iGuard™ LM Séries

Manuel Opérateur

Version 3.6.

Commission de Communications Fédérale (FCC) Déclaration

Cet Équipement a été conçu et testé en observant les limites pour un dispositif digital de Classe A, conformément à la Partie 15 des règles de FCC. Ces limites sont conçues pour fournir une protection raisonnable contre les interférences nuisibles dans une installation résidentielle. Cet équipement produit, utilise et peut émettre l'énergie de fréquence radio et, si il n'est pas installé et employé conformément aux instructions, peut causer des interférences nuisibles aux communications radio. Cependant, il n'y a aucune garantie que l'interférence n'arrivera pas dans une installation particulière. Si cet équipement cause des interférences nuisibles à la radio ou la réception de télévision, qui peut être déterminée en arrêtant l'alimentation électrique de l'équipement , l'utilisateur est encouragé à essayer de corriger l'interférence par une ou plus des mesures suivantes :

- Réorienter ou Déplacer l'antenne de réception
- Augmentez la séparation entre l'équipement et le récepteur.
- Connecter l'équipement sur un circuit électrique différent de celui auquel le récepteur est connecté.
- Consulter le vendeur ou un technicien radio /TV expérimenté pour obtenir de l'aide

CE

EMC DIRECTIVE 89/336/EEC (EN55022 / EN55024)

Nom Commercial: iGuard
No Modèle FPS110 / LM

Table des Matières

1.INSTALLATION

1.1. Installation

Avant l'installation de votre iGuard, il est important de vérifier quelques critères pour une installation sûre et facile. Pour cela, lisez s'il vous plaît les notes de pré installation inscrites ci-dessous quant aux précautions à prendre avant l'implantation d'iGuard.

1.1.1. Notes de Pré Installation

- Le terminal iGuard est conçu pour une installation à l'intérieur. Si vous voulez l'installer à l'extérieur, vous devez pour cela prendre garde à son exposition à l'eau ou à des conditions dures
- A l'installation vous devez connecter le panneau de métal arrière d'iGuard à la terre pour empêcher des impulsions électriques et des chocs pouvant affecter des utilisateurs ou les autres terminaux iGuard.
- Pour empêcher les problèmes électriques ou court-circuit, ne pas partager l'alimentation d'énergie de l'iGuard avec un autre dispositif, par exemple la serrure électrique.
- Pour assurer la sécurité, en cas de coupure de courant ou d'autres cas d'urgence. Ne reliez pas le bouton de porte au terminal iGuard. Reliez-le directement à la gâche de porte.
- Pour intensifier le niveau de sécurité des locaux, installez le relais externe ensemble avec l'iGuard. Cela augmentera la sécurité puisque le relais externe est placé dans des locaux de bureau et non à l'extérieur, comme est l'iGuard.
- Ne pas installer le lecteur à proximité d'une source de chaleur ni l'exposer à la lumière directe du soleil.
- Si le modèle de lecteur de carte à puce est employé, assurez-vous s'il vous plaît que le Code de Société soit mis. Voir la Configuration.

1.1.2. Installation

Déterminez l'emplacement pour l'installation iGuard, le relais externe, la serrure de porte et la ligne d'alimentation d'énergie. Fixez le panneau arrière de métal à l'emplacement où le terminal sera installé. Reliez le terminal avec l'alimentation d'énergie fournie par l'utilisateur.

Connexions Terminal iGuard

- Borne #1 – Terre
- Borne #2 - + 12V
- Bornes #3/4 - Normalement Ouvert
- Bornes #4/5 – Normalement Fermé

- Bornes #6/7 - Détecteur de Porte (option)
- Bornes #8/9 – Réservé
- Bornes #10/11 - Alarme Extérieure (option)
- Prise - Commutateur de Relais Externe (option)

IGuard peut être connecté directement à votre réseau d'entreprise via la norme RJ-45 des protocoles de TCP/IP et le CÂBLE. Assurez-vous que votre ordinateur a été installé et configuré avec les protocoles TCP/Installation

Installation peut aussi être connecté directement à la carte réseau du PC par un câble croisé RJ-45

Paramètres Réseau et Adresse TCP/IP

- Sur l'iGuard, presser **FUNC**, entrer le mot de passe (par défaut "123"), presser **FUNC**, presser **5**.
- Entrer Date + **Inst**allation
- Entrer Heure + **Inst**allation
- Entrer le nom du dispositif + **FUNC** pour continuer.
- Entrer l'adresse IP (selon votre réseau d'entreprise, par exemple 192.168.0.101) + **FUNC** pour continuer.
- Entrer le masque de Sous Réseau (selon votre réseau d'entreprise, par exemple. 255.255.255.0) + **FUNC** pour continuer.
- Entrer la Passerelle par défaut + **FUNC** pour continuer.
- Entrer DNS (option) + **FUNC** pour continuer.
- Sélectionner le Mode Maître/Esclave (1 pour **Maître** or 2 pour **Esclave**).
- Presser **1** pour accepter ces valeurs ou **2** pour annuler.

Pour tester si l'iGuard fonctionne dans le réseau, essayer le dispositif PING de votre PC.
Sur votre PC, allez sur Commande du menu Démarrer.

