît :

Appuyez sur les touches suivantes;
Touche [1] pour initialiser la configuration,
Touche [2] pour effacer tous les utilisateurs,
Touche [3] pour effacer le fichier vérification,
Touche [4] pour initialiser le terminal.

5.6.6.1 INIT CONFIG

Si l'utilisateur sélectionne [ENT~] → [4. System] → [6. Database] → [1. Init Config] dans l'écran initial, l'écran suivant apparaît :



Appuyez sur [1.Yes] pour initialiser toutes les configurations. Appuyez sur [2.No] et sur [ENT] pour annuler.

Si rien n'est entré pendant un certain temps dans cet écran, le système reviendra à l'écran initial sans avoir initialisé.

Ceci rétablit en valeurs usine toutes les configurations du terminal excepté l'adresse MAC (physique). Les utilisateurs et le fichier de vérification ne sont pas supprimés. Si la configuration est réinitialisée avec succès, l'appareil revient au menu parent et un ronfleur émet une tonalité de réussite.

5.6.6.2 EFFACER TOUS LES UTILISATEURS

Si l'utilisateur sélectionne [ENT~] → [4. System] → [6. Database] → [2. Delete All Users] dans l'écran initial, l'écran suivant apparaît :

Appuyez sur [1.Yes] pour effacer tous les utilisateurs. Appuyez sur [2.No] et sur [ENT] pour annuler.

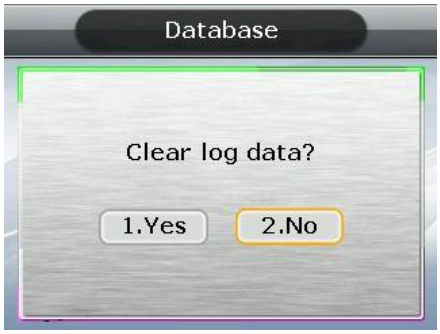
Si rien n'est entré pendant un certain temps dans cet écran, le système reviendra à l'écran initial sans rien avoir effacé.

L'utilisateur et l'administrateur seront supprimés et les utilisateurs supprimés ne peuvent plus être restaurés après la suppression.

Si la suppression est réussie, l'appareil revient au menu parent et un ronfleur émet une tonalité de succès.

5.6.6.3 EFFACER FICHIER VERIFICATION

Si l'utilisateur sélectionne [ENT~] → [4. System] → [6. Database] → [3. Clear Log Data] dans l'écran initial, l'écran suivant apparaît :



Appuyez sur [1.Yes] pour effacer tous les fichiers de vérification sauvegardés dans le terminal. Appuyez sur [2.No] et sur [ENT] pour annuler.

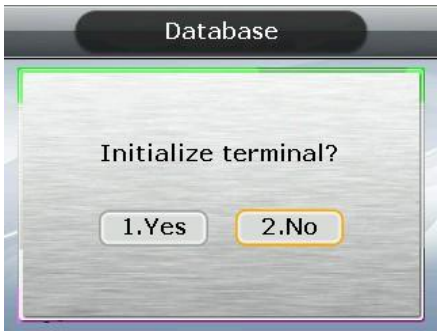
Si rien n'est entré pendant un certain temps dans cet écran, le système reviendra à l'écran initial sans rien avoir effacé.

Ceci supprime tous les fichiers logs de vérification et les logs effacés ne peuvent plus être restaurés après la suppression.

Si la suppression est réussie, l'appareil revient au menu parent et un ronfleur émet une tonalité de succès.

5.6.6.4 REINITIALISER TERMINAL

Si l'utilisateur sélectionne [ENT~] → [4. System] → [6. Database] → [4. Initialize Terminal] dans l'écran initial, l'écran suivant apparait :



Appuyez sur [1.Yes] pour réinitialiser le terminal (rétablir valeurs d'usine). Appuyez sur [2.No] et sur [ENT] pour annuler.

Si rien n'est entré pendant un certain temps dans cet écran, le système reviendra à l'écran initial au lieu de réinitialiser.