- Tapez 'ipconfig " pour contrôler l'adresse IP de votre PC et être sur qu'il est dans le même réseau qu'iGuard.
- Tapez l'adresse IP par défaut d' iGuard: 192.168.0.100.
- Si le Installation répond comme suit, Installation est correcte et vous êtes prêts à passer :

```
C:\> ping 192.168.0.100

    > Installation 192.168.0.100 with 32 bytes of data:
    > Reply from 192.168.0.100: bytes=32 time<10ms TTL=128
    > Reply from 192.168.0.100: bytes=32 time<10ms TTL=128
    > Reply from 192.168.0.100: bytes=32 time<10ms TTL=128

    > Installation statistics for 192.168.0.100:
    > Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    > Approximate round trip times in milli-seconds:
    > Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ouvrez le navigateur Internet de votre PC, Internet Explorer ou le Navigateur Netscape et tapez http://192.168.0.100 (l'Adresse IP de votre iGuard) et vous serez en mesure de voir l'interface d'iGuard dans la fenêtre du navigateur.

1.2. Alimentation Electrique

IGuard exige une alimentation d'énergie commutée DC 12V / 500mA. On recommande de ne pas partager cette alimentation d'énergie entre l' IGuard et la gâche de porte frappe à cause des problèmes potentiels en arrière.
** Avertissement : n'employez pas s'il vous plaît d'autres systèmes d'alimentation électrique, cela peut mener au non fonctionnement du système et à des opérations incertaines.

1.3. Ou l'installer ?

IGuard est une unité murale avec un faible encombrement et peut être commodément installé n'importe où. Cependant, on recommande que l'iGuard soit installé si possible près de la porte, pour que l'utilisateur puisse ouvrir la porte dans la période de temps mort, par défaut 5 secondes. Notez aussi les points suivants:

- Prévoir une circulation d'air afin d'éviter une trop forte chaleur interne
- Ne pas installer le lecteur à proximité d'une source de chaleur ni l'exposer à la lumière directe du soleil.

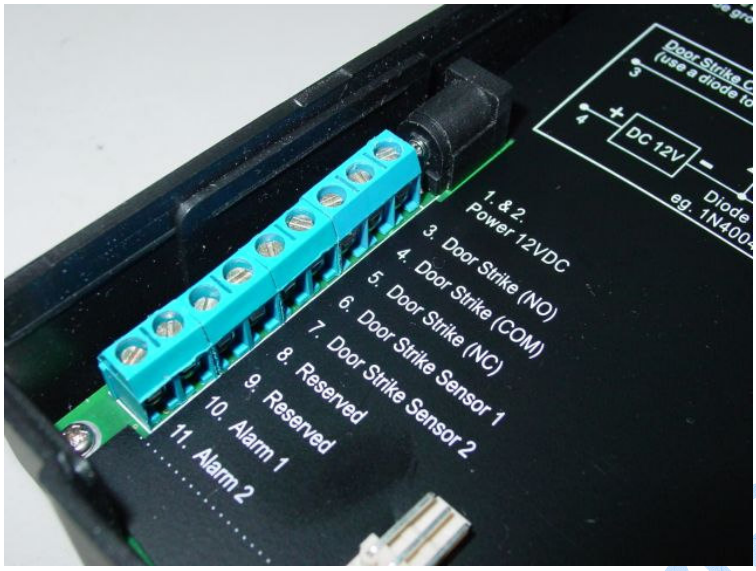
1.4. **Important** Montage du Panneau arrière métallique

IGuard est livré avec un panneau de montage mural métallique. ***Ce panneau doit être relié à la Terre***. En procédant ainsi, l'électricité statique que les utilisateurs émettent peut être déchargée facilement par la terre, ce qui améliore les images d'empreinte digitale d'utilisateurs.

1.5. Connexions - Alimentation & contrôles externes

IGuard fournit des bornes d'accès libre pour des connexions aux commandes externes, incluant : la gâche de porte, le détecteur de porte, l'état de la porte, les contacts NO, NF et l'alarme externe

.



Alimentation (12V DC):
Bornes #1 (terre) & #2 (+12V). L'alimentation requise, est 12V DC, 150mA (inoccupé), 500mA (sommet).

Gâche de Porte (Bornes 3 - 5):
(3 - 4 Normalement Ouvert, 4 - 5 Normalement Fermé). Ces bornes sont connectées directement au relais interne, évalué à 12V / 1A. Si la gâche de porte est sans limite de courant, elle peut être directement connectée à ces bornes. Si le système est employé seulement pour la gestion de Temps de présence, ces bornes peuvent être laissés débranchées.

Détecteur de Porte (option):
Bornes #6 & #7. Elles fournissent à iGuard, le statut actuel de la porte (ouverte / fermée). Si la porte est laissée ouverte plus de 10 secondes, iGuard produira une alarme sonore.

Alarme Externe (option):
Bornes #10 & #11. Elles sont utilisées pour une alarme externe (option). Si le dispositif est forcé pendant l'opération (comme un cambriolage), un détecteur interne déclenchera cette connexion et cela déclenchera l'alarme externe.

Relais Externe (option):
Connecter du bon coté. Pour utiliser un relais externe, Vous devez connecter le deux connecteurs au bornier d'iGuard et le connecter ensuite en arrière au relais externe. Cela contrôle la gâche de porte de l'intérieur les locaux, intensifiant la sécurité et empêchant des cambriolages.

1.6. Connexions – Réseau d'Entreprise

Vous pouvez connecter iGuard directement à votre réseau d'ordinateur d'entreprise via la norme RJ-45 des protocoles de TCP/IP et le CÂBLE {TRANSMISSION PAR CÂBLE}. En le connectant au réseau, vous pouvez gérer et contrôler l'unité via n'importe quel navigateur Internet standard, comme le navigateur Netscape de Microsoft et Internet Explorer.

La connexion est très directe comme indiqué dans l'image suivante:

Alimentation

Après le branchement, iGuard effectuera un test, ensuite, il se mettra en mode stand-by comme montré ci-dessous.

Description	***LCD Display***
Alimentation- Quand iGuard est alimenté, il effectuera un test interne	`Initialisation...`
Après environ 10 sec, l'unité chargera le programme système …	`IGuard Système chargement...`
Après le chargement du programme, iGuard se mettra en mode stand-by et sera prêt à être utilisé.	`Lundi 30 13:49 ID#:`

2. CONFIGURATION

2.1. Configurer la date et l'heure

Vous devez entrer à la date et l'heure pour qu'iGuard puisse enregistrer tous les accès et les rapports de service de temps de présence. Suivez ces étapes pour configurer la date de système et l'heure: -

Description	***Affichage Ecran***
En Mode Stand-by, presser la touche **FUNC** pour entrer dans le Menu Installation. Vous serez invités à entrer le Mot de passe d'Administrateur comme indiqué.	**Entrer Mot de Passe: _**
Entrer le Mot de Passe Administrateur (par défaut: 123).	**Entrer mot de passe: 123_**
Presser la touche **Func** pour continuer. Le Menu Installation se déroulera doucement comme montré.	**Presser 1: Ajout/Mise à jour ID** **:** **Presser 5: Configuration Système …**
Entrer **5** pour sélectionner le menu **Configuration Système**. La date courante est affichée. Si nécessaire, entrer la nouvelle date et ensuite presser la touche **Func** pour continuer.	**Date (J/M/A): 30/08/1999**
Après avoir pressé la touche **Func**, l'heure courante est affichée. Entrer la nouvelle heure, et presser la touche **Func** pour continuer.	**Heure (H:M:S): 13:45:23**
Le système demandera alors l'ID du Terminal. L'ID Terminal est utilisée pour identifier IGuard sur votre réseau, spécialement si vous avez plus d'un IGuard installé *(suite dans la prochaine section)*.	**Terminal ID:**

Note:
IGuard peut conserver la date et l'heure courante sans alimentation pour approximativement deux jours. Il y a un logiciel utilisateur pour synchroniser l'horloge du dispositif iGuard avec le PC de bureau (iSetClock.exe), qui peut être téléchargé librement au site Web.

2.2. Installation Réseau & adresse TCP/IP

Vous pouvez connecter iGuard directement au réseau de l'entreprise. Pour cela, vous devrez donner un Nom et une Adresse IP au produit. Il est possible d'utiliser le serveur DHCP de votre réseau pour assigner une adresse IP Dynamique, mais il est suggérer d'assigner une Adresse IP Statique au produit pour éviter les problèmes.

Les procédures suivantes montrent, comment assigner le nom, l'adresse IP, et d'autres paramètres liés. Rassemblez toute l'information avant d'agir.

Description	***Affichage Ecran***
En Mode Stand-by, presser la touche **Func** pour entrer dans le menu Installation. Vous serez invite à entrer le Mot de Passe Administrateur (par défaut: 123).	**Entrer Mot de Passe: _**
Entrer **5** pour sélectionner le menu **Configuration Système**.	**Presser 1: Ajout/Mise à jour ID** **:** **Presser 5: Configuration Système …**
Presser la touche **Func** avant que vous ne voyiez "DHCP/Statique IP"	
Presser la touche **Func** pour continuer, et presser **1** pour sélectionner DHCP ou **2** pour IP Statique.	**DHCP/Statique IP (1/2)? Statique**
Presser la touche **Func** pour continuer. Il vous sera demandé d'entrer l'adresse IP de l'unité. Par défaut: 192.168.0.100. Entrer l'adresse IP statique assignée à l'unité (e.x, 192.168.1.123).**Note: Configurez s'il vous plaît Installation selon votre réseau d'entreprise**	**Adresse IP: 192.168.001.123**
Presser la touche **Func** pour continuer. Entrer ici le Masque de Sous Réseau (ex., 255.255.255.0).	**Masque sous réseau: 255.255.255.000**
Presser la touche **Func** pour continuer. Entrer l'adresse de Passerelle par défaut (ex., 192.168.0.200).	**Passerelle: 192.168.000.200**

Presser la touche **Func** pour continuer. Entrer l'adresse DNS (e.x. 192.168.0.200). Assurez-vous que l'adresse IP de toutes les unités est unique. **(Attention: Des adresses IP identiques causeraient des erreurs de réseau et l'iGuard ne fonctionnerait pas).**	**DNS:** **192.168.000.200**