Ceci efface toutes les configurations, utilisateurs et journal d'informations excepté l'adresse MAC (physique) stockée dans le terminal, ce qui permet de rétablir le terminal dans ses valeurs d'usine. Attention car le rétablissement des données est impossible après que les paramètres d'usine aient été restaurés. Si le retour aux paramètres d'usine est réussi, l'appareil retourne au menu parent et un ronfleur émet une tonalité de succès.

5.7 TERMINAL

Lorsqu'on sélectionne '5. Terminal' dans le menu principal, l'écran suivant apparait:

Appuyez sur la touche associée à l'élément que vous souhaitez adapter.

5.7.1 OPTIONS TERMINAL

Si l'utilisateur sélectionne [ENT~] → [5. Terminal] → [1. Terminal Option] dans l'écran initial, l'écran suivant apparait :

▸ Paramètre par défaut: Identique à l'écran à ci-contre

▸ Dooropen

La porte s'ouvre si la touche '0' est pressée. Ceci apparaît uniquement si le terminal est verrouillé. Cette option n'est normalement pas affichée.

▸ Tamper Alarm

Si coché (☑), un avertissement sonore sera généré lorsque le terminal est ouvert.

▸ Lock Terminal

Cette fonctionnalité permet à l'administrateur de définir le blocage direct du terminal via le terminal même et non via le programme serveur. Si coché (☑), le terminal est bloqué et donc personne n'a accès jusqu'à ce que l'administrateur libère le terminal.

▸ KeyLed ON

Si coché (☑), la touche LED est toujours allumée de sorte que les touches tactiles soient visibles.

▸ Dooropen

C'est le menu qui indique que l'administrateur a l'autorisation d'ouvrir temporairement la porte si le terminal est défini comme verrouillé dans le serveur.

L'utilisateur peut quitter le menu parent et sauvegarder les valeurs adaptées en appuyant sur [ENT~]. Il peut aussi appuyer sur [F4 (←)] pour annuler la configuration.

5.7.2 CONTROLE DE VOLUME

Si l'utilisateur sélectionne [ENT~] → [5. Terminal] → [2. Volume Control] dans l'écran initial, l'écran suivant apparait :

▸ Paramètre par défaut: Identique à l'écran à ci-contre

Réglez le volume vocal et le volume du ronfleur.
Si la valeur est sur '0', aucune voix ni tonalité ronfleur ne sera générée.

L'utilisateur peut quitter le menu parent et sauvegarder les valeurs adaptées en appuyant sur [ENT~]. Il peut aussi appuyer sur [F4 (←)] pour annuler la configuration.

5.7.3 PORTE

Si l'utilisateur sélectionne [ENT~] → [5. Terminal] → [3. Door] dans l'écran initial, l'écran suivant apparait :

▸ Paramètre par défaut: Identique à l'écran à ci-contre

▸ Lock Type

Choisissez '1' si vous optez pour le type serrure de porte ou lorsqu'une porte automatique est connectée au terminal. Sélectionnez '2' si une serrure motorisée est reliée au terminal. Définissez '3' en cas de connexion du voyant d'avertissement au port verrou pour afficher la réussite ou l'échec de l'authentification. Dans le cas où rien n'est branché choisissez également '1'.

▸Door Monitor

Cette fonction est utilisée pour contrôler l'état de la porte.

- ‘3.Désactiver’ – L’état de la porte n’est pas contrôlé
- ‘1.Normalement Ouvert’: Dans le cas d’un type verrouillage pour porte automatique
  (Quand l’état de la serrure est ouvert lorsque la porte est fermée)
- ‘2.Normalement fermé’: Dans le cas d’un type serrure
  (Quand l’état de la serrure est ferme lorsque la porte est fermée)

▸Open Duration (x 0.1 sec)

Ceci indique le temps que la porte est ouverte et fermée si l'authentification est réussie. Un facteur de multiplication de 0,1 étant d’application, vous devez compléter une valeur de 30 pour obtenir un temps de 3 secondes. Le type Serrure se réfère au temps que la porte est ouverte et à nouveau fermée lorsque l'authentification est terminée.

▸ Warn Door Open (x 1 Sec)

C’est cette fonction qui contrôle le terminal pour vérifier le temps d’ouverture de la porte et générer une tonalité d'avertissement si le délai spécifié est dépassé (min 5 s ~ max 30 sec). Si la valeur est définie sur ‘00’, aucune tonalité d'avertissement ne sera émise. Même si vous donnez une valeur de 01 ~ 04, la tonalité ne sera générée qu’après un délai de 5 secondes.

La tonalité d'avertissement est aussi générée dans le cas où la porte n'a pas été fermée dans le délai prédéfini bien qu’elle devrait être fermée. Ceci permet d’entreprendre des mesures appropriées pour fermer la porte en informant sur le fait que la porte n'est pas fermée.

Pour utiliser cette fonction, le contrôle de l’état de la serrure doit être activé et le penne ou verrou à contrôler doit certainement être relié au terminal. En outre, ces paramètres sont activés uniquement si le Contrôle de porte mentionné précédemment est défini sur '4. Normalement ouvert’ ou ‘5. Normalement fermé’.

L'utilisateur peut quitter le menu parent et sauvegarder les valeurs adaptées en appuyant sur [ENT~]. Il peut aussi appuyer sur [F4 (←)] pour annuler la configuration.

5.7.4 WIEGAND

Si l’utilisateur sélectionne [ENT~] → [5. Terminal] → [4. Wiegand] dans l’écran initial, l’écran suivant apparait :

▸ Paramètre par défaut: Identique à l’écran à ci-contre

C’est le menu qui définit la sortie Wiegand.

Ceci est uniquement valable si un contrôleur séparé fonctionnant avec une entrée Wiegand est utilisé. Après une authentification réussie, les données sont envoyées vers les terminaux de port Wiegand sous la forme suivante ;

2.None	C’est le fonctionnement normal; la sortie Wiegand n’est pas utilisée dans ce cas.
3.26bit	Cela transmet “Facilitycode[1byte] + ID Utilisateur[2byte]”, si l’ID utilisateur est défini sur 4 chiffres ou moins. Exemple : Dans le cas de FacilityCode : 045 (2Dh), GID : 6543 (198Fh), cela sera envoyé comme 1 10001111 0 00101101 0001 1001 »
4.34bit	Cela transmet “Facilitycode[1byte] + ID Utilisateur[3byte]” si l’ID utilisateur est défini sur 7 chiffres ou moins. Dans le cas d’un ID utilisateur de 8 chiffres, “ID Utilisateur[4byte]” est envoyé sans Facility code. Exemple : Dans le cas de FacilityCode : 001(1h), GID : 123456 (1E240h), cela sera

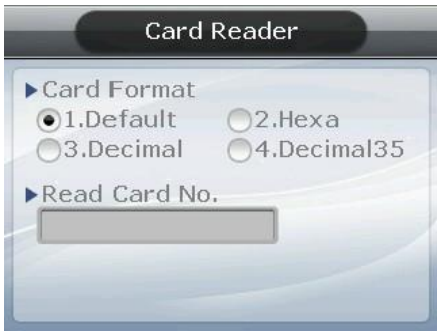
	envoyé comme 00000001 00000001 0 0 ' 01000000 11100010
5.Custom	Ceci peut être défini dans le serveur comme les paramètres sous la définition d'utilisateur. Le type de paramètres peut seulement être demandé au terminal.

Attention : si Bypass est coché, indépendamment des paramètres de sortie Wiegand, les données obtenues via l'entrée Wiegand au moment de l'authentification réussie sont envoyées telles quelles vers la sortie Wiegand.

L'utilisateur peut quitter le menu parent et sauvegarder les valeurs adaptées en appuyant sur [ENT~]. Il peut aussi appuyer sur [F4 (←)] pour annuler la configuration.