Presser la touche **Func** pour continuer. On vous demandera si le dispositif est un Maître ou un Esclave (1/2) ? Si vous avez seulement une unité iGuard, choisissez (1) Maître. Si vous avez plusieurs unités d'iGuard, vous devez décider qui est le Maître et qui est l'Esclave (s). Si vous choisissez (2) Esclave, le système vous demandera de fournir l'Adresse IP du Maître, par défaut : 192.168.0.100. S'il vous plaît lisez aussi la section du Mode Esclave et mode Maître.	**Maître/Esclave** **(1/2)? Maître**
IGuard FPS110 peut être configuré comme un Dispositif Esclave ou Maître. Choisissez un et presser ensuite la touche **Func**. Le système se remettra à zéro et retournera ensuite au Mode Stand-by.	**Lun 30 Août** **13:46 ID #:_**

2.3. Le Code Société

Le Code de Société est présenté pour les unités ayant l'option de Carte à puce. Le Code de Société est employé pour s'assurer que l'unité lit seulement les cartes à puce publiées par la société. Par exemple, si le Code de Société de l'unité est 1234, il lit seulement les cartes à puce avec le même Code de Société et ignorera les cartes avec un code de société différent.

Toutes les unités d'une même société doivent avoir le même code et ce code de société doit être tenu confidentiel. Le code de société est inséré dans la page Web « Administration : Installation Terminal » via le navigateur Internet.

Notez s'il vous plaît que dans la configuration Maître / Esclave, toutes les unités Esclave doit avoir le même code société que l'unité Maître.

2.4. Configuration du Mot de passe d'Administrateur et Mot de passe d'Accès

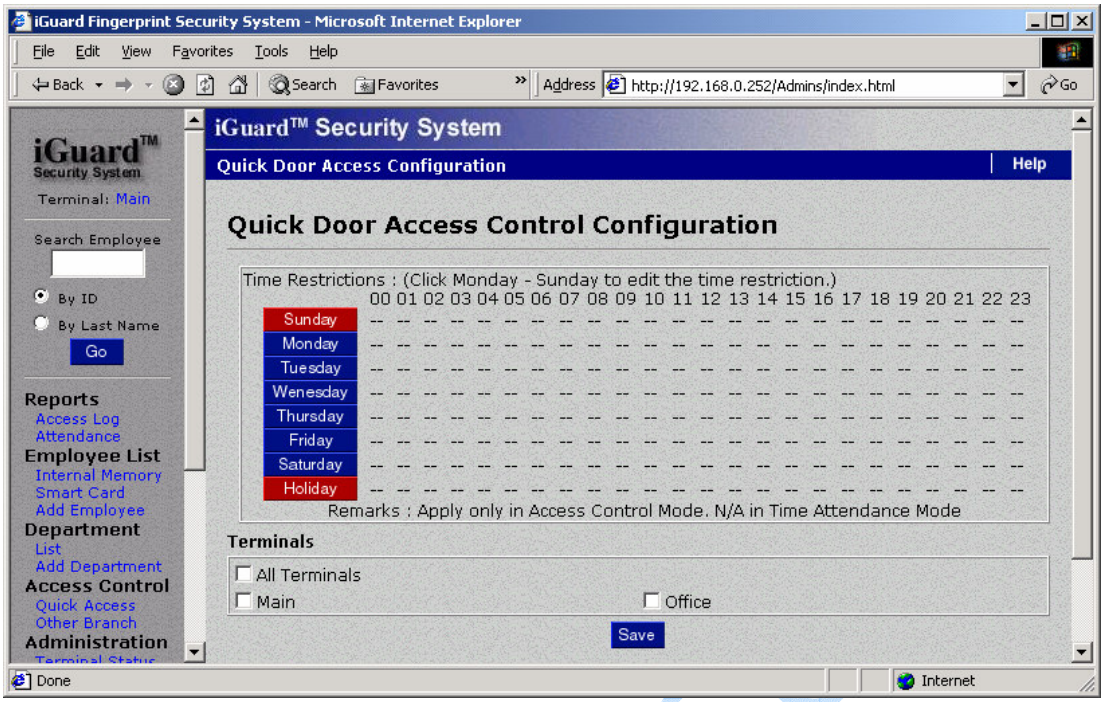
iGuard à trois mots de passe "globaux" le Mot de passe d'Administrateur de Système est employé pour avoir accès au menu du système et configurer le système (comme l'accès au menu d'installation dans le dernier exemple). Le Mot de passe d'Administrateur d'Utilisateur est employé pour gérer les comptes d'utilisateur. Le Mot de passe d'Accès de Porte est employé pour actionner la gâche de porte dans l'option d'Accès Rapide.

Suivez les étapes pour assigner et éditer ces 3 mots de passe :

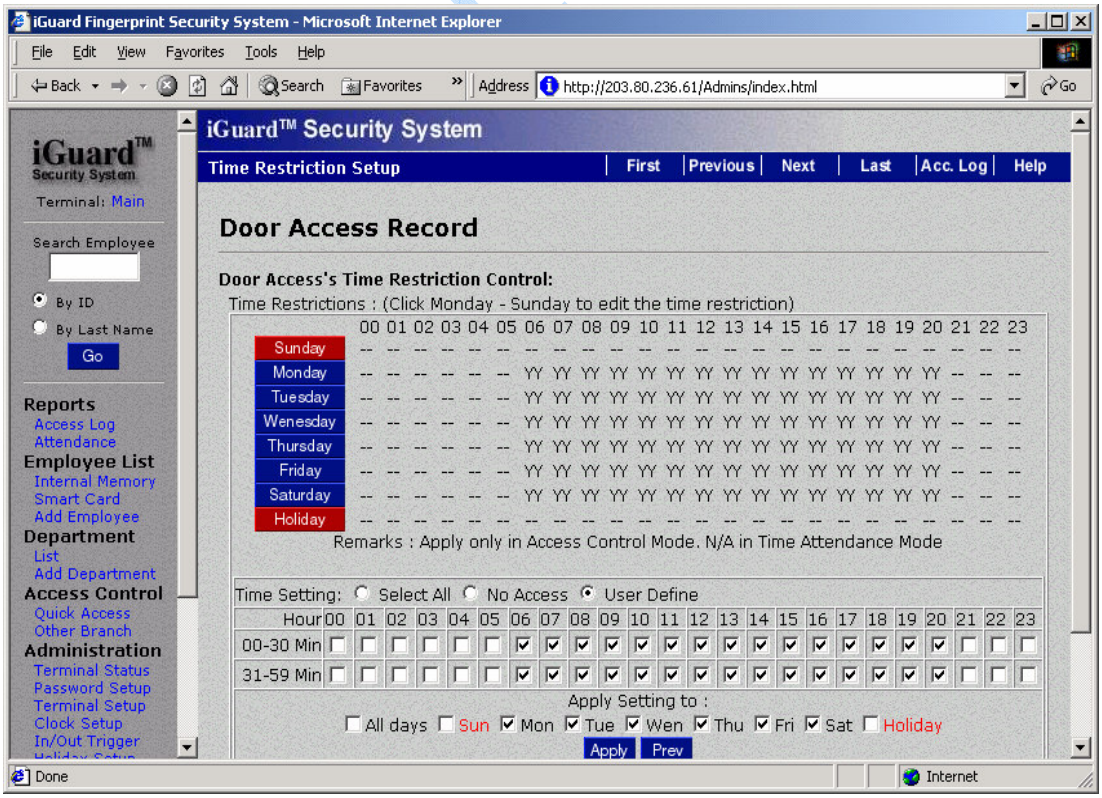
Description	***Affichage Ecran***
En Mode Stand-by, presser la touché **Func** pour entrer dans le menu Installation. Entrer le Mot de Passe Administrateur Système (défaut 123) et presser la touche **Func**, presser **6** pour sélectionner le menu « Installation mot de passe » Le menu "Admin /Personnel (1/2) ?" apparaît. pressez 1 pour choisir le mot de passe d'Administrateur.	**Admin Système: 123_**
Presser pour effacer le vieux mot de passe et entrer le nouveau mot de passe (par exemple, AB456). La limite de taille des champs pour des mots de passe individuels est 10 chiffres, de 0-9 et A/B.	**Admin Système: AB456_**
Presser la touche **Func** pour accepter le nouveau Mot de Passe Administrateur Système. Vous serez alors incités pour le Mot de passe d'Administrateur d'Utilisateur comme indiqué.	**Admin Usager: _**
Entrer le nouveau Mot de Passe Administrateur Usager (e.x. 7890BA).	**Admin Usager: 7890BA_**
Presser la touche **Func** pour accepter le nouveau Mot de Passe Administrateur Usager. Vous serez alors incités pour le Mot de passe d'Accès de Porte comme indiqué.	**Accès Porte: _**
Entrer le nouveau Mot de Passe d'Accès Porte (e.x, 9394AB709). Il est suggéré d'employer un long et le mot de passe de conjecture dur.	**Accès Porte: 9394AB709_**
Presser la touche **Func** pour retourner en mode stand-by.	**Lun 30 Août 13:49 ID #:_**

Note:

Vous devez permettre le Mot de passe d'Accès de Porte avant qu'il ne puisse être employé, en spécifiant la transmission le temps autorisé et les terminaux. Il est mis hors de service dans les paramètres d'usine. La seule façon de le permettre est via le Navigateur Internet (discutée dans des sections postérieures), sous "l'Accès Rapide" comme montré dans la page qui suit :-



Comme indiqué dans la photo ci-dessus, il n'y a aucun temps autorisé assigné dans les paramètres par défaut et aucun des terminaux n'est choisi. Vous devez spécifier la période autorisée en cliquant sur un des boutons des Jours (c'est-à-dire, dimanche à samedi et des boutons de Jour férié {*congé*}), choisir ensuite la période désirée (dans un intervalle de 30 minutes). La photo suivante montre un paramétrage typique :-



Après la spécification du temps autorisé et des terminaux, vous pouvez gagner l'accès employant le Mot de passe d'Accès de Porte et il est illustré dans les étapes suivantes:-

Description	***Affichage Ecran***
En Mode Stand-by, Presser la touche **Func**. Il vous sera demandé d'entrer le Mot de Passe	**Entrer Mot de Passe: _**
Entrer le Mot de Passe d'Accès Porte (comme 9394AB709). Pour des raisons de sécurité le Mot de passe est montré sous forme d'étoiles.	**Entrer Mot de Passe : ***********
Pressez la touche FUNC de nouveau pour passer. Si le mot de passe est juste, iGuard actionnera la gâche de porte et retournera au Mode Stand-by.	**Lun 30 Août 13:49 ID #:_**

Plus de détails de l'utilisation du Navigateur Internet seront discutés dans des sections postérieures.

1Vous ne devez pas confondre ces Mots de passe Globaux avec le Mot de passe Personnel, qui peut être assigné uniquement à chaque individu. Plus de détails du Mot de passe Personnel seront discutés dans des sections postérieures.

3. OPERATIONS de BASE

3.1. INSCRIPTION (ENRÔLEMENT)

3.1.1. Enrôlement avec Empreinte Digitale

L'inscription d'empreinte digitale doit enregistrer un calibre d'empreinte digitale pour l'identification postérieure. Une bonne inscription est cruciale pour tous les systèmes d'identification d'empreinte digitale fiables, incluant l'iGuard.

IGuard profite du DFX avancé (l'Extraction d'Empreinte digitale Difficile) la technologie (à l'origine développé par les Labs Bell des ETATS-UNIS), qui travaille exactement avec les images d'empreinte digitale les plus populaires. IGuard peut réaliser un taux de Faux rejet exceptionnellement bas de moins de 1 %.

Cependant, comme des individus, nos mains ont les niveaux différents d'humidité. Dans quelques cas, iGuard peut avoir de la difficulté dans la reconnaissance des images d'empreinte digitale des utilisateurs spécifiques, le plus généralement, les gens avec la peau sèche. Le problème est plus considérable pendant le processus d'inscription puisque le détecteur exige une image d'empreinte digitale de qualité plus précise et plus haute que le processus de vérification normal. La façon la plus facile de contourner ce problème est d'appliquer une petite quantité de lotion sur nos doigts pendant le processus d'inscription. Cela est seulement nécessaire dans l'étape d'inscription et ne sera pas nécessaire dans le processus de vérification quotidien.

Dans le cas de mauvaise qualité d'empreinte digitale ou de doigt sec, iGuard vous demandera si vous voulez baisser la sécurité correspondante. Un niveau de sécurité bas apportera plus de convenance à l'utilisateur, mais avec un sacrifice mineur de sécurité. Nous recommandons de choisir la sécurité basse seulement pour l'application de gestion de temps de présence.
Chaque personne doit enregistrer deux doigts : un comme le primaire et l'autre comme le secondaire. Dans le cas où le doigt primaire n'est pas approprié pour la vérification quand le doigt est endommagé, la personne peut employer son doigt secondaire pour le processus d'identification.

Pendant le processus, chaque image d'empreinte digitale est capturée trois fois pour l'analyse de minuties et l'extraction. Si la qualité d'une des trois images n'est pas assez bonne, on vous demandera de reprendre les trois images de nouveau.

Il est suggéré d'employer vos deux pouces comme vos doigts primaires et secondaires. Parce que vos pouces sont d'habitude plus grands et peuvent mieux couvrir le secteur de scanner.

IMPORTANT: Pendant le processus d'inscription, vous devez placer le centre de votre doigt au centre du détecteur d'empreinte digitale. Le centre de l'empreinte digitale contient la plupart des points de minuties que le détecteur d'empreinte digitale peut extraire. Une bonne image d'empreinte digitale capturée pendant le processus d'inscription peut significativement réduire le taux de faux rejet pendant les vérifications postérieures.

Les étapes suivantes vous montrent comment enregistrer le calibre d'empreinte digitale de l'utilisateur :

Description	***Affichage Ecran***
En mode stand-by, presser la touche **Func** pour entrer dans le menu Installation. Entrer le mot de passe Administrateur (défaut 123) et presser la touche **Func**, ensuite presser **1** pour sélectionner le menu "Ajout /Mise à jour ID". Presser **1** pour entrer l'empreinte digitale.	**Par Doigt/Mot de Passe (1/2)?** **Entrer ID # et scanner 1er Doigt**