5.7.5 LECTEUR DE CARTE

Si l'utilisateur sélectionne [ENT~] → [5. Terminal] → [5. Card Reader] dans l'écran initial, l'écran suivant apparait :



- Paramètre par défaut: Identique à l'écran à ci-contre
- Lire Carte N°.

  Si l'utilisateur présente la Carte dans cet écran, le numéro de la carte s'affiche à l'écran LCD

- Card Format

C'est le menu dans lequel vous définissez la manière dont le numéro de carte doit être affiché. Comme illustré ci-dessous, vous voyez que le numéro de carte affiché varie selon la configuration. Par conséquent, si le format doit être modifié après l'installation initiale, la carte doit à nouveau être enregistrée.

Carte RF exemple Numéro de carte (5byte): 08h 01h 16h 1Dh D6h

Format carte	Numéro de carte	Mode d'expression
1. Default	02207638	Nombre décimal (3+5) chiffres [022(16h)+07638(1DD6h)]
2. Hexa	0801161DD6	Nombre hexadécimal 10 chiffres
3. Decimal	0018226646	Les derniers 4byte qui doivent être exprimés en un nombre décimal de 10 chiffres (01161DD6h)
4. Decimal 35	02207638	Même que '1. Default'

Carte SC exemple Numéro de carte (4byte): 52h 9Dh 06h E3h

Format carte	Numéro de carte	Mode d'expression
1. Default	529D06E3	Exprimé dans un nombre hexadécimal de 8 chiffres
2. Hexa	E3069D52	Exprimé dans un nombre hexadécimal de 8 chiffres avec modification de l'ordre des bytes
3. Decimal	1386022627	Nombre hexadécimal 529D06E3 exprimé en un nombre décimal de 10 chiffres
4. Decimal 35	3808861522	Nombre hexadécimal E3069D52 exprimé en un nombre décimal de 10 chiffres

L'utilisateur peut quitter le menu parent et sauvegarder les valeurs adaptées en appuyant sur [ENT~]. Il peut aussi appuyer sur [F4 (←)] pour annuler la configuration.

5.7.6 DISPOSITIF EXTERNE

Si l'utilisateur sélectionne [ENT~] ([5. Terminal] [6. External Device]) dans l'écran initial, l'écran suivant apparait :

▸ Paramètre par défaut: Identique à l'écran à ci-contre

▸Printer

Si cochée (☑), le résultat de l'authentification est imprimé. Si défini sur '1', lorsque l'authentification réussite, l'ID du terminal, l'ID utilisateur, le temps de vérification, le mode d'authentification, etc... seront imprimés via l'imprimante connectée au port RS232 (debug) du terminal. Le type d'impression peut varier selon la configuration. Si défini sur 'Format 2', le nom du terminal est imprimé comme sujet principal. L'imprimante utilisée est de type sériel ''SRP-350''.

▸ Lock Controller

Définissez cette fonction si un utilisateur connecte un appareil distinct à la place du port serrure terminal pour contrôler la porte. Dans le cas où l'utilisateur connecte directement une serrure sur le terminal, cette fonction doit être configurée sur ''4. None''. Si vous connectez un LC010, cette fonction doit être définie sur ''5. LC010''.

L'utilisateur peut quitter le menu parent et sauvegarder les valeurs adaptées en appuyant sur [ENT~]. Il peut aussi appuyer sur [F4 (←)] pour annuler la configuration.

5.8 INFORMATION

Sélectionnez '6. Information' dans l'écran initial, l'écran suivant apparait :

Menu pour demander les paramètres du Terminal.

Appuyez sur :

Touche [1] pour demander un certain nombre de configurations optionnelles du terminal,

Touche [2] pour demander la configuration réseau telle que l'adresse IP,

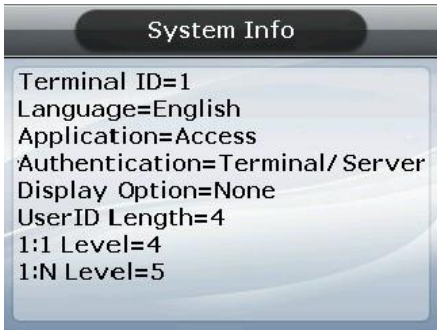
Touche [3] pour demander le statut d'enregistrement de l'utilisateur,

Touche [4] pour demander le journal data,

Touche [5] pour demander la version firmware.

5.8.1 INFO SYSTEME

Sélectionnez [ENT~] → [6. Information] → [1. Info System] dans l'écran initial, l'écran suivant apparait :



Appuyez sur [F4(←)] pour retourner au menu supérieur.

5.8.2 INFO RESEAU

Sélectionnez [ENT~] → [6. Information] → [2. Network Info] dans l'écran initial, l'écran suivant apparait :

Appuyez sur [F4(←)] pour retourner au menu supérieur.

5.8.3 INFO DATABASE

Sélectionnez [ENT~] → [6. Information] → [3. Database Info] dans l'écran initial, l'écran suivant apparait :

-Registered User: Nombre d'utilisateurs enregistrés (incluant Administrator)

-Registered Admin: Nombre d'administrateurs enregistrés.

-Max User: Nombre maximum d'utilisateurs pouvant être enregistrés.

-Registered FP: Nombre d'empreintes digitales entières enregistrées.

-Max FP: Nombre maximal d'empreintes digitales qui peuvent être enregistrées.

Appuyez sur [F4(←)] pour retourner au menu supérieur.

5.8.4 VISUALISER JOURNAL

Sélectionnez [ENT~] → [6. Information] → [4. View Log] dans l'écran initial, l'écran suivant apparait :

-All Log: Nombre de journaux stockés dans le terminal

-Max Log: Nombre maximal de journaux qui peuvent être enregistrés

Appuyez sur [F4(←)] pour retourner au menu supérieur.

5.8.5 INFO VERSION

Sélectionnez [ENT~] → [6. Information] → [5. Version Info] dans l'écran initial, l'écran suivant apparait :

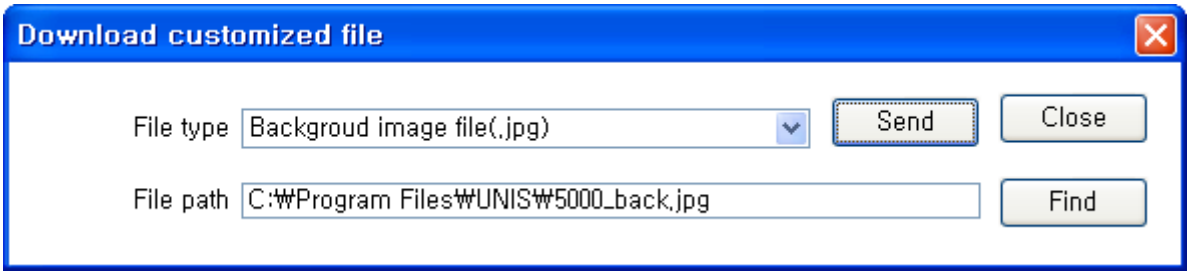
Appuyez sur [F4(←)] pour retourner au menu supérieur.

5.9 TELECHARGER FICHIERS UTILISATEUR

Cette fonctionnalité permet à l'utilisateur de modifier les images d'arrière-plan et des messages vocaux si nécessaire. Le fichier de des utilisateurs peut être téléchargé à partir du programme UNIS.