Entrer l' ID usager # (e.x. A01). L'ID peut avoir de n'importe quelle longueur de 1 à 8 caractères.	**Entrer ID# A01_**
Presser la touche **Func** pour confirmer l'ID #. Le dispositif commence maintenant à capturer la 1e image du doigt primaire. La barre horizontale sur la deuxième ligne indique la qualité de l'image. Soulevez l'obturateur de détecteur avec votre pouce droit et placez-le fermement sur le détecteur avant que la barre de qualité n'atteigne la fin. Vous pouvez devoir déplacer et faire tourner le pouce un peu pour réaliser la qualité exigée.	**Scannage 1 de 3...** : : **Scannage 1 de 3...**
Après que la barre de qualité ait atteint la fin, on vous demandera d'enlever le doigt du détecteur.	**Analyse. SVP Enlever doigt...**
Quand le dispositif détecte que vous avez enlevé le doigt, il vous demandera de le replacer de nouveau pour la 2ème image.	**Presser Func pour scan 2 de 3**
Pressez la touche **Func** et répétez la même procédure et on vous demandera de parcourir la 3ème fois le même doigt primaire.	**Presser Func pour scan 3 de 3**
Pressez la touche **Func** de nouveau et répétez la procédure pour la troisième fois. On vous demandera alors de faire pareil pour le doigt secondaire.	**Presser Func pour scan 2nd Doigt**
Pressez la touche **Func** et répétez les susdits pas pour parcourir le doigt gauche trois fois de nouveau. Si toutes les images sont OK, vous verrez le message suivant "ID : A01 Ajouté OK!" Momentané, alors le dispositif est prêt pour l'inscription suivante	**ID: A01 Ajouté OK!** : : **Entrer ID # et scan 1er Doigt**

Presser ← pour retourner en mode stand-by.	Lun 30 Août 12:00 ID #:_
Dans le cas de doigt sec (mauvaise image d'empreinte digitale), il vous avertira pour le doigt sec. Vous pouvez ou bien humidifier votre doigt avec la lotion et essayer de nouveau, ou continuer.	Scanner 1 de 3 === Trop Sec!===
Si vous continuez avec un doigt sec, à la fin, il vous demandera si vous voulez mettre la sécurité à low2. Nous recommandons de choisir la sécurité basse seulement pour la gestion de présence de temps.	Niveau Sécurité plus bas oui (1)/Non (2)?

3.1.2. Permission Automatch

Cette particularité permet au dispositif d'identifier une personne sans exiger que l'utilisateur entre d'abord son ID utilisateur et doit être programmée via le Navigateur Internet, comme décrit dans la section suivante. Tout ce que vous avez à faire est de présenter votre doigt inscrit au détecteur et attendre la comparaison de votre calibre d'empreinte digitale avec des calibres stockés. Une fois qu'Automatch est fait, la porte s'ouvre et le système retourne alors au mode stand-by.

Il est recommandé de limiter à 30 le nombre maximal d'utilisateurs auquel il est permis d'avoir accès à l'iGuard en utilisant l'automatch. Ceci pour limiter le temps que l'iGuard exigerait pour traiter l'empreinte digitale et la comparer avec TOUTE la base de données stockée sur votre iGuard. On recommande donc que la particularité d'automatch soit laissée pour des cadres supérieurs, le reste du personnel peut employer ID plus l'Empreinte digitale pour l'accès. L'utilisateur ayant une mauvaise qualité d'empreinte digitale n'emploiera pas la fonction automatch.

3.1.3. Enrôlement avec Smart Card. (pour Modèles avec lecteur Smart Card.)

L'utilisateur doit être créé avant l'utilisation cette fonction, ou bien l'empreinte digitale est inscrite ou bien le mot de passe est ajouté. Après la procédure d'inscription, l'ID utilisateur et le calibre d'empreinte digitale sont stockés dans la mémoire interne.

Notez s'il vous plaît que seulement le calibre d'empreinte digitale du doigt primaire soit stocké sur la carte à puce.

Les étapes suivantes illustrent comment écrire l'information d'utilisateur sur la Smart Card.

Description	***Affichage Ecran***
En mode stand-by, presser la touche **Func** pour entrer dans le menu Installation. Entrer le mot de passe Administrateur (défaut 123) et presser la touche **Func**, ensuite presser **9** pour sélectionner le menu "Ajout/Import Card.". Presser **1** pour ajouter une Smart Card.	**Entrer ID #: _**
Entrer le N° ID que vous voulez écrire sur la Smart card. (ex, A01).	**Entrer ID #: A01_**
Presser **Func** pour confirmer. Il vous sera demandé de présenter la Smart Card.	**Attente Smart Card...**
Présenter une Smart card près du clavier. L'unité écrira alors les informations de l'usager dans la mémoire de la Smart card.	**Ecriture....**
Après l'écriture à la carte, on vous demandera si vous voulez enlever les informations d'empreinte de l'utilisateur de la mémoire interne. On recommande de ne pas enlever les informations de l'utilisateur de la mémoire.	**Effacer Mémoire Interne Oui (1)/Non (2)?**
L'unité demandera alors pour une autre ID	**Entrer ID #: _**
Presser la touche <-- une fois ou attendez la fin de temps, l'unité retournera en mode stand-by.	**Lun 30 Août 12:00 ID #:_**

Notez s'il vous plaît que la susdite procédure effacera toute l'information existante déjà stockée dans la Carte à puce.

3.1.4. Enregistrement d'une Smart Card. existante

La première fois qu'un utilisateur a accès à une unité éloignée dans une filiale éloignée avec cette Smart card. l'utilisateur doit enregistrer la Carte à cette unité. De plus, après l'enregistrement l'administrateur de système doit aussi assigner

les départements auxquels l'utilisateur appartient, et accorder à l'utilisateur les droits d'accès exigés. Après cela, l'utilisateur peut employer sa carte pour avoir accès à l'unité éloignée comme dans celui de sa propre filiale.

La procédure d'enregistrement lit l'information d'utilisateur de la Carte à puce et stocke l'information de la Mémoire de la Carte à puce dans la base de données d'utilisateur interne.

La procédure est effectuée via la **Fonction 0** dans le menu Installation, et illustré dans les étapes suivantes.

Description	***Affichage Ecran***
En mode stand-by, presser la touche **Func** pour entrer dans le menu Installation. Entrer le mot de passe Administrateur (défaut 123) et presser la touche **Func**, ensuite presser **9** pour sélectionner le menu “Ajout/Import Card". Presser **2** pour importer une Smart Card.	`Entrer ID #: _`
Presser **Func** pour confirmer. Il vous sera demandé de présenter la Smart Card.	`Attente Smart Card...`
Présenter une Smart card près du clavier. L’unité écrira alors les informations de l’usager dans la mémoire de la Smart card.	`Ecriture....`

3.1.5. Vérification avec Empreinte digitale

L'appareil utilise les informations d'empreintes enregistrées pour identifier la personne. Le processus de vérification est très direct et est illustré dans les étapes suivantes :-

Description	***Affichage Ecran***
En mode stand-by, Tapez le Numéro ID de l'utilisateur (e.x, A01).	**Lun 30 Août 13:49** **A01_**
Soulever l'obturateur et placez votre premier doigt (pouce droit) ou votre second doigt (pouce gauche) sur le sensor. Vous devez placer le doigt de la même manière que lors de la procédure d'inscription. L'appareil entame automatiquement le scanner quand le volet de l'obturateur est en position haute.	**Scan... A01_** : : **Vérification...**
Si vous êtes authentifié, l'appareil ouvrira la porte et retournera en mode stand-by	**A01 Autorisé!** : : **Lun 30 Août 13:49** **ID #:_**

Note: Il y a une autre particularité appelée « Automatch », qui permet à l'utilisateur d'avoir accès au dispositif sans avoir besoin d'entrer son ID d'abord.

3.1.6. Vérification avec Automatch

La particularité d'Automatch permet aux utilisateurs d'être authentifié sans introduire leur N° ID. Cette particularité permet aux cadres supérieurs d'entrer aux locaux sans avoir à entrer leur ID, leur permettre l'accès plus rapide.

Description	***Affichage Ecran***

En Mode Stand by, placez votre premier ou votre second doigt sur le sensor en soulevant le volet. L'appareil démarre automatiquement le scan dès que le volet est complètement soulevé	`Lun 30 Août 13:49`
	`== Automatch !==`
	`:`
	`:`
	`Lun 30 Août 13:49`
	`Vérification...`

Si vous êtes authentifié, l'appareil ouvrira la porte, et retournera en mode stand by.	`Lun 30 Août 13:49` `Autorisé !`

3.1.7. Vérification avec Smart Card.

La procédure d'authentification utilisant la smart card est simple et direct, elle est illustrée dans les étapes suivantes -

Description	***Affichage Ecran***
En mode stand-by, présentez la smart card près du clavier. L'unité lira les données stockées sur la carte, et si la carte est valide (si ce n'est pas une carte vierge, et avec le code compagnie correct), on vous demandera de scanner votre doigt.	`Jacky Hui` `Attente Doigt`