5.9.1 MODIFIER IMAGE D'ARRIERE PLAN

En sélectionnant 'Download customized file' dans le programme UNIS, l'écran suivant apparaît :



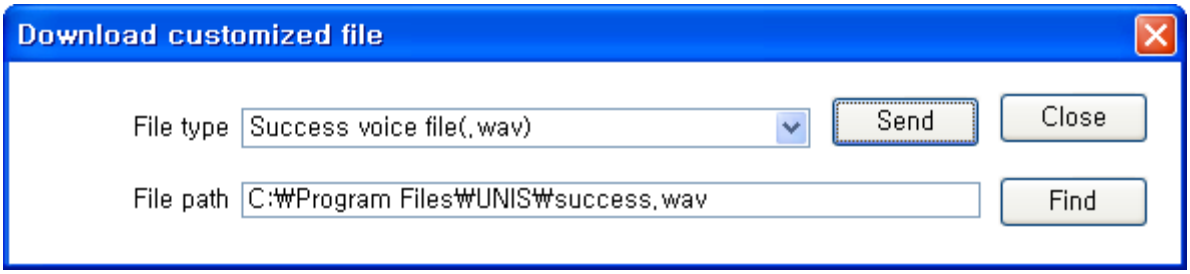
Désignez le type de fichier comme 'Background image file (.jpg)', sélectionnez le fichier image (.jpg) et cliquez sur le bouton 'Send', l'écran de sélection du terminal apparaîtra. Sélectionnez le terminal dans la liste terminal et cliquez sur le bouton 'Send' à nouveau, le fichier sera envoyé et le résultat téléchargé est affiché.

Dans ce cas, le nom du fichier peut être de maximum 15 caractères y compris le nom de l'extension avec le fichier jpg uniquement de grandeur 320*240. Si des données sont téléchargées dans un format différent, le résultat téléchargé affichera une erreur de version.

Pour modifier l'image d'arrière-plan, l'utilisateur peut la sélectionner directement dans le menu '5.5.5 Ecran'.

5.9.2 MODIFIER MESSAGE VOCAL

En sélectionnant 'Download customized file' dans le programme UNIS, l'écran suivant apparaît :



Désignez le type de fichier comme 'Success voice file (.wav)', sélectionnez le fichier Wav (.wav) et cliquez sur le bouton 'Send', l'écran de sélection du terminal apparaîtra. Sélectionnez le terminal dans la liste terminal et cliquez sur le bouton 'Send' à nouveau, le fichier sera envoyé et le résultat téléchargé est affiché.

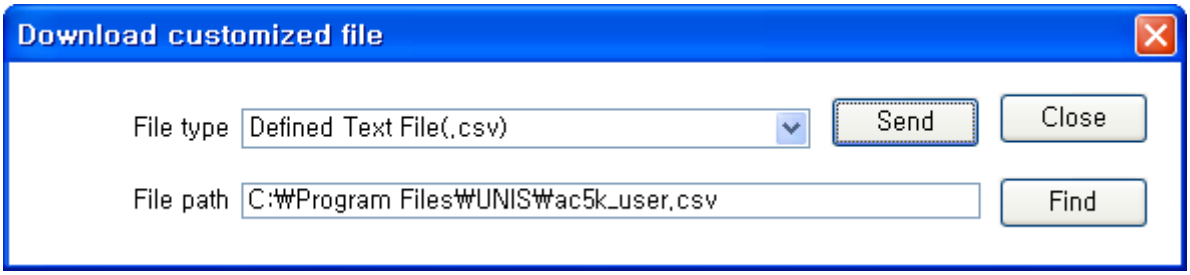
Dans ce cas, le nom du fichier peut être de maximum 15 caractères y compris le nom de l'extension avec le fichier Wav en 8KHz, 16bit, en format mono uniquement. Si des données sont téléchargées dans un format différent, le résultat téléchargé affichera une erreur de version.

Dans le cas d'un échec de la voix, sélectionnez le fichier type 'Fail voice file (.wav)' et remplacer le de la même façon.

Pour utiliser la voix définie par l'utilisateur comme la voix par défaut, cochez la case 'User Voice' dans le menu '5.5.5 Ecran'.

5.9.3 MODIFIER TEXTE UTILISATEUR

En sélectionnant ‘Defined Text File’ dans le programme UNIS, l’écran suivant apparaît :



Désignez le type de fichier comme ‘Defined Text File (.csv)’, sélectionnez le fichier CSV (.csv) et cliquez sur le bouton ‘Send’, l'écran de sélection du terminal apparaîtra. Sélectionnez le terminal dans la liste terminal et cliquez sur le bouton ‘Send’ à nouveau, le fichier sera envoyé et le résultat téléchargé est affiché.

Le fichier CSV peut être créé et stocké sous la forme d’un type csv après modification du texte désiré dans le fichier Excel (.xls) file fourni avec le Firmware du terminal.

Pour utiliser les textes définis par l’utilisateur comme texte standard, cochez la case ‘User Text’ dans le menu ‘5.5.5 Ecran’.

6 COMMENT UTILISER LE TERMINAL

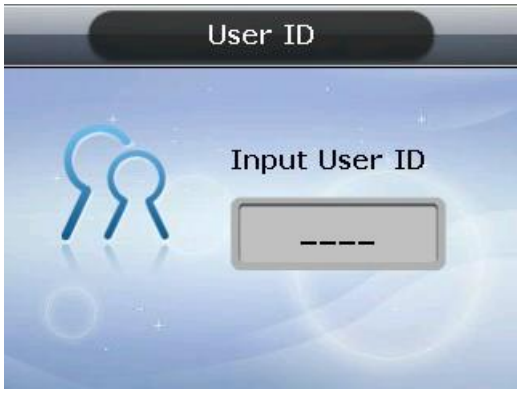
6.1 CHANGER LE MODE D'AUTHENTIFICATION

<Figure 4-1>

Les touches ne sont normalement pas visibles; mais si l'utilisateur approche la main de l'endroit où vous devez présenter la carte comme illustré sur la figure gauche, les LEDs s'allument et le clavier apparaît comme illustré dans la figure de droite. Lorsque les touches sont visibles, appuyez sur la touche de fonction appropriée pour changer le mode d'authentification tel que par exemple Arriver Bureau [F1], Quitter Bureau [F2], Sortir [F3], Revenir [F4], Accès [ENT], etc…

6.2 INTRODUIRE ID

Normalement, ceci n'est pas visible ; mais comme le montre la Figure <4-1>, si l'utilisateur touche de la main l'endroit où la carte doit être présentée, les LEDs s'activent et le clavier est visible. Dans ce cas l'écran d'introduction ID apparaitra si l'utilisateur saisit un chiffre.



Effacez avec la touche [F4 (←)] si un chiffre de l'ID a été mal introduit lors de ce processus. Si [ENT] est pressé après avoir saisi l'ID, l'écran d'introduction des empreintes digitales ou de saisie du mot de passe apparaît selon la méthode d'authentification de l'utilisateur.

Attention, l'authentification échoue si un utilisateur de carte saisit d'abord un ID. Par conséquent, assurez-vous que seule la carte soit utilisée.

6.3 AUTHENTIFICATION

6.3.1 AUTHENTIFICATION D'EMPREINTE DIGITALE

Lorsque le doigt est positionné sur le capteur d'empreintes digitales, le ronfleur s'active avec la lampe du senseur l'empreinte digitale est dûment saisie. Veillez à ne pas enlever le doigt du capteur jusqu'à ce que la lampe du senseur s'éteigne et le ronfleur s'arrête.

Dans le cas de l'authentification 1:1, le fait d'introduire l'ID et d'appuyer sur [ENT] provoque le clignotement du senseur. Placez alors le doigt sur le capteur d'empreintes digitales.

6.3.2 AUTHENTIFICATION CARTE

Approchez la carte de la figure 'Carte' comme montré en <Figure 4-1>.

6.3.3 AUTHENTIFICATION MOT DE PASSE

Appuyez sur [ENT] après avoir introduit l'ID, l'écran pour la saisie du mot de passe apparait. Si un chiffre erroné est introduit, appuyez sur [F4(←)] pour effacer. Introduisez le mot de passe et pressez [ENT].