L'image d'empreinte digitale correspond aux données stockées dans la carte, l'utilisateur est authentifié. L'unité retourne au mode stand-by et est prête pour la carte suivante.	`Jacky Hui` `Autorisé`

3.1.8. Vérification avec Mot de Passe

Description	*Affichage Ecran*
En mode stand-by, Tapez votre N° ID (e.x, A01).	`Lun 30 Août 13:49 A01_ IN`
Au lieu de lever l'obturateur et de placer le doigt sur le sensor, pressez la touche **Func**.	`Mot de Passe:`
Entrer votre Mot de Passe personnel (e.x, 123456)	`Mot de Passe: ******`
Pressez encore la touche **Func** pour confirmer. Si le mot de passe personnel est correct, la personne est authentifiée et ce message apparaît.	`A01 Autorisé`

3.1.9. Suspension / Reprise Utilisateur

Vous pouvez provisoirement suspendre un ID utilisateur. C'est utile si vous voulez empêcher provisoirement un utilisateur d'entrer dans les locaux et vous voulez pouvoir lui redonner son droit d'accès plus tard. C'est est fait via la fonction "ID Inactif" et est illustré dans les étapes suivantes: -

Description	*Affichage Ecran*
En mode stand-by, presser la touche **Func** pour entrer dans le menu Installation. Entrer le mot de passe Administrateur (défaut 123) et presser la touche **Func**, ensuite presser **2** pour sélectionner le menu “Désactivation ID".	`Entrer ID:`
Entrer le N° ID # que vous voulez suspendre (e.x : A01).	`Entrer ID: A01`
Presser la touche **Func** pour confirmer. Le N) d’ID est suspendu, Et l'utilisateur ne peut plus être authentifié. Le système retournera en mode stand-by.	`ID A01: Désactivé !`

3.2. AUTRES FONCTIONS

3.2.1. Suppression ID

Vous pouvez supprimer un N° ID en utilisant la procédure décrite et illustrée ci dessous: -

Description	***Affichage Ecran***
En mode stand-by, presser la touche **Func** pour entrer dans le menu Installation. Entrer le mot de passe Administrateur (défaut 123) et presser la touche **Func**, ensuite presser **4** pour sélectionner le menu "Suppression ID"	**ID à supprimer:**
Entrer le N° ID que vous voulez supprimer (e.x, A01).	**ID à supprimer: A01**
Presser la touche **Func** pour confirmer. Le N° ID est supprimé, Et l'utilisateur ne peut plus obtenir l'accès. Le système retournera en mode stand-by.	**ID #A01 Supprimé!**

Note:
Une fois qu'un N° ID est supprimé, toute les informations associée à l'ID employé , comme les données d'empreinte digitale et les droits d'accès, sont aussi supprimées de manière permanente . Vous devez ré inscrire l'employé si nécessaire.

3.2.2. Réinitialisation du dispositif

Le dispositif peut être éteint facilement en coupant simplement l'alimentation. Cependant, il y a une très petite chance que l'unité soit dans le processus d'accès ou de mise à jour de la mémoire interne au moment où l'alimentation est coupée. Cela peut aboutir à la perte de données.

La façon sûre d'éteindre l'unité est de faire une fermeture appropriée en ayant accès à la **Fonction 7** dans le menu. Vous pouvez aussi restaurer la base de données utilisateur et les rapports d'accès avec cette fonction. De plus, vous pouvez remettre tous les paramètres par défaut d'usine (comme l'adresse IP par défaut 192.168.0.100 et le nom du terminal à iGuard... Etc.)

3.2.3. Procédures d'urgence

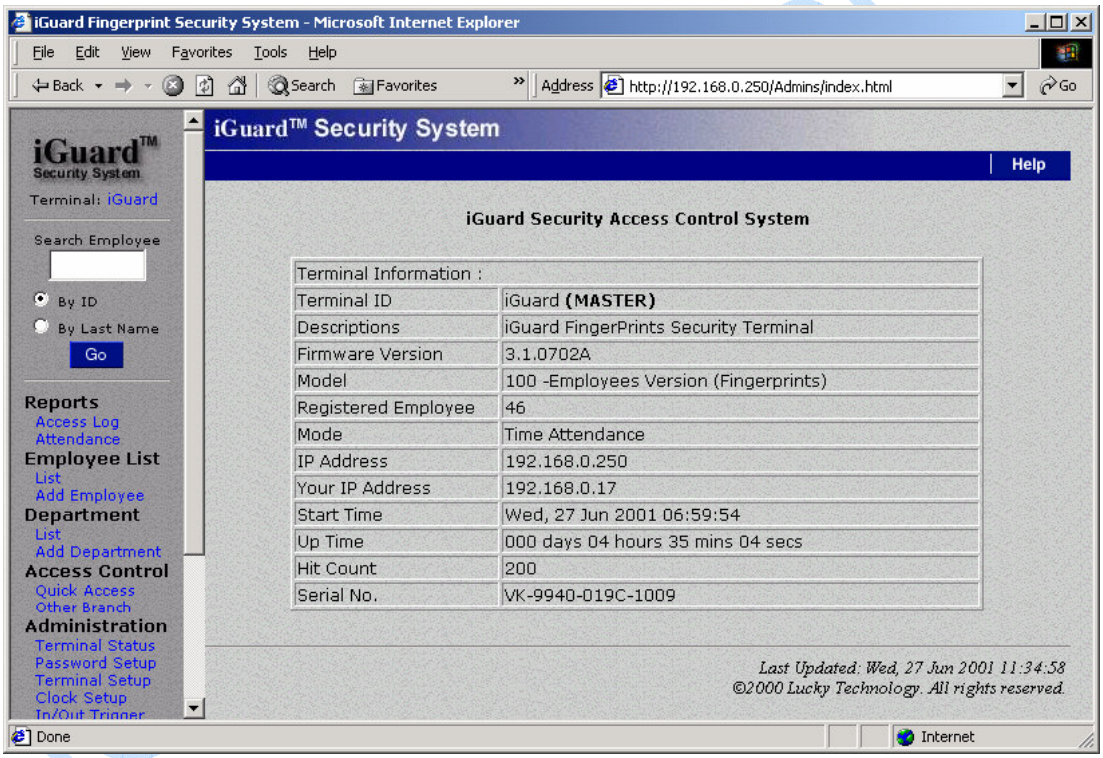
Cette particularité a été ajoutée comme une précaution de sécurité, si par hasard votre iGuard ne réussit pas à vous répondre et n'ouvre pas la porte comme programme. En mode Stand-by, pressez la touche Func pour entrer en Mode d'Installation. Entrez votre Mot de passe d'Administrateur (par défaut 123) et pressez la touche Func à nouveau. Pressez alors sur la touche B pour ouvrir la porte manuellement.

4. ADMINISTRATION

4.1. Utilisation du navigateur Web

Le Serveur Web incorporé dans chaque dispositif iGuard vous permet d'employer le logiciel de Navigation Internet pour gérer et configurer le dispositif et avoir accès aux rapports de ces dispositifs. Vous pouvez employer Microsoft Internet Explorer ou le logiciel de Navigation Netscape courant sous Windows 98, Windows 2000, Windows ME, Apple de Macintosh, Linux et Unix.

Une fois connecté à votre réseau d'ordinateur d'entreprise, vous pouvez avoir accès au dispositif en spécifiant l'adresse IP (ex., http://192.168.0.100). C'est l'adresse IP assignée au dispositif pendant la procédure d'installation. L'écran suivant sera montré :-

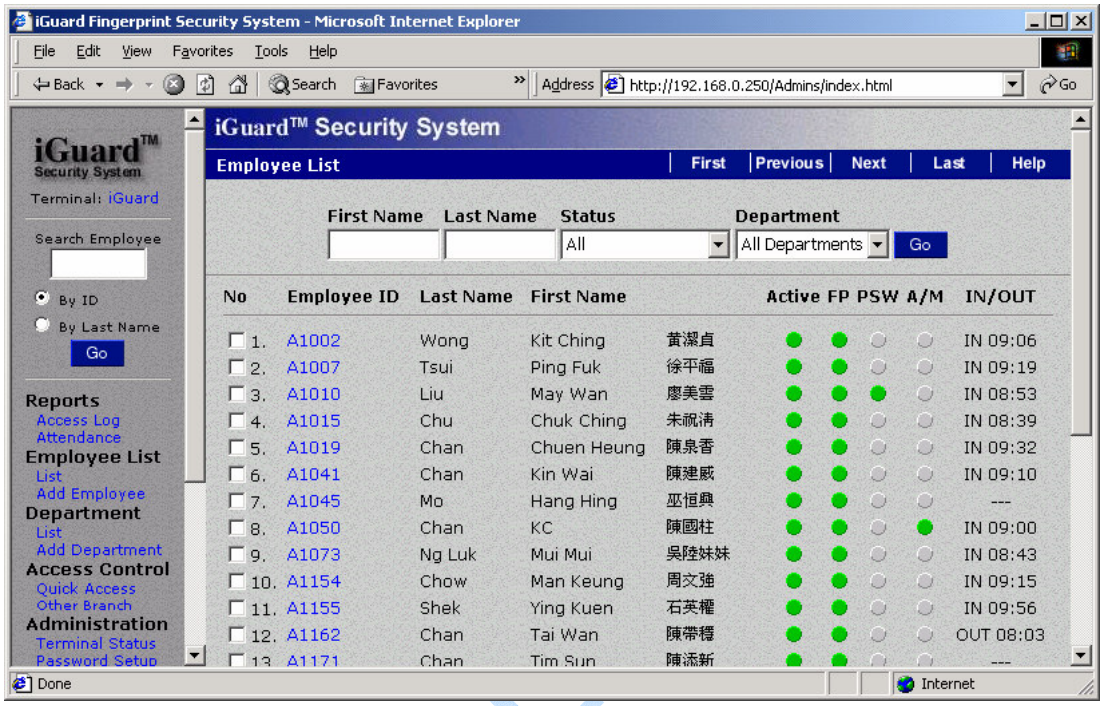


La page d'accueil de l'iGuard est divisée en panneaux gauches et droits. Vous pouvez choisir des fonctions différentes dans le panneau gauche et le panneau droit montrera les résultats correspondants.
Note: La page d'accueil de votre iGuard peut différer de celle montrée ci-dessus selon le modèle que vous avez.

Chaque article dans le panneau gauche correspond aux pages différentes dans le panneau droit et sera montré dans les sections suivantes.

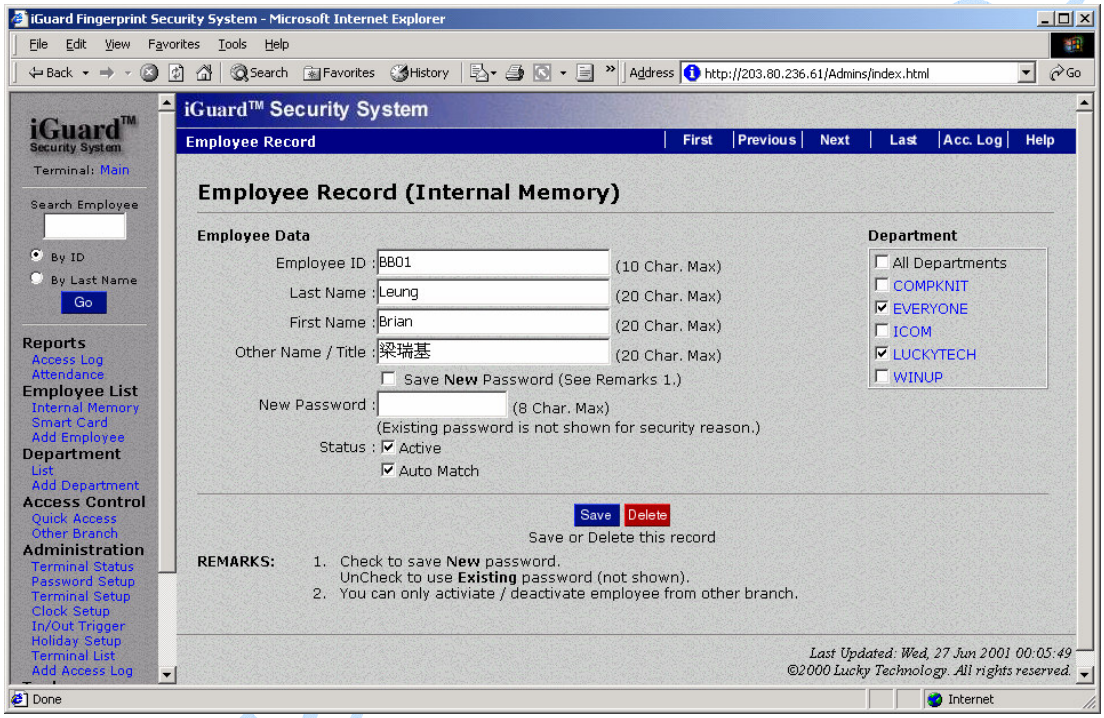
4.2. Liste des Employés

Cliquez sur "Liste Employés", il montrera la liste complète des employés.



4.3. Liste des Employés - Ajouter Employé

Normalement un nouvel employé est ajouté par le processus d'inscription, comme déjà décrit dans la section "Opération de Base - Inscription». Cependant, vous pouvez aussi ajouter un employé la page "Ajouter Employé». Notez s'il vous plaît que bien qu'un employé soit rajouté on exige toujours cette page, pour enregistrer son image d'empreinte digitale physiquement au dispositif avant qu'il / elle ne puisse être authentifier par le dispositif.

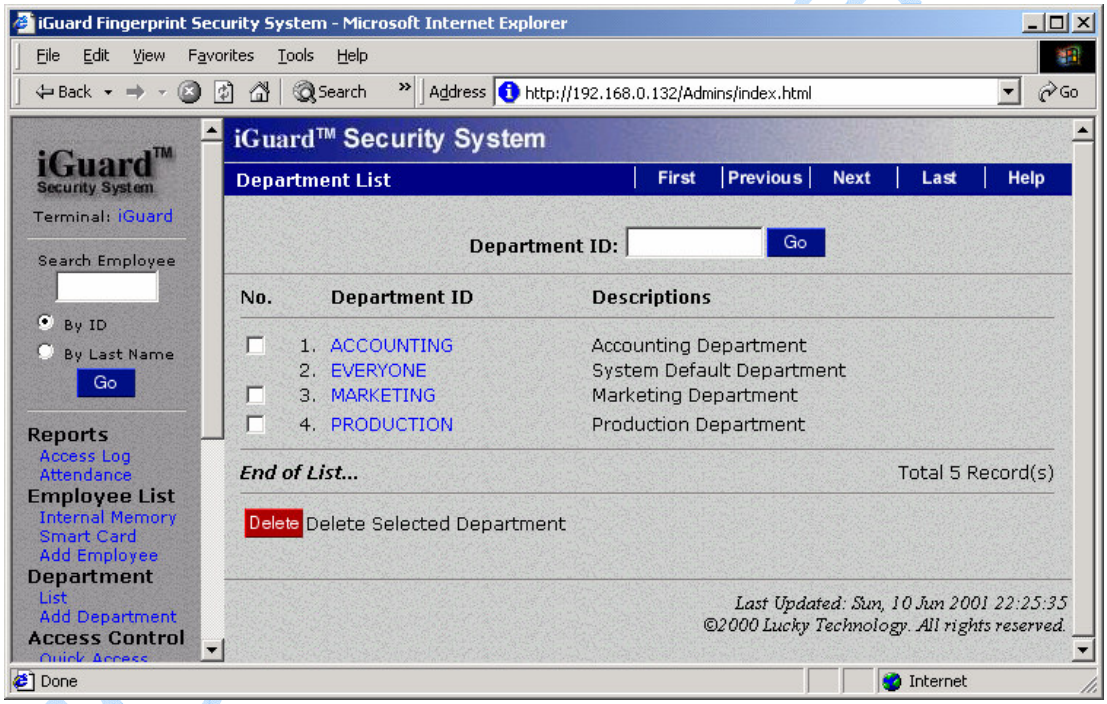


4.4. Liste des Départements -

Un des buts de créer des départements permet de diviser les employés dans des groupes différents. Chaque département a son propre temps d'accès autorisé. Par exemple, vous pouvez assigner la période autorisée pour le Département de Marketing de 9:00 est à 6:00 de l'après-midi et tous les membres dans le Département de Marketing peuvent avoir accès au dispositif seulement dans la période spécifiée.

Le nombre maximum de départements est de 32.

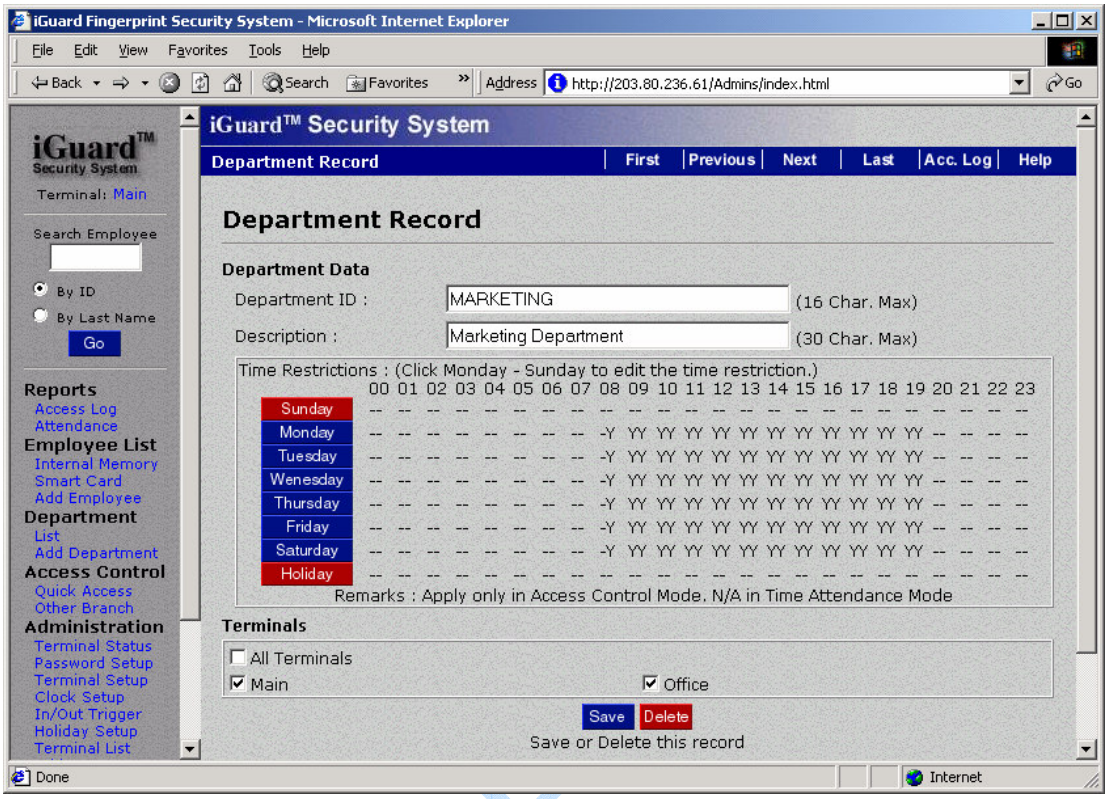
La page “Liste des Départements” est montrée comme suit :



Cette page inscrit tous les départements disponibles. Le département EVERYONE est le département par défaut et ne peut pas être supprimé. Quand un nouvel employé est ajouté, ce nouvel employé est automatiquement ajouté à la liste de membre d' EVERYONE. Vous pouvez éditer la restriction de temps de ce département par défaut (montré dans la section suivante) et vous pouvez aussi enlever l'employé du département.
Vous pouvez supprimer un département simple ou un groupe de départements en cochant la case correspondante dans la "liste des Départements" et en pressant le bouton "Supprimer". Notez s'il vous plaît que vous ne pouvez pas supprimer le département par défaut EVERYONE.

.

Pour éditer la période autorisée d'un département particulier, cliquez sur l'ID département dans la susdite page (par exemple, COMMERCIAL). La page suivante apparaîtra: -

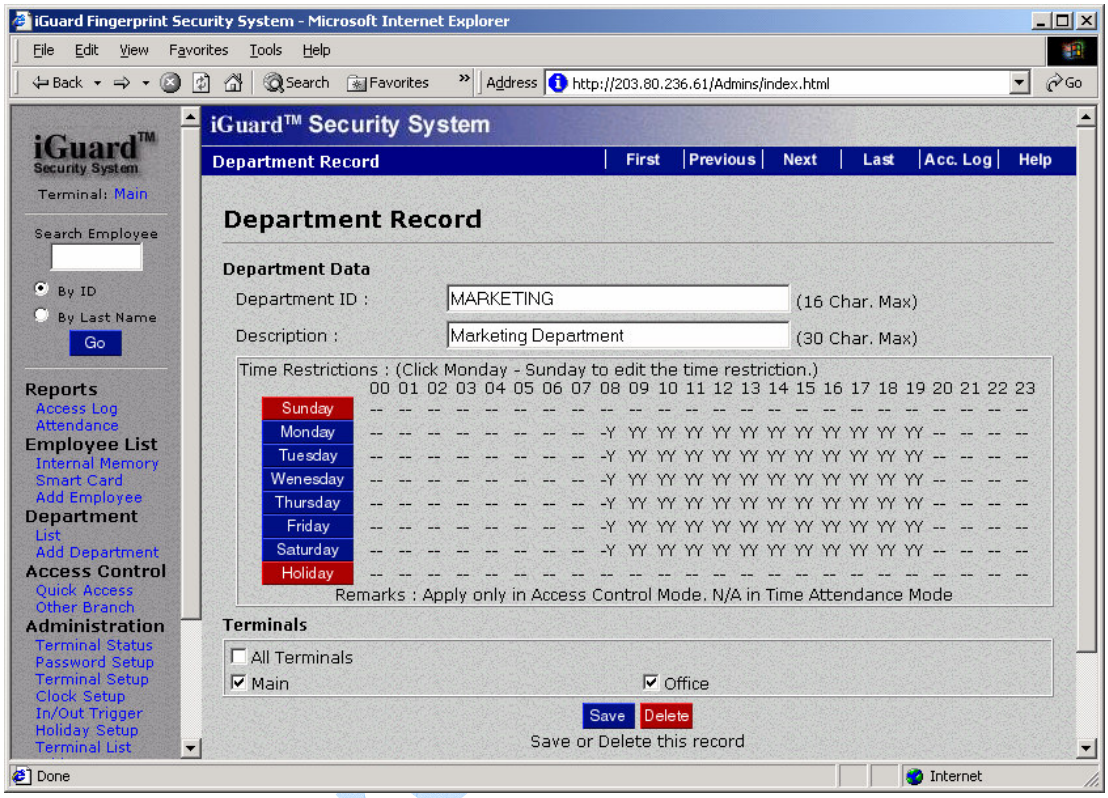


La susdite page indique que la période autorisée pour le département Marketing est de 8:30 à 7:59 de l'après-midi, de lundi à samedi. En conséquence, tous les membres de ce département peuvent seulement être autorisés dans cette période.

Vous pouvez éditer le temps autorisé d'un jour particulier (par exemple, lundi) en cliquant sur le bouton lundi et la page Web dans la page suivante apparaîtra. Vous pouvez choisir la période autorisée au fond de la page. Si vous voulez choisir toutes les périodes de temps, vous pouvez simplement cocher la case "Sélectionner Tout" ci-dessus. Vous pouvez aussi cocher la case "Tous les Jours" pour inclure tous les jours de la semaine.

4.5. Département - Ajouter Département

Pour ajouter un nouveau département, cliquez sur la ligne« *Ajouter Département* »sur le panneau gauche. Il apparaîtra la page suivante. Notez que le nombre maximum de département est de 32.



Entrez l'ID Département et la Description dans les susdites boîtes de texte. Après cela, vous devez cliquer un jour pour faire les Restrictions de Temps pour permettre aux employés d'entrer dans les locaux.

Si vous voulez définir les choix du temps spécifiques d'accès, dans paramètres de Temps, choisissez "Utilisateur défini". Cela vous permettra de vérifier les choix du temps d'accès, qui peut être de 08:00 - 19:00. Choisissez alors les jours que vous voudriez que ces changements affectent. Pour tous les jours, cochez la case"Tous Jours". Pour d'autres, vérifiez les boîtes correspondantes des jours que vous voulez que ces changements s'effectuent.

Après la sélection des jours, cliquez sur "Appliquer" pour sauvegarder ces paramètres.

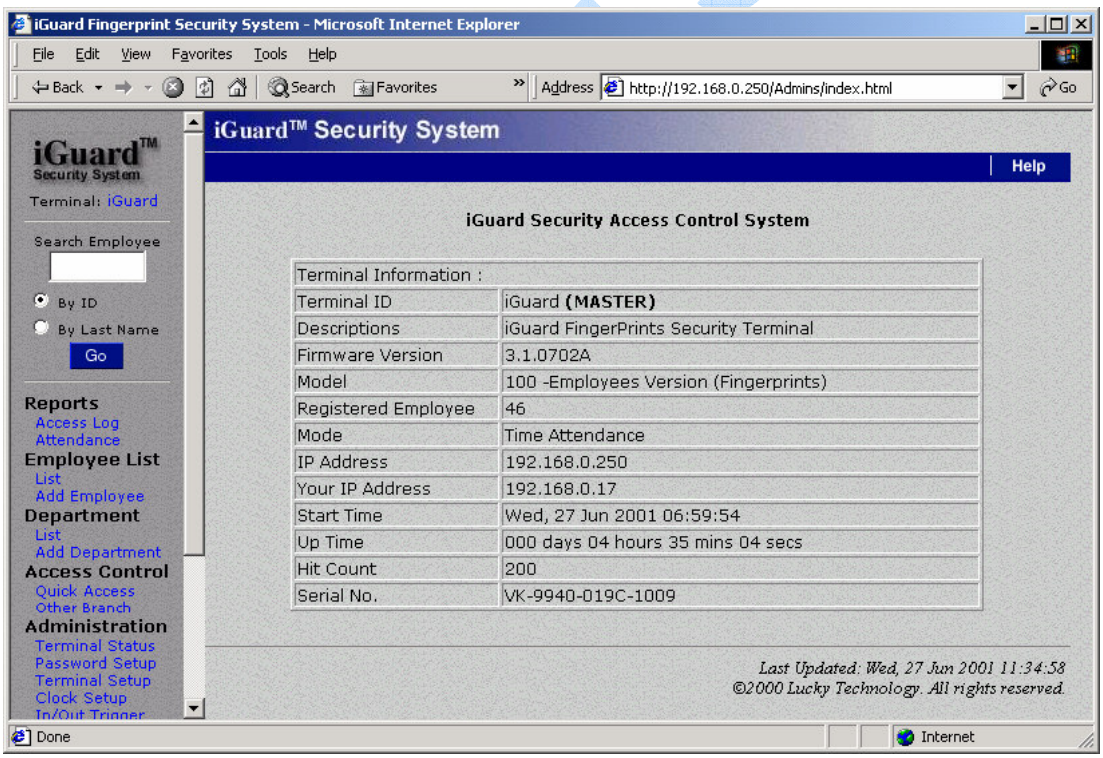
4.6. Contrôle d'Accès – Accès Rapide

L'accès Rapide peut être employé pour contourner le processus d'authentification d'empreinte digitale. Les paramètres par défaut ne vous permettent pas d'employer le Mot de passe d'Accès (voir Administration - Installation de Mot de passe) ou la Carte à puce (pour le modèle de Carte à puce) pour contourner le processus d'authentification d'empreinte digitale.

La procédure pour l'installation de cette page est semblable à la procédure pour créer le département. Une fois que le temps actuel est dans la période valable, les utilisateurs peuvent employer le Mot de passe d'Accès ou la Carte à puce pour entrer aux locaux.

4.7. Administration – Statuts du Terminal

C'est la page d'accueil du dispositif. Il montre l'information générale du dispositif, incluant le modèle, le nombre d'utilisateurs enregistrés, le numéro de série de l'unité et plus.

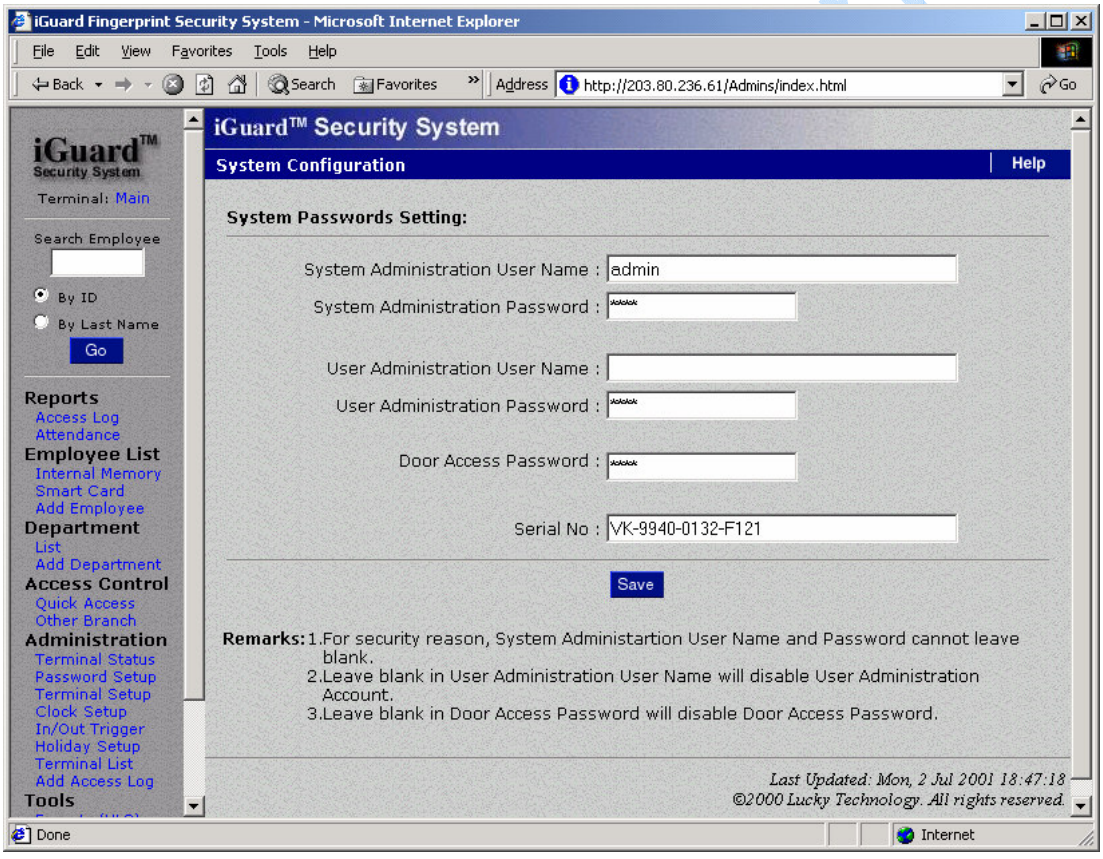


4.8. Administration – Installation Mot de Passe

Installation des Mots de passe d'Administrateur et le Mot de passe d'Accès de Porte comme suit

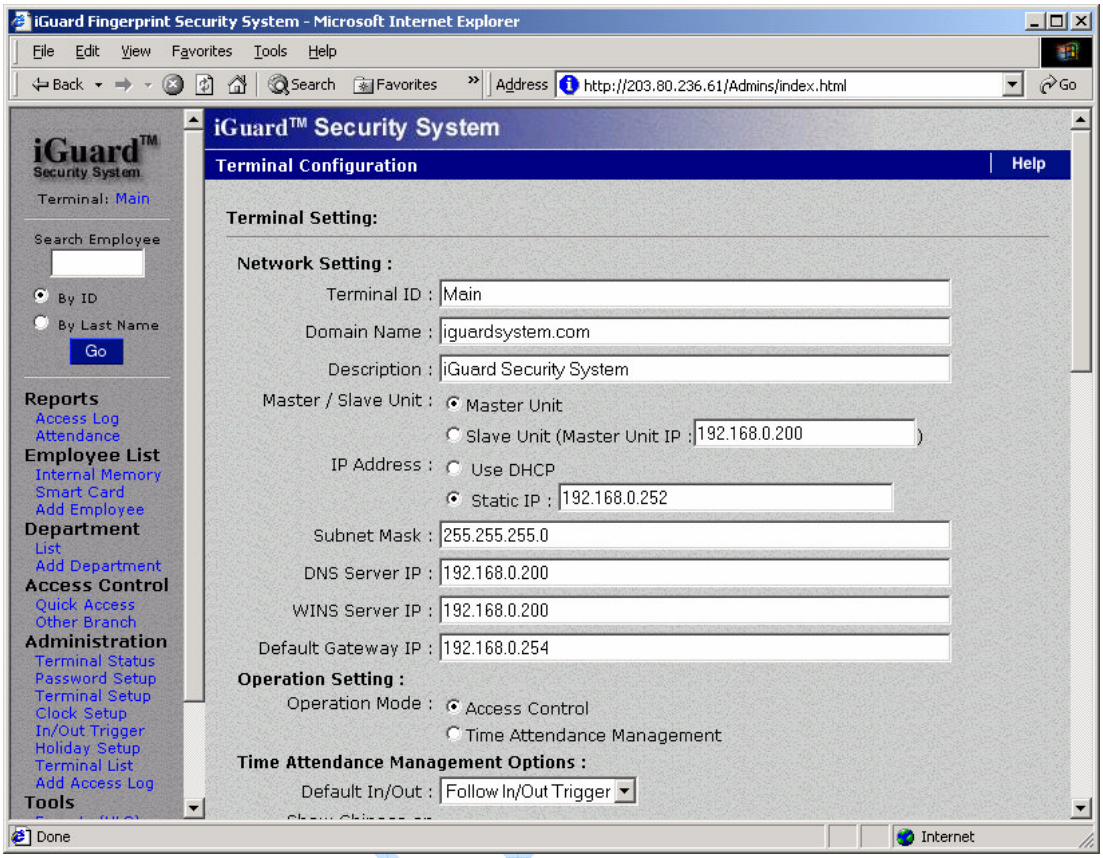
:

- l'Administration de Système - c'est le nom d'utilisateur et le mot de passe exigé pour configurer le système (comme l'installation de l'adresse IP du dispositif) et administrer les paramètres des utilisateurs (comme l'addition et la suppression d'utilisateurs). Le nom par défaut est admin et le mot de passe par défaut est 123
- l'Administration Utilisateur - c'est semblable au précédent, sauf qu'il ne peut pas être employé pour configurer le système. Il n'y a aucune valeur par défaut.
- le Mot de passe d'Accès de Porte - c'est le mot de passe d'accès rapide pour la configuration d'Accès Rapide. C'est le mot de passe commun que tous les utilisateurs emploient pour ouvrir la porte pendant le trafic haut la période (comme pendant le bureau normal l'heure), quand la haute sécurité n'est pas nécessaire.



4.9. Administration – Installation Terminal

Sélectionner: installation Terminal



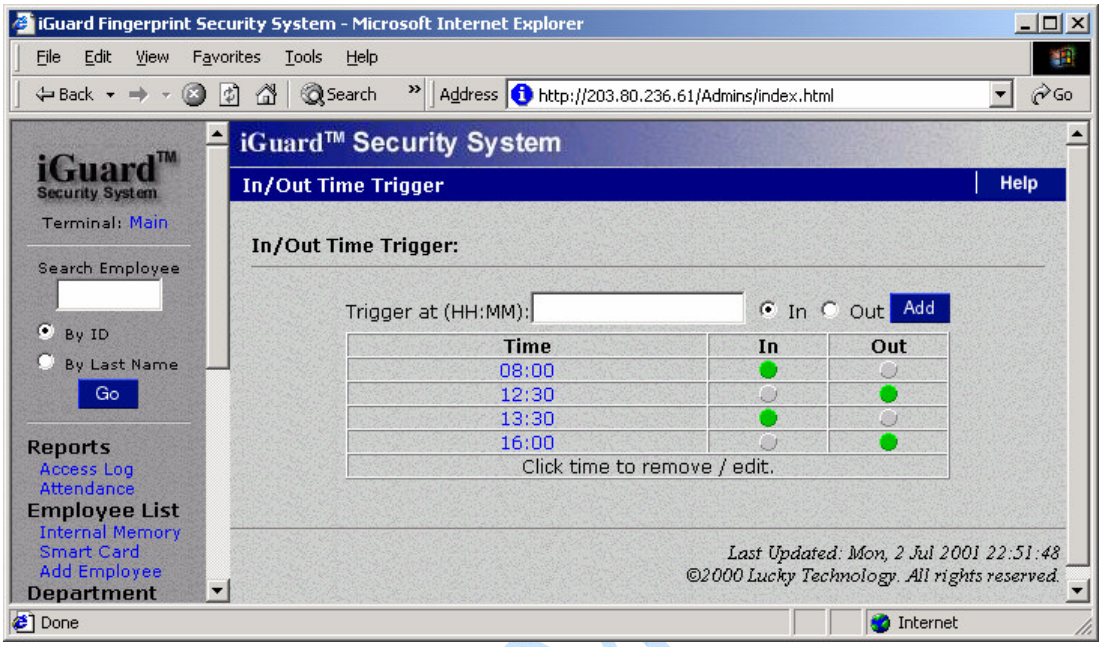
4.10. Administration – Installation Horloge

Valeur Automatique Date / Heure : Quand cela est autorisé, le temps de votre iGuard est automatiquement configuré comme le temps sur votre système d'ordinateur.
Localisation (Zone Horaire): Pour spécifier le fuseau horaire de votre région, choisissez s'il vous plaît l'option dans ce menu.
No de Série.: C'est le numéro de série unique de cette machine. Vous pouvez devoir fournir l'information si vous avez besoin de l'assistance technique pour le dispositif.
Il y a un logiciel pour vous permettre de synchroniser automatiquement l'horloge avec l'horloge de votre PC quotidiennement. Celui-ci est disponible sur le site.

S'il vous plaît notez aussi que si un dispositif est configuré comme le dispositif de Maître et est relier à d'autres dispositifs Esclave dans le même réseau, le nouveau paramètre d'horloge mettra automatiquement à jour tous les dispositifs esclave.

4.11. Administration – Bascule Entrée / Sortie

La bascule Entrée / Sortie définit le temps pour ou bien "ENTREE" ou bien "SORTIE" pour le rapport d'accès.



Le paramètre de Temps Entrée / Sortie est utile seulement si le dispositif est configuré pour le but de gestion de Temps de présence. Dans le susdit paramètre, le dispositif mettra par défaut Entrée / Sortie comme Entrée à 6:00 et le mettront à Sortie 12:00pm... Etc.

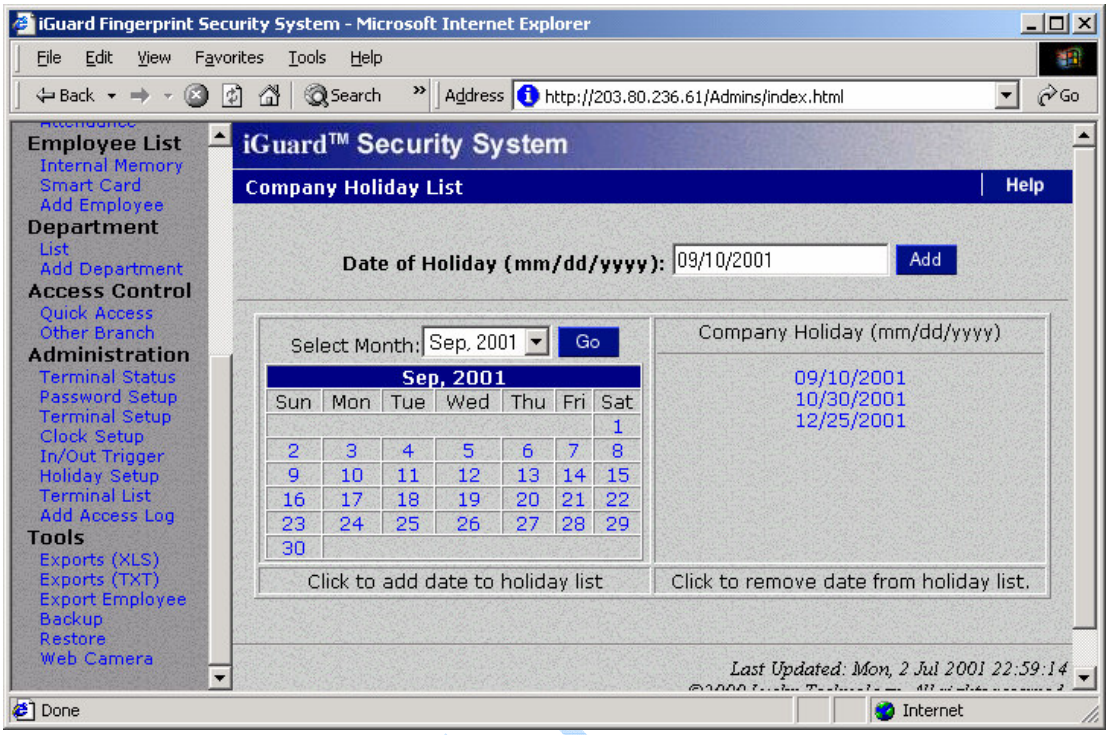
Le statut par défaut Entrée / Sortie est montré sur l'écran LCD de l'appareil comme suit :

Description	***Affichage Ecran***
Entrée par Défaut (position pour Chronométrage Entrée).	`Lundi 30 13:49` `ID#_ Entrée`
Sortie par Défaut (position pour Chronométrage Sortie).	`Lundi 30 13:49` `ID#_ Sortie`

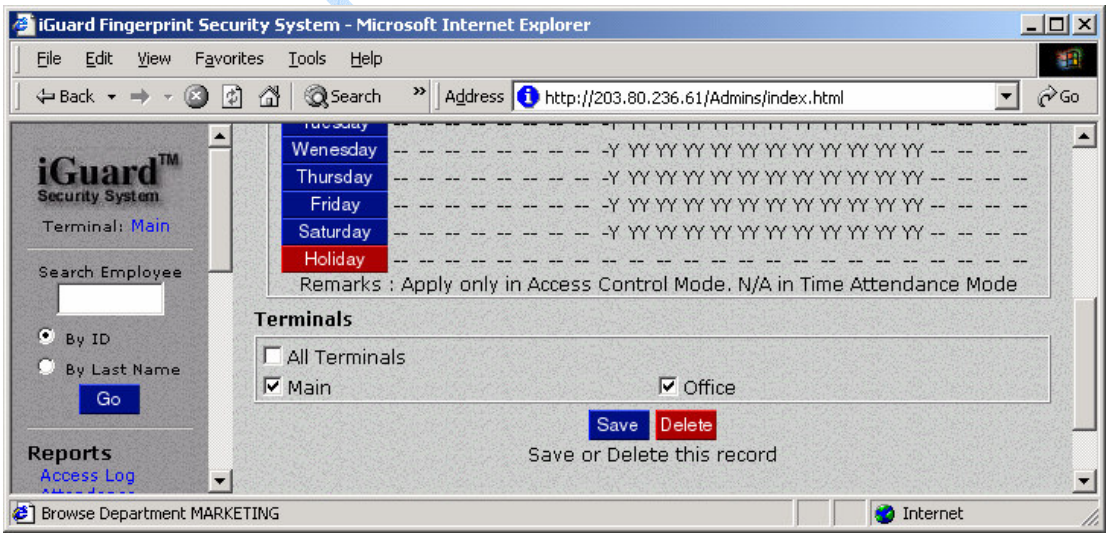
L'utilisateur peut ignorer le paramètre par défaut en appuyant sur la touche d'espacement arrière avant l'entrée l'ID utilisateur.

4.12. Administration – Installation Congés

La "liste des Jours de congés" est employée pour paramétrer les restrictions d'accès (avec les restrictions des jours de semaine).



Dans le susdit exemple de dates, 10/09/2001, 30/10/2001 et 25/12/2001 sont mis comme des vacances. Ces jours, le temps autorisé suivra les restrictions pour la date " Jour de congé, comme indiqué dans l'écran suivant: -

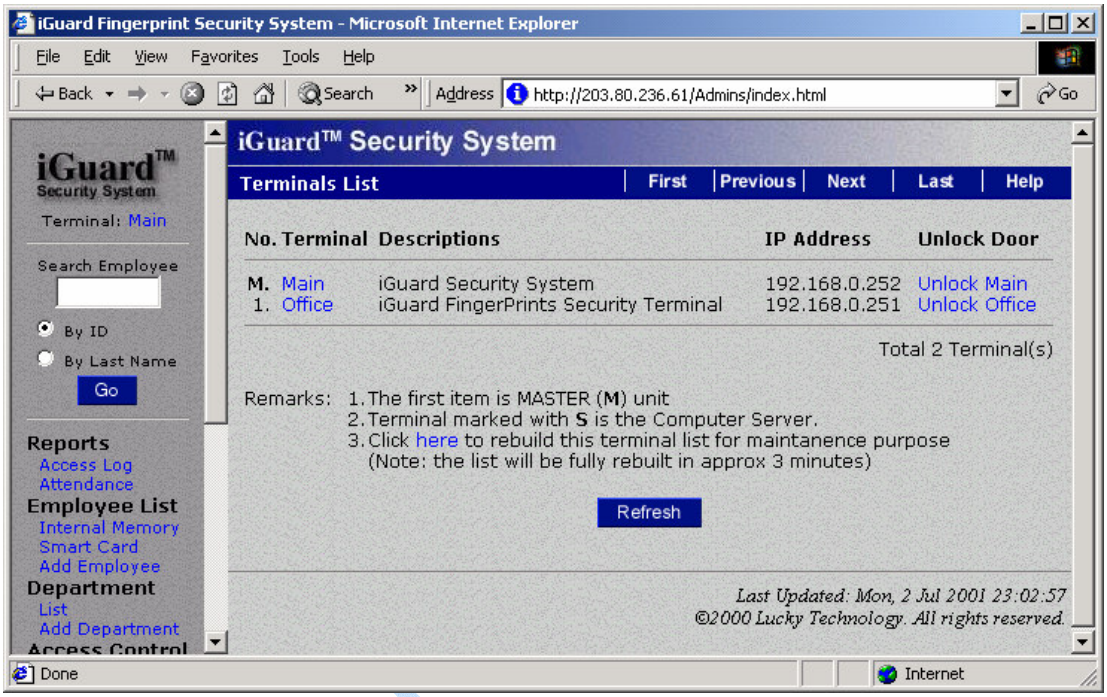


Comme indiqué dans la susdite page, tous les employés appartenant au département Marketing ne seront pas autoriser sur les trois jours de vacances indiqués.

Attribuez s'il vous plaît à la section "Liste des Départements " ci-dessus comment changer les paramètres de restriction de temps.

4.13. Administration – Liste des Terminaux

Cette page montre les dispositifs esclaves actuels dans un réseau en mode maître / esclave



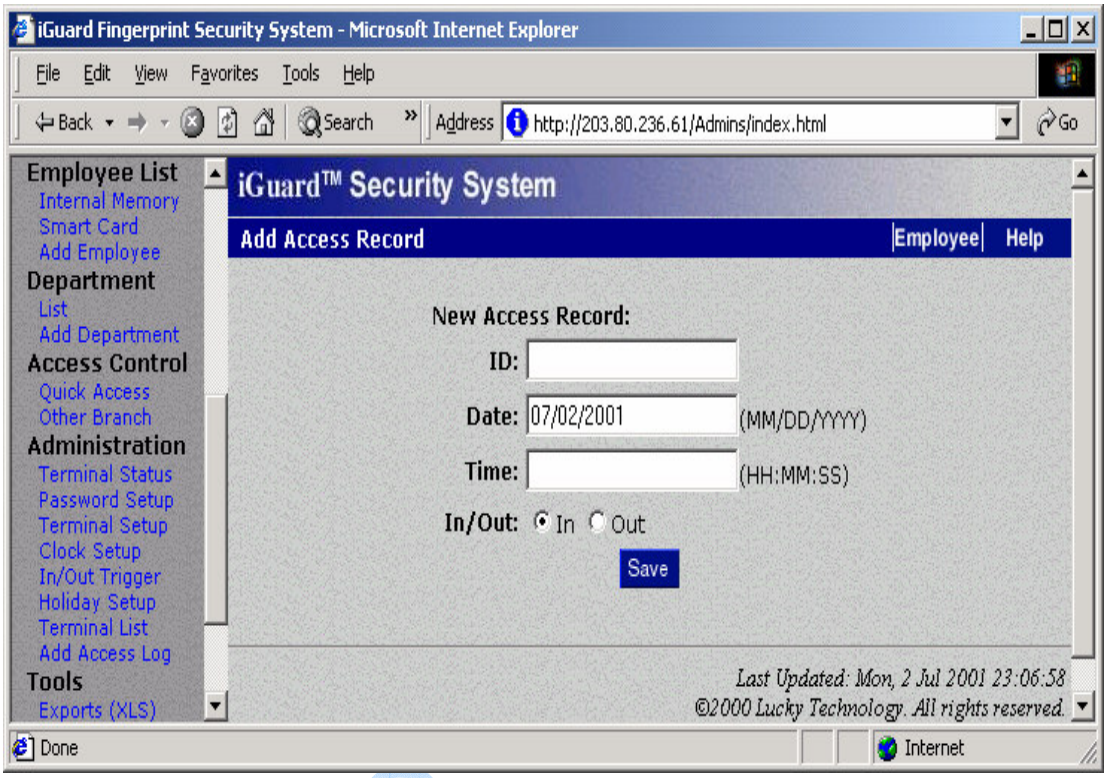
Dans le susdit exemple, le dispositif "Principal" est l'unité de maître et il a une unité esclave nommée "Bureau".

L'adresse IP correspondant à chaque appareil est également montrée

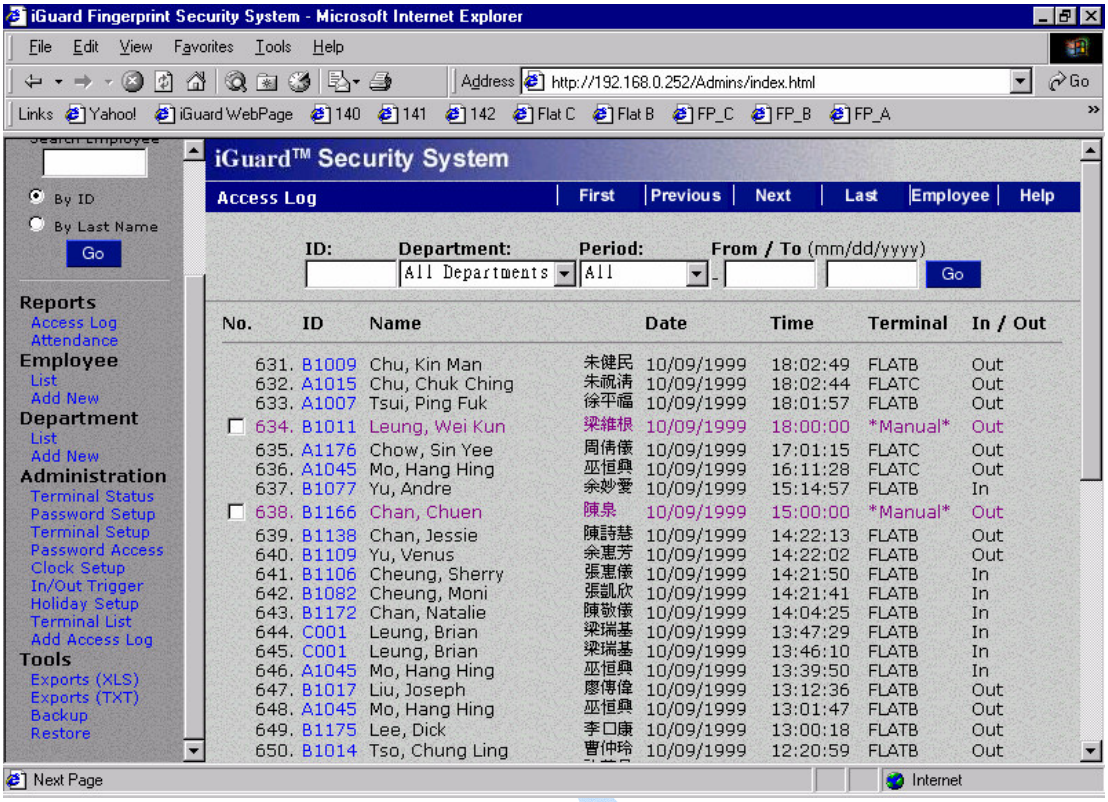
Comme particularité, vous pouvez à distance ouvrir les portes en cliquant sur Ouverture Principal et/ou Ouverture Bureau, et aussi effectuer une remise à zéro de l'un ou l'autre des terminaux.

4.14. Administration – Ajout de rapports d'accès

Par défaut, tous les rapports d'accès ne peuvent ni être changés, ni effacés. Cependant, vous pouvez ajouter un rapport d'accès pour un employé qui oublierait. Cette particularité est d'habitude exigée seulement pour les feuilles d'émargement



Un rapport d'accès ajouté manuellement est montré de manière différente. Il est montré comme suit: -



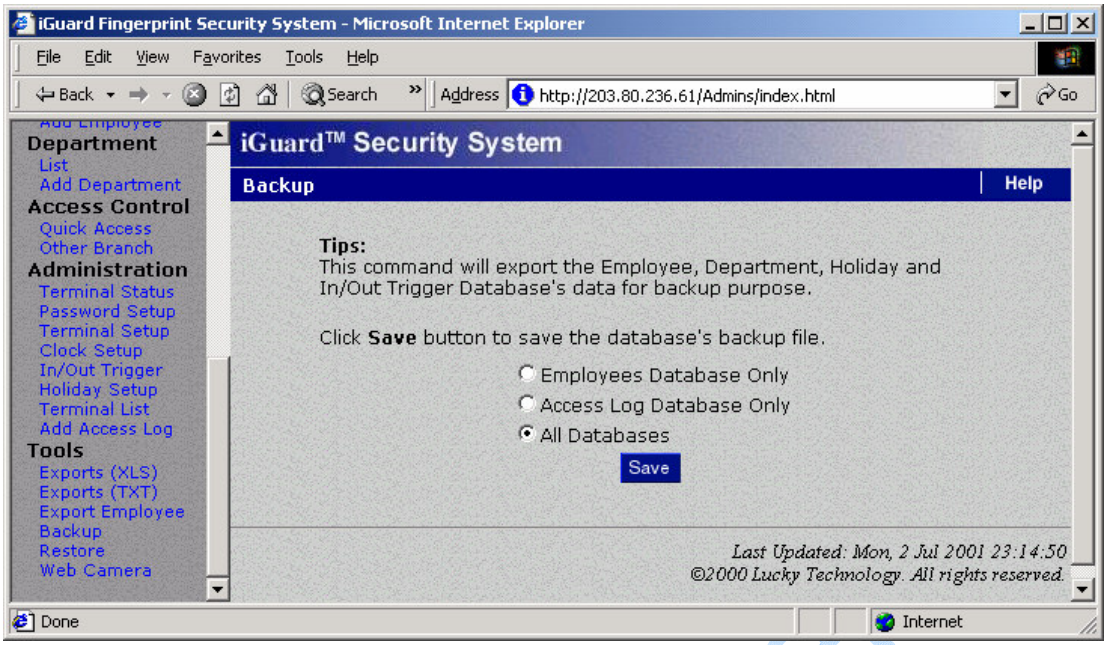
Les rapports de couleur rose avec la case à cocher à côté d'eux indiquent que ces rapports ont été ajoutés manuellement. Vous pouvez plus tard supprimer ces rapports en cochant la case et en appuyant ensuite sur le bouton Supprimer au fond de la page.

4.15. Outils - Export Employé

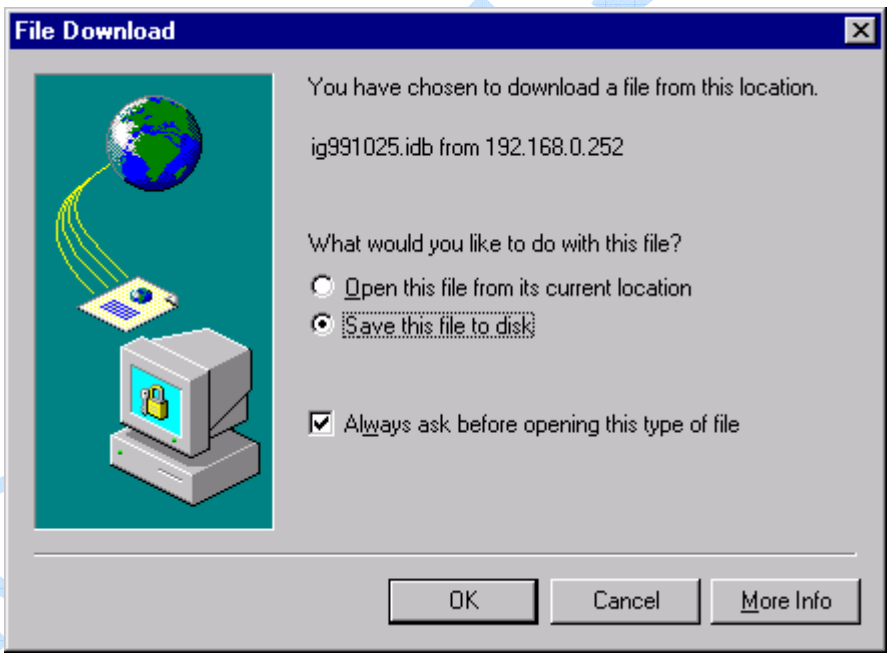
Sélectionner “Export Employé” pour exporter un employé ou un groupe d’employés par ID

4.16. Outils - sauvegarde & restauration

Il est suggéré de sauvegarder les données internes périodiquement à l'ordinateur de bureau (comme une sauvegarde quotidienne). Dans l'éventualité peu probable que le système doivent être remplacé, les anciennes données peuvent être reconstituées sur le nouveau dispositif et les employés n'ont pas à être ré inscrits de nouveau.

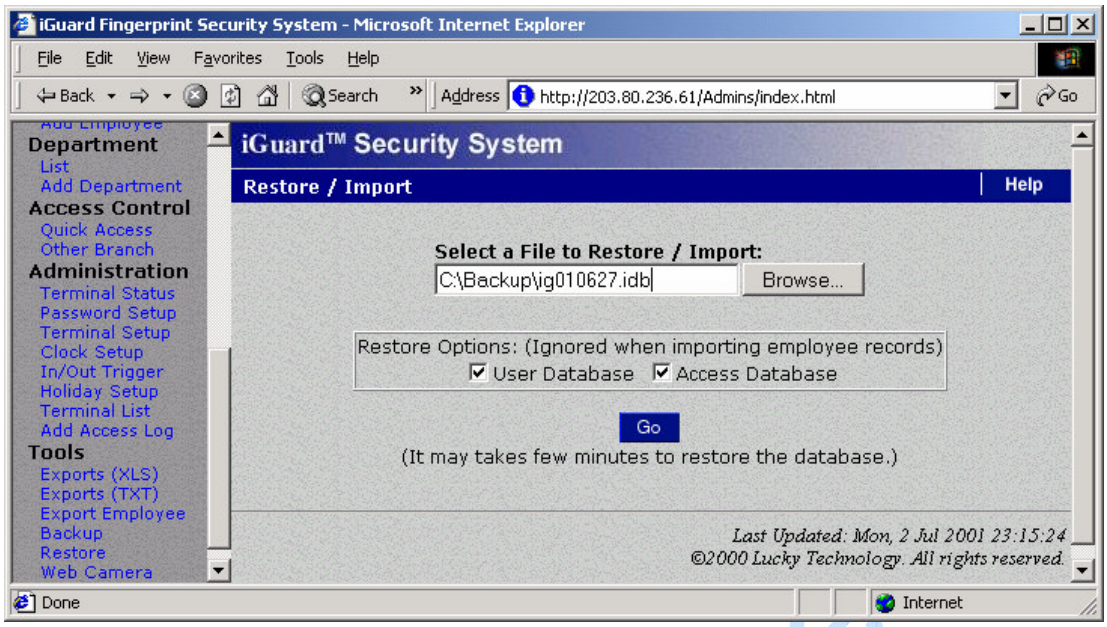


Presser le bouton **Sauvegarde**, et une boite de dialogue comme celle-ci dessous apparaît :



Presser le bouton **OK** pour sauvegarder les données sur votre ordinateur

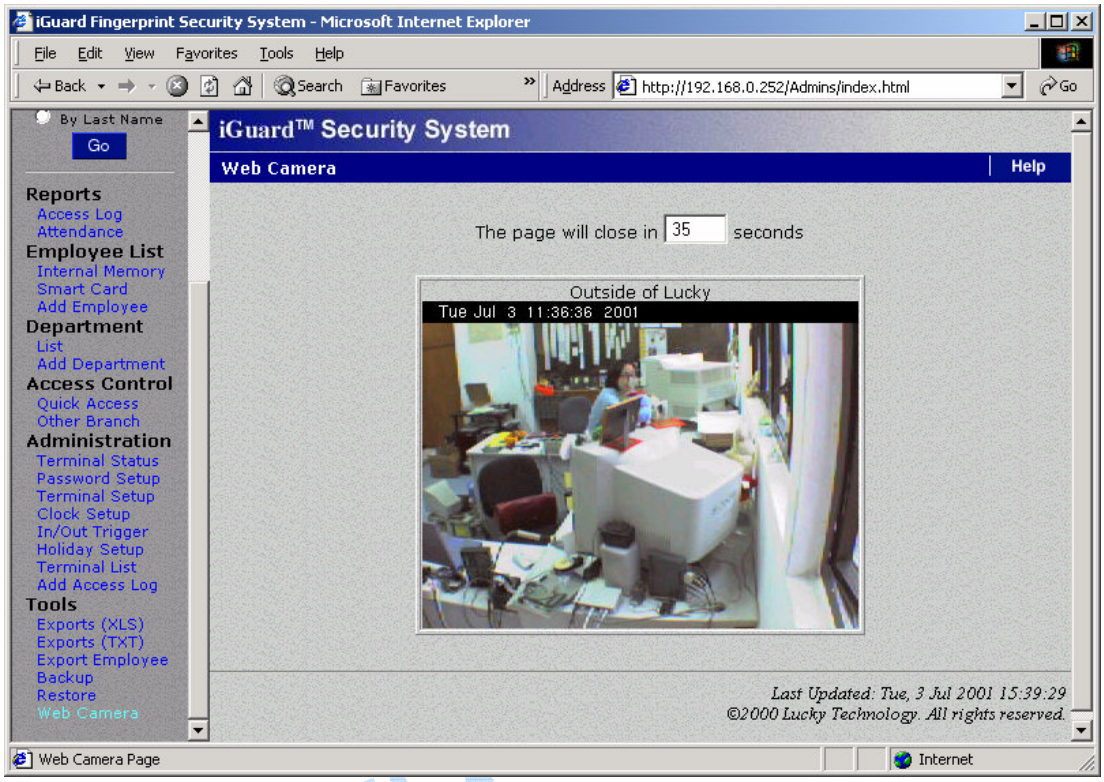
Quant il est nécessaire de restaurer les données (par exemple, un nouvel appareil à été installé), aller à la page RESTAURER et spécifier le nom de dossier comme suit :



Presser le bouton **Go** et les fichiers de données seront restaurés sur le nouvel appareil.

4.17. Outils - Camera Web

Si une caméra Web est disponible sur le réseau, iGuard peut faire suivre l'image de la caméra au navigateur comme indiqué ci-dessous: -



Actuellement la seule caméra web soutenue est *Axis 2100 Network Camera* et la caméra de JVC.

<file:///C:\Documents%20and%20Settings\Dexter\®à±\LM_Manual\print\ig_tools_webcam.html > jusqu'à quatre caméras Web peuvent être soutenues en même temps et montrées dans la même page.

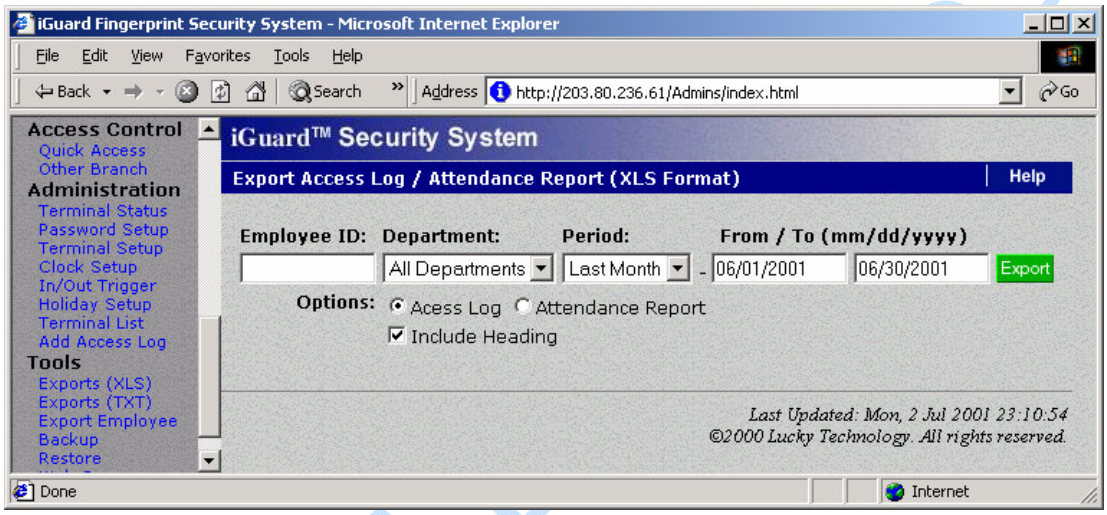
Référez vous à la section "Administration - Installation Terminal" pour plus de détails dans l'installation des caméras web.

http://www.axis.com

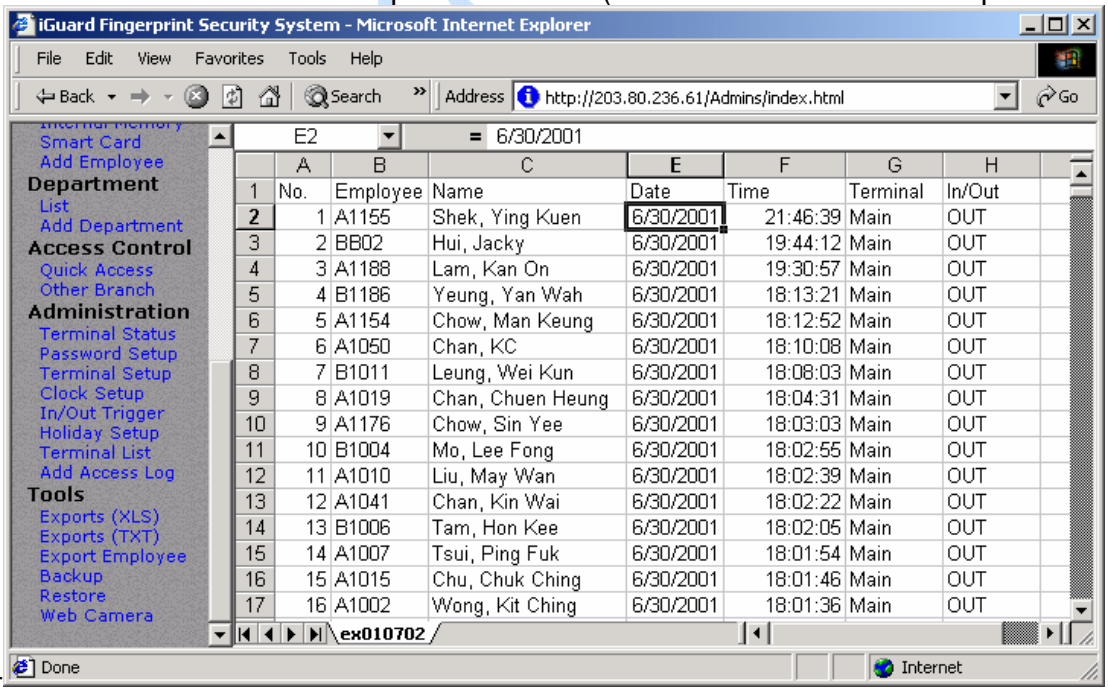
5 RAPPORTS

5.1. Outils Export (XLS)

Les rapports (incluant le Rapport d'Accès et le Rapport de gestion de présence) peuvent être exportés directement dans le format de XLS, qui permet l'intégration avec des applications de bureau comme Microsoft Excel. Des rapports divers peuvent alors être facilement produits employant les particularités incorporées de l'application de bureau. De cette façon, les sociétés peuvent concevoir leurs propres formats de rapport qui sont les meilleurs appropriés à leurs opérations existantes.



L'écran suivant est un exemple du résultat (avec Microsoft Internet Explorer 5.0):



5.2. Outils - Exports (TXT)

Le FICHIER TEXTE est utile pour l'exportation aux programmes de feuille d'émargement existants employés en société.

Le format du fichier texte est comme suit:

" N° "," Employé ID "," Nom "," Autre Nom "," Date "," Temps "," Terminal "," Entrée / Sortie "

"1","A1155","Shek, Ying Kuen","admin","09/30/1999","20:02:04","F1103","Out"

"2","B1077","Yu, Andre","account","09/30/1999","19:58:58","FLATB","Out"

"3","C001","Leung, Brian","director","09/30/1999","19:58:50","FLATB","Out"

"4","B1166","Chan, Chuen","support","09/30/1999","19:56:45","FLATB","Out"

"5","A1174","Go, Kai Yin","engineer","09/30/1999","19:52:30","F1103","In"

"6","B1082","Cheung, Moni","engineer","09/30/1999","19:21:05","FLATB","Out"

"7","B1011","Leung, Wei Kun","manager","09/30/1999","19:06:18","FLATB","Out"

"8","B1067","Lau, Ester","engineer","09/30/1999","18:58:11","FLATB","Out"

"9","A1154","Chow, Man Keung","assistant","09/30/1999","18:36:48","F1103","Out"

"10","A1050","Chan, KC","support","09/30/1999","18:20:59","FLATB","Out"

"11","A1002","Wong, Kit Ching","shipping","09/30/1999","18:19:07","F1103","Out"

5.3. Rapports – Enregistrements d'Accès

Cliquer sur la ligne **Enregistrement Accès** sur le panneau gauche et vous verrez quelque chose de similaire à l'écran suivant :

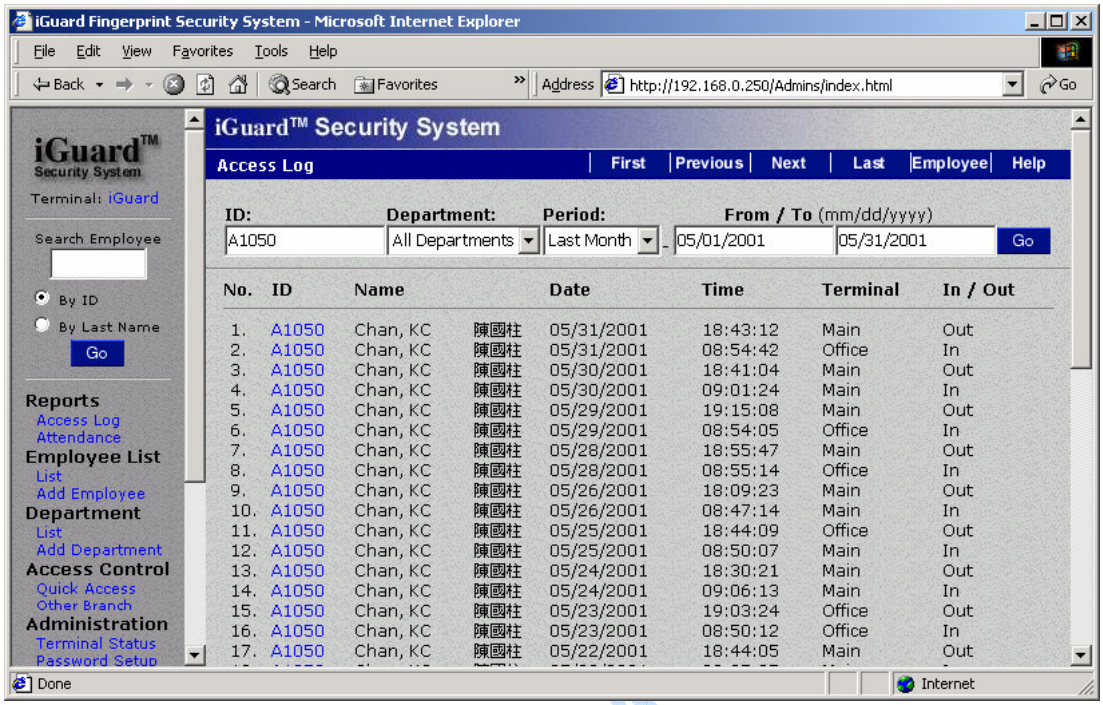
Cette page montre les "Enregistrement d'Accès" des employés. Si vous voulez voir les enregistrements d'une personne en particulier (e.x, C001), entrer son N° ID dans la boite d'édition et presser le bouton **Go**, Et le navigateur montrera seulement les rapports de cette personne.

Vous pouvez aussi spécifier le Département, et seulement les membres de ce département seront affichés.

La Période de temps peut aussi être limitée, qui montrerait seulement les rapports indiqués. Vous pouvez aussi spécifier la Période en choisissant la période choisie et en l'entrant directement dans les champs "de / à".

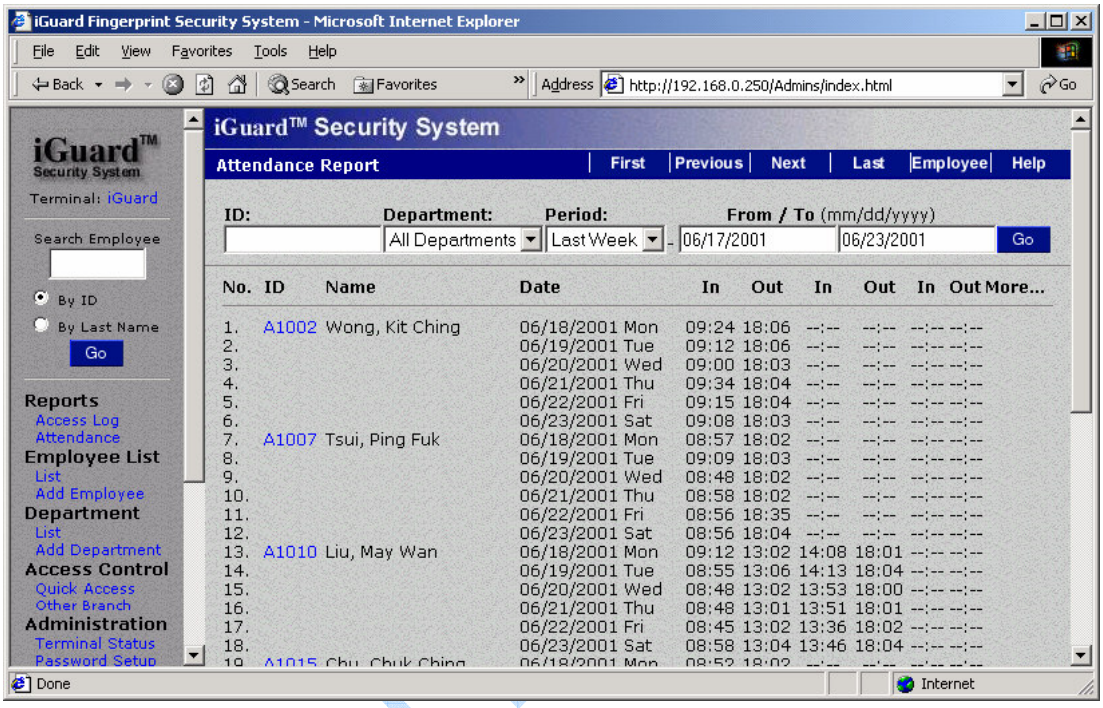
Pour examiner les rapports, comme pour appeler la page suivante, pressez sur le bouton "Suivant" dans la barre navigation au sommet de la page, ou aller à n'importe quelle page particulière en cliquant sur le numéro de page au fond.

L'exemple suivant montre les rapports du mois précédent de l'employé N° ID: A1050



5.4. Rapports – Présence

Les rapports de gestion de présence fournissent des enregistrements d'accès consolidés comme suit: -



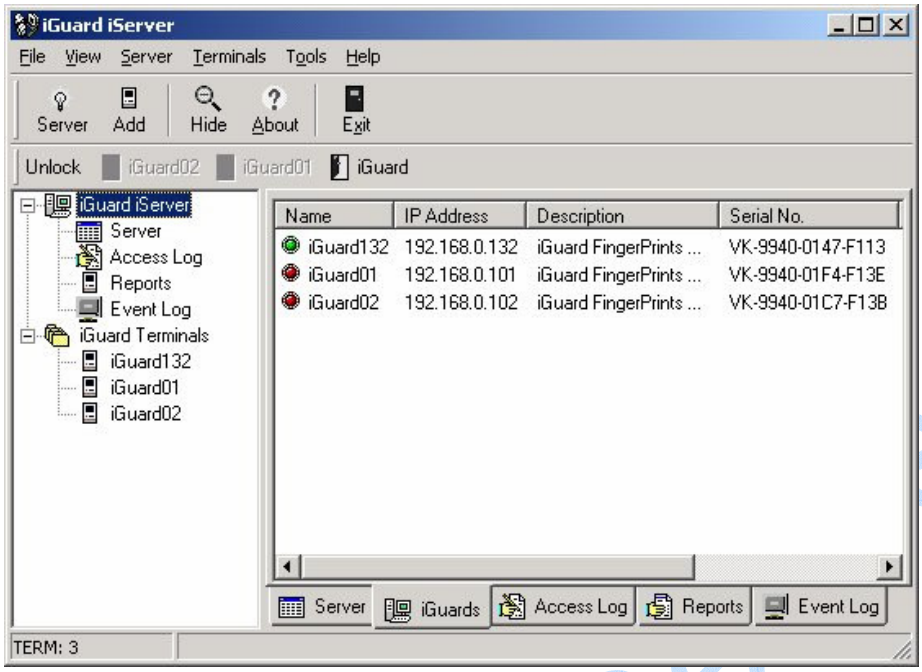
***Entrée / Sortie quotidienne

Le rapport de présence est particulièrement utilisé pour la gestion de la paye. Semblable au rapport de mouvements d'Accès, vous pouvez spécifier l'ID de l'employé et / ou la période du rapport de gestion de présence.

5.5. Serveur Internet

Le serveur Internet est basé sur le programme Windows pour rassembler des rapports de transaction d'iGuard et les sauvegarder sur le format de base de données ODBC. Le Serveur Internet utilise par défaut Microsoft Access.

Si vous voulez employer des bases de données conformes à ODBC autre que MS ACCESS, vous devez faire les choses suivantes pour arriver à connecter le Serveur Internet aux base de données. La syntaxe est soumise à la base de données que vous avez.



Création de Bases de Données

Vous devez créer une base de données et créer 2 tables. Nous avons des exemples de 2 sortes de bases de données

La Structure de Table par défaut est MS ACCESS (ibonussrv.mdb) :

5.5.1. MS Access

Table: Mouvements d'accès

RCDID Int AUTO_INCREMENT,

ID Employé caract (16),

Date caract (10),

Heure caract (10),

ID Terminal caract (20),

Entrée / Sortie Int,

Clef Primaire (RCDID, ID Employé, Date, Heure, ID Terminal)

Table: Employé

ID Employé caract (16),

Nom caract (40),

Prénom caract (40),

Titre caract (40),

Mot de Passe caract (16),

Statuts Emp Int,

Numéro Minutie1 Int,

Numéro Minutie2 Int,

Dossier Photo caract (40),

Image Minutie1,

Image Minutie2,

Photo image,

Département caract (50),

Clef Primaire (ID Employé)

Il y a quelques différences de syntaxe pour créer la table dans d'autre base de données comme le Serveur SQL et Oracle. La suite est pour vous la référence.

5.5.2. SQL Serveur

Table: Mouvements d'Accès

RCDID Int IDENTITE Oui,

ID Employé caract (16),

Date caract (10),

Heure caract (10),

ID Terminal caract (20),

Entrée / Sortie Int,

Clef Primaire (RCDID, ID Employé, Date, Heure, ID Terminal)

Table: Employé

La même syntaxe que MS Access

La base de données créée dans le Serveur SQL doit avoir un établissement de la connexion pour avoir accès aux tables. Voir l'étape "créer le DSN" plus loin.

5.5.3. Oracle

Table: Mouvements d'Accès

Nombre RCDID (38) Pas Nul, <- Contraint – Auto incrémentation

ID Employé Caract (16) Pas Nul,

Date Caract (10) Pas Nul,

Heure Caract (10) Pas Nul,

ID Terminal Caract (20) Pas Nul,

Nombre Entrée / Sortie (38)

Table: Employé

ID Employé Caract (16) Pas Nul,

Nom Caract (40),

Prénom Caract (40),

Titre Caract (40),

Mot de Passe Caract (40),

Statuts Emp Nombre (38),

Numéro Minutie1 Nombre (38),

Numéro Minutie 2 Nombre (38),

Dossier Photo Caract (40),

Minutie1 BLOB,

Minutie2 BLOB,

Photo BLOB,

Département Export 2(50)

Il a beaucoup de méthode pour créer une table dans Oracle et faire le champ d'incrémentation automatique (RCDID). La méthode suivante est la plus commune.

Pour créer une table Oracle :

1. a) Vous pouvez employer les outils d'administration dans Oracle pour la manipulation de table si vous employez la version 8 ou plus, ou;
   b) Vous pouvez employer la commande de sql pour créer la table dans sql plus la feuille de calcul ou sql.

1. pour créer un champ d'auto incrémentation (RCDID):
   a) Créer un ordre et ajouter un constant à un champ, ou;
   b) Créez une détente pour incrémenter le champ.

Comme le Serveur SQL, vous devez avoir un établissement de la connexion pour la base de données. Vous devez vous assurer le nom d'utilisateur et le mot de passe soient corrects et le nom d'utilisateur doit avoir le droit d'accès au mouvement d'accès et à l'Employé. Vous devez être conscient que les utilisateurs dans Oracle ont leur propre droit d'accès à la table. Si vous ne nommer pas d'utilisateur et de mot de passe, vous ne pourrez pas entrer dans la base de données d'Oracle. Si votre nom d'utilisateur n'a pas de droit d'accès à la table, vous ne pourrez rien faire à cette table, vous ne pourrez pas vous connecter à la base de données d'Oracle. Après l'établissement de la connexion pour la base de données, vous pouvez l'évaluer comme suit.

Test (Option):

1) Utilisation de SQL Plus à l'établissement de la connexion comme même utilisateur nomme et même mot de passe que dans le Serveur Internet.
2) Sélectionner et insérer la déclaration à cette table dans le SQL Plus.

5.5.4. Créez Nom de Source de Données (DSN)

Dans Panneau de Contrôle -> outils Administratif -> ODBC -> Système DSN -> Ajouter

Pour le Serveur SQL et la base de données Oracle, ces procédures sont similaires.

Indiquer le Nom de Source de Données par défaut "Serveur Internet".

Pour la base de données de Serveur SQL, vous pouvez employer le nom d'utilisateur d'établissement de la connexion, dire "sa" qui a un privilège le plus grand et le mot de passe pour créer le DSN.

Pour Oracle, vous pouvez essayer de choisir le driver “Orahome” si vous avez et c'est la voie du succès pour notre client

Finalement, quand vous commencez le "Serveur internet" c'est un excellent travail. Quand vous employez la base de données ODBC compatible autre que MS ACCESS, vous ne voulez pas créer MS ACCESS quand il vous y a incité pour la première connexion.

6 MAÎTRE-ESCLAVE /SUPER MAÎTRE

6.1 Mode Maître et Mode Esclave

Dans un environnement de multi dispositif où plus d'un dispositif iGuard sont connectés au même réseau d'entreprise, un dispositif est assigné comme le dispositif Maître et tout les autres sont assignés comme les dispositifs Esclave.

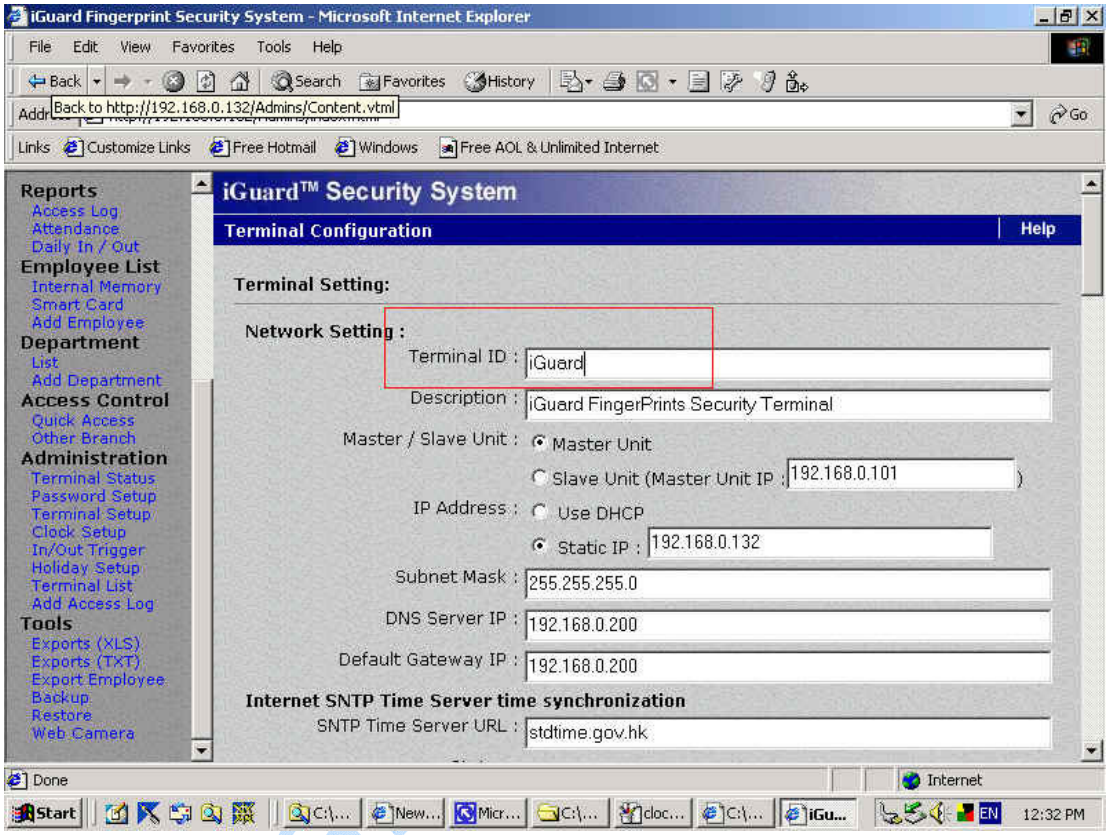
Avant qu'une personne ne puisse être identifiée, la personne doit soumettre son échantillon d'empreinte digitale au système, mieux connu comme "inscription d'empreinte digitale". Cela peut être fait dans n'importe quel dispositif, Maître ou Esclave. Les données de l'utilisateur seront alors automatiquement reproduites à tous les autres dispositifs. Autrement dit, une fois que vous vous êtes inscrits dans le dispositif Maître, votre information d'empreinte digitale est aussi disponible dans tous autres dispositifs esclave (et vice-versa) et vous pouvez avoir accès à chacun de ces dispositifs, tant que vous avez les niveaux d'accès appropriés.
Tous les rapports d'accès et les enregistrements d'Heures Entrée / Sortie sont aussi automatiquement reproduits des dispositifs Esclave au dispositif Maître et donc le dispositif Maître contient toute l'information nécessaire. Donc, vous devez seulement avoir accès au dispositif Maître, employant n'importe quel navigateur Internet standard, pour obtenir tout les enregistrements d'accès et les rapports de gestion de présence du système entier sans devoir avoir accès aux dispositifs Esclave.
IGuard peut être configuré en Mode Esclave ou Maître. L'iGuard Maître et l'Esclave peuvent être logiquement connectés employant le protocole de TCP/IP. Avec un câble de RJ45 branché de votre unité iGuard à votre RÉSEAU LOCAL d'entreprise, vous pouvez connecter votre iGuard au réseau d'entreprise. Une fois que vous les avez connectés, vous devez configurer l'adresse IP des unités pour le fonctionnement, si c'est une unité Esclave, vous devez spécifier l'adresse IP de son unité de maître pour qu'il puisse retransmettre toute l'information à et du dispositif de maître.
Quand vous vous ajoutez à une unité Maître, l'unité vous donne l'accès à lui même et non aux autres départements pour des raisons de sécurité. Pour le configurer, vous devez aller sur le serveur Web par le réseau et le cliquez dans "Liste des Départements". Vous pouvez cliquer sur le département par défaut "EVERYONE". Sous "Terminaux" vous devez vous donner les droits d'accès "Tous les Terminaux" cliquez sur "Sauvegarder".

Pour synchroniser les données entre vos dispositifs, vous DEVEZ les mettre en Mode Esclave / Maître. Ci-dessous, nous avons dépeint sur comment cela peut être réalisé pour une organisation avec 3-4 dispositifs connectés dans une telle configuration.

Attention: LM séries et FPS110 séries (ancien) ne peuvent être mélangés dans le mode Maître / Esclave

6.2 Paramètres ID du Terminal

Le terminal ID de chaque iGuard doit être rebaptisé (par défaut : iGuard) avec des noms différents afin d'éviter la confusion en mode Maître / Esclave. Choisissez "Installation terminal" dans le Navigateur Internet et rebaptisez l'ID terminal en conséquence.



6.3 Super Maître

Le Super Maître, est un matériel différent, employé dans le cas ou plus de mille utilisateurs sont exigé dans un réseau en mode Maître/ Esclave
Le Super Maître sera employé comme un dispositif Maître remplaçant une norme iGuard le dispositif Maître dans le réseau. Avec le Super Maître, l'esclave iGuard fonctionnera dans le mode de cache ce qui signifie qu'ils stockent seulement les 1,000 utilisateurs les plus récemment employé dans la mémoire. Pendant l'authentification, si l'utilisateur ne peut pas être trouvé sur l'esclave, iGuard demandera le transfert l'information d'utilisateur au Super Maître via le réseau. La nouvelle information d'utilisateur sera stockée sur l'esclave iGuard et remplacera l'information d'utilisateur la plus ancienne. Notez aussi que les utilisateurs avec l'Automatch permis seront toujours stockés dans la mémoire cache.
Le maître Superbe a le serveur Web iGuard incorporé pour l'administration éloignée.

7 DIVERS

7.1 Relais de Contrôle de Porte à distance

Le relais de Porte Éloigné est employé pour la sécurité absolue pour le contrôle d'accès. Dans ce cas, le relais à l'arrière de l'iGuard n'est pas employé et le Relais de Porte Éloigné est installé à l'intérieur du bâtiment.

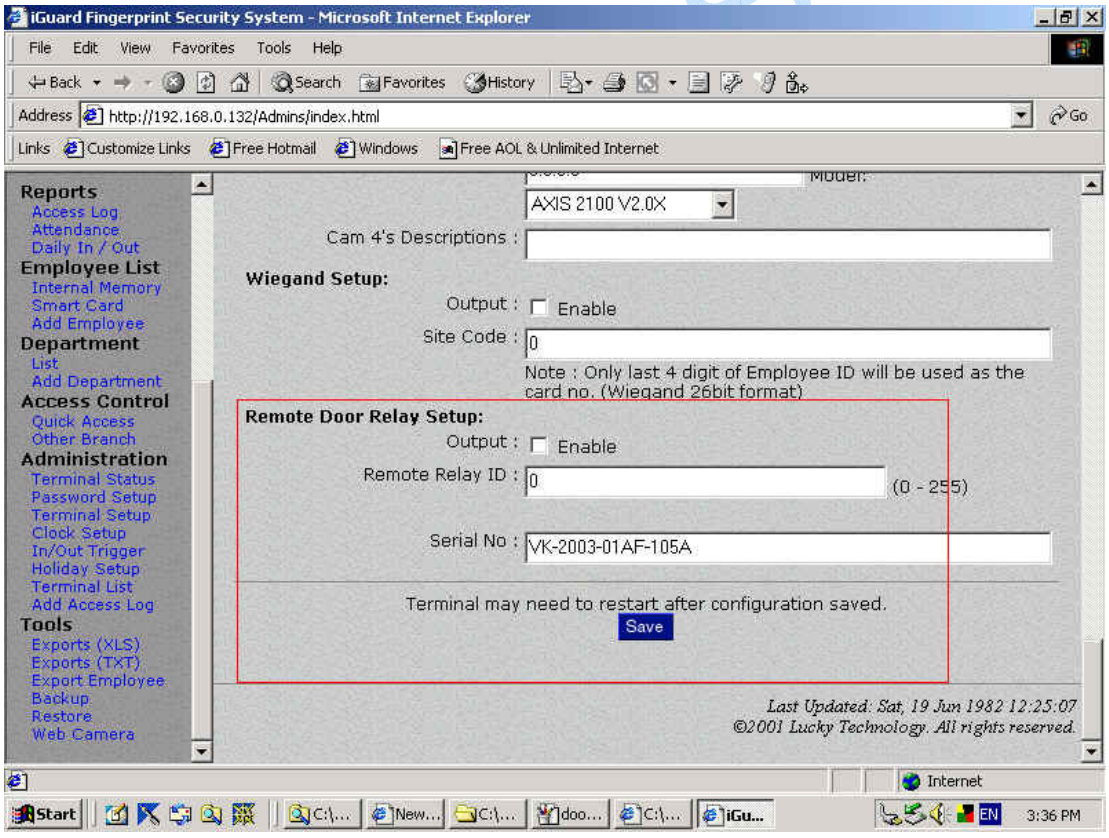
Description des connexions de Relais de Porte Éloignée:

ID	
NO	Contact porte Normalement ouvert
COM	Contact porte Commun
NC	Contact porte Normalement fermé
DOOR SW	Commutateur porte
DOOR SW	Commutateur porte
A- RS485 Connexion	Connexion iGuard
B- RS485 Connexion	Connexion iGuard
+12VDC	+12VDC
GND	Terre

Sélection Commutateur:
Tourner huit commutateurs de choix pour sélectionner le numéro d'ID. Pour le Relais Éloigné. Chaque Commutateur représente un nombre et l'ID choisi est la somme de ces nombres. Par exemple, pour mettre l'ID de la boîte de relais à 12, sélectionnez les commutateurs No 3 et 4. La table suivante montre le numéro de chaque commutateur :

Commutateur	Nombre	Exigences:
1	1	Pour employer ce tableau de Relais de Porte Éloigné, une condition spéciale d'iGuard est nécessaire. 1. Version du Programme: 3.2.9987A ou + (peut être mis à jour par le patch programme), 2. IGuard logiciel de support de Relais de Porte Éloigné. Il peut être vérifié en contrôlant la page Web des statuts de l'iGuard; "on trouvera le Relais de Porte Éloigné" dans la section "Autre Particularité". Si l'article 2 n'est pas satisfait, vous devez entrer en contact avec Lucky Technology pour obtenir une mise à niveau du matériel.
2	2	
3	4	
4	8	
5	16	
6	32	
7	64	
8	128	

Dans "Installation terminal", on doit autoriser cela.

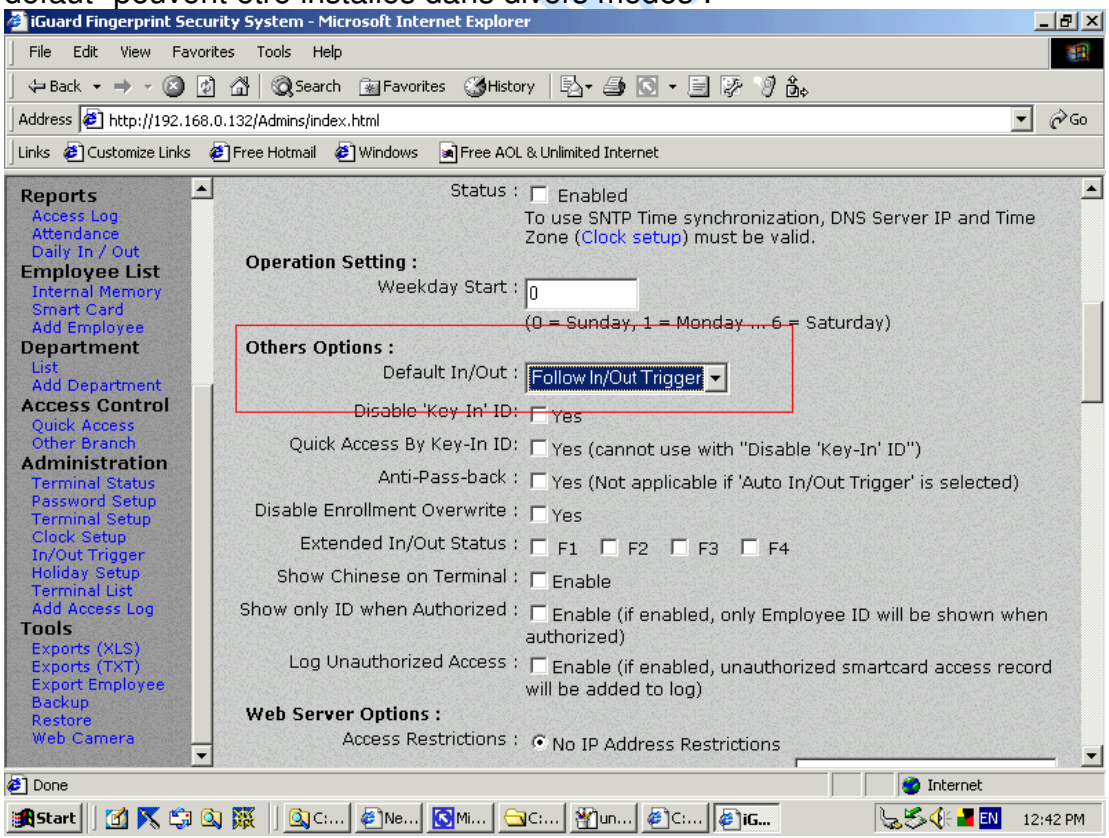


7.2 Différents Modes Entrée / Sortie

Ces fonctions ne seront pas incluses dans la LM série standard. Entrez s'il vous plaît en contact avec nos revendeurs.

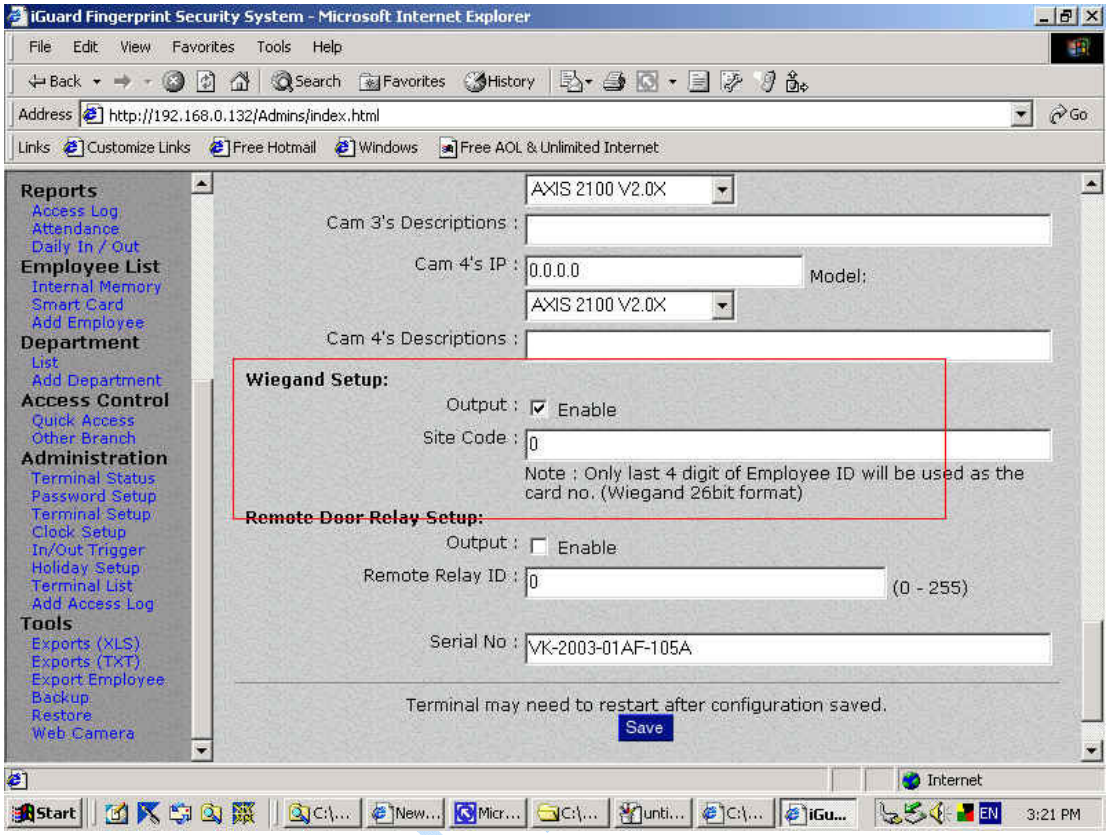
Différents Modes	Description
Suivre Bascule Entrée/Sortie (défaut)	Si cette valeur par défaut est choisie, les paramètres Entrée / Sortie seront définis dans l'installation « bascule Entrée / Sortie » (voir section Administration- Bascule Entrée/Sortie)
Toujours Sortie	Cela paramètrera iGuard et enregistrera toute la gestion de présence comme "Sortie"
Toujours Entrée	Cela paramètrera iGuard et enregistrera toute la gestion de présence comme "Entrée"
Ne pas montrer	Cela paramètrera iGuard et montrera toute la gestion de présence comme "Entrée"
Bascule Entrée/Sortie Auto	Cela basculera automatiquement entre Entrée et Sortie pour les utilisateurs.
Statuts étendus Entrée/Sortie	En plus de Entrée et Sortie, 4 labels supplémentaires F1, F2, F3 et F4 peuvent être choisis manuellement en employant le bouton < - . Dans le mouvement d'accès, on montrera ces labels en conséquence. Dans quelques applications, ces labels peuvent être employés comme le code de travail.

Choisissez "Installation terminal" dans le Navigateur Internet, "Entrée/Sortie défaut" peuvent être installés dans divers modes :



7.3 Sortie 26 bits Wiegand

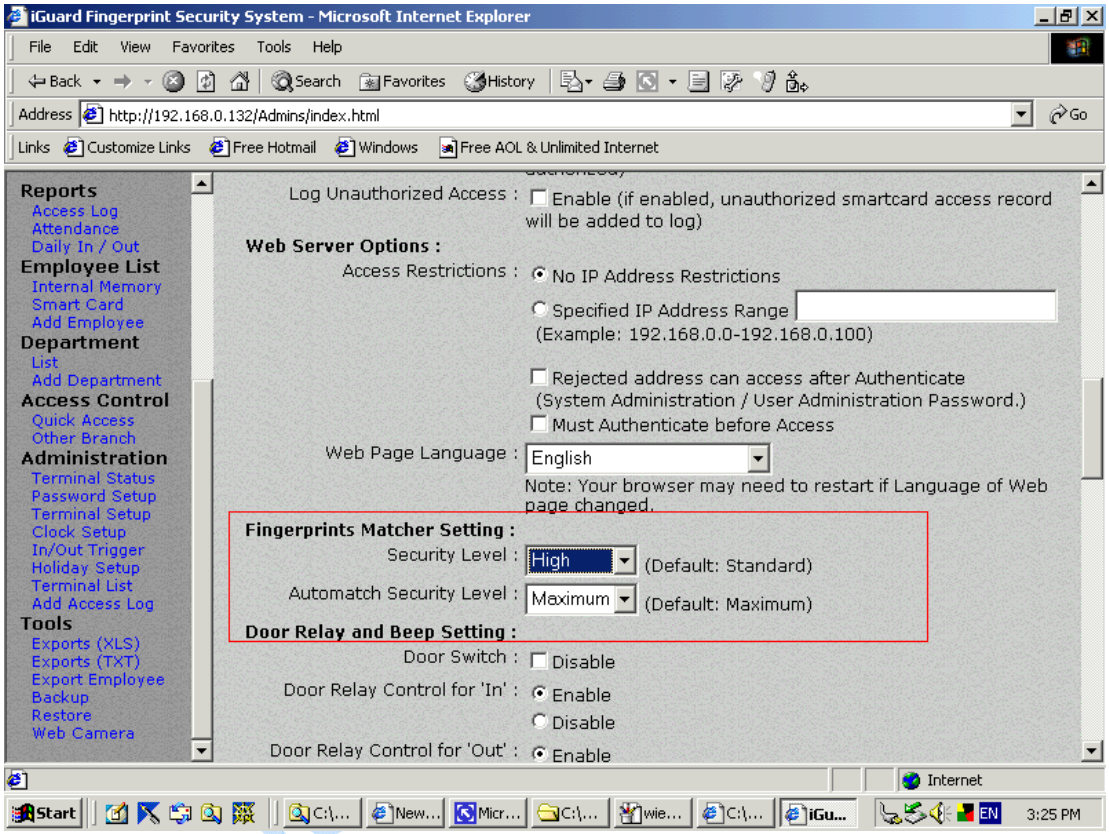
Il y a un connecteur de sortie Wiegand à l'arrière d'iGuard et on peut permettre des données au format Wiegand 26 bits l'installation terminal.



7.4 Correspondance de Sécurité entre Empreinte digitale et Automatch

Cette option permet à l'administrateur de mettre le niveau de sécurité pour la correspondance d'empreinte digitale. Mettez-la bas pour l'application normale. Si vous devez employer le dispositif où la haute sécurité est exigée, mettre cette sécurité "à haut". Cependant, il doit être noté que l'on doit attendre un taux de faux rejets plus élevés.

Aller à « Installation Terminal »

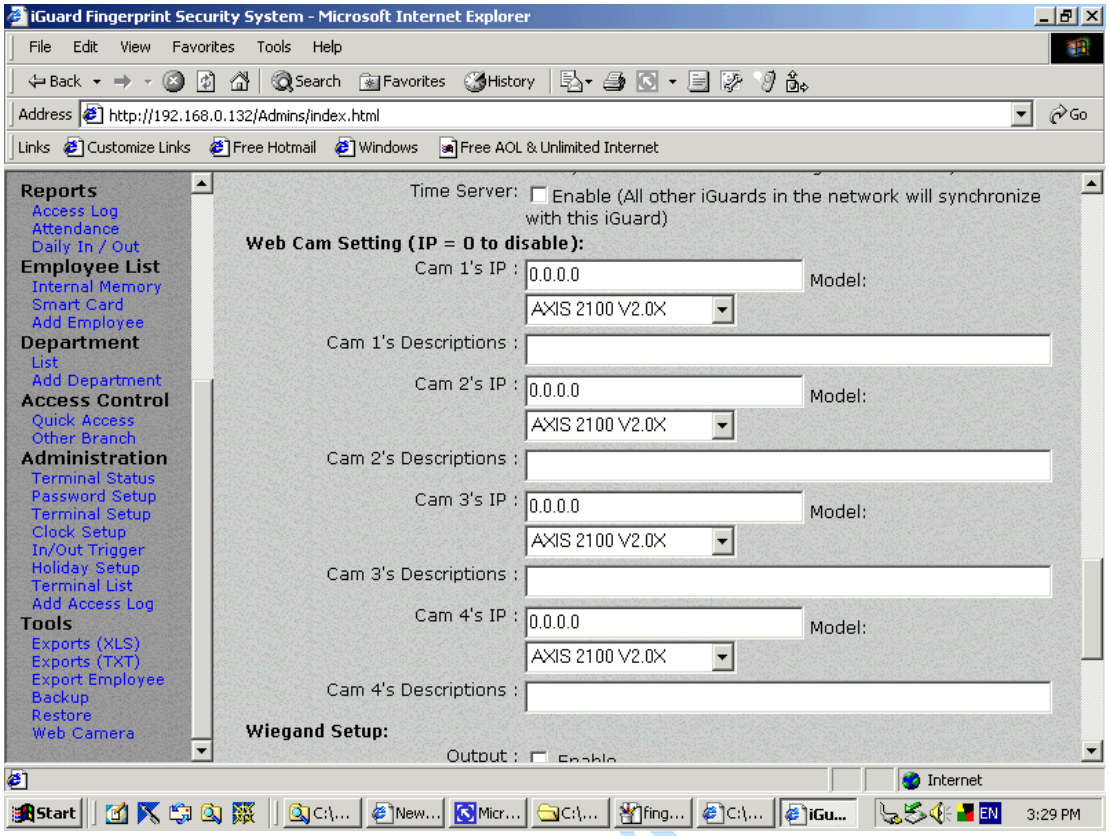


7.5 Installation de camera Web

Paramètres Web-Cam

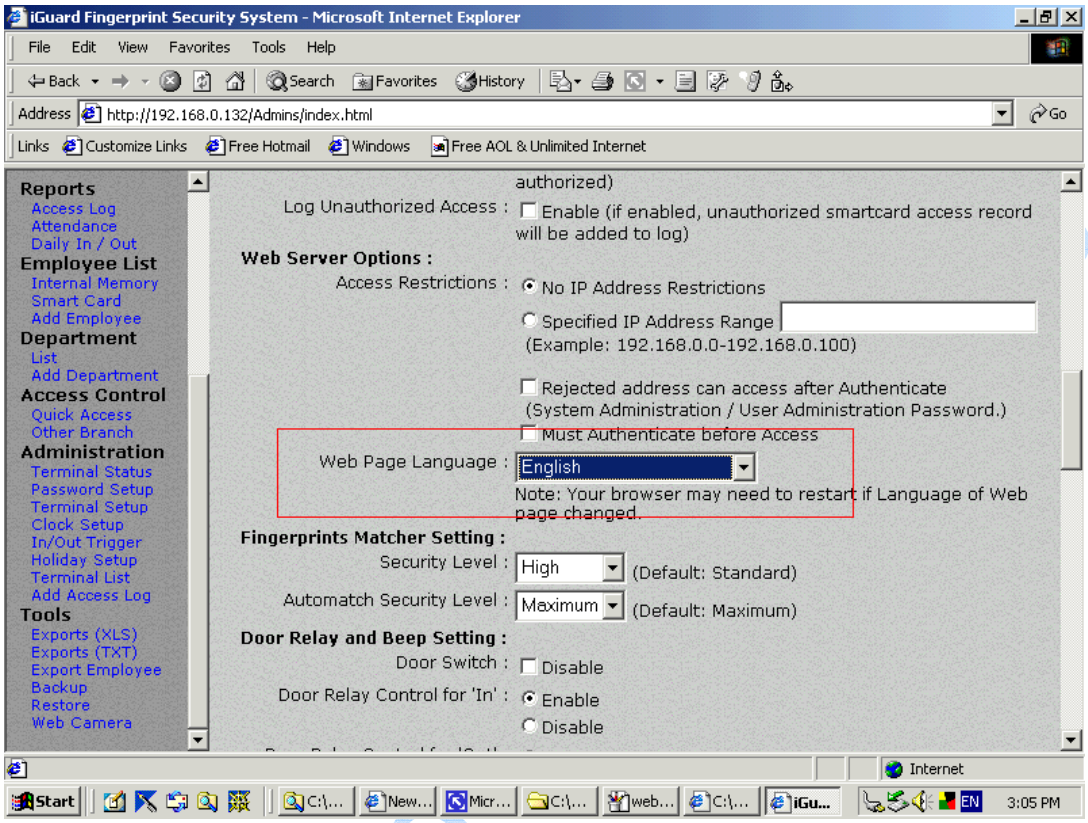
Vous pouvez employer le dispositif pour faire suivre vos images de caméra web au monde extérieur. Actuellement les seules caméras web soutenues sont *Axis 2100 Network Camera* d'*Axis Communications* et la Caméra Réseau de *JVC*. Une à quatre caméras peuvent être gérées.

Dans "Installation terminal", tapez les adresses IP des Caméras du Web et choisissez le modèle de Caméra Web.


iGuard Fingerprint Security System - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.0.132/Admins/index.html
Go
Links Customize Links Free Hotmail Windows Free AOL & Unlimited Internet
Reports
Access Log
Attendance
Daily In / Out
Employee List
Internal Memory
Smart Card
Add Employee
Department
List
Add Department
Access Control
Quick Access
Other Branch
Administration
Terminal Status
Password Setup
Terminal Setup
Clock Setup
In/Out Trigger
Holiday Setup
Terminal List
Add Access Log
Tools
Exports (XLS)
Exports (TXT)
Export Employee
Backup
Restore
Web Camera
Time Server: Enable (All other iGuards in the network will synchronize with this iGuard)
Web Cam Setting (IP = 0 to disable):
Cam 1's IP : 0.0.0.0 Model: AXIS 2100 V2.0X
Cam 1's Descriptions :
Cam 2's IP : 0.0.0.0 Model: AXIS 2100 V2.0X
Cam 2's Descriptions :
Cam 3's IP : 0.0.0.0 Model: AXIS 2100 V2.0X
Cam 3's Descriptions :
Cam 4's IP : 0.0.0.0 Model: AXIS 2100 V2.0X
Cam 4's Descriptions :
Wiegand Setup:
Output : Enable
Internet
Start
3:29 PM

7.6 Langues Pages Web

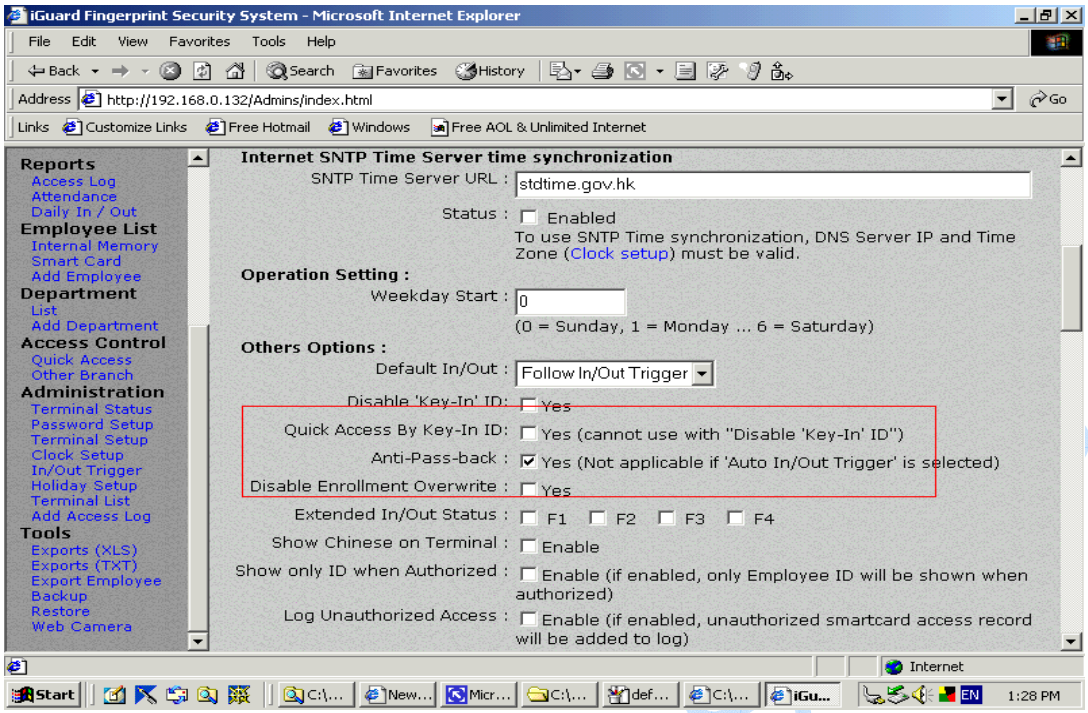
La langue employée dans les pages web d'administration peut être changée. Actuellement peu de langues sont gérées. Entrez en contact avec nos services si vous voulez incorporer vos langues.



7.7 Anti-Passback

Cette fonction n'est pas disponible dans les LM Séries standard. Contacter nos services.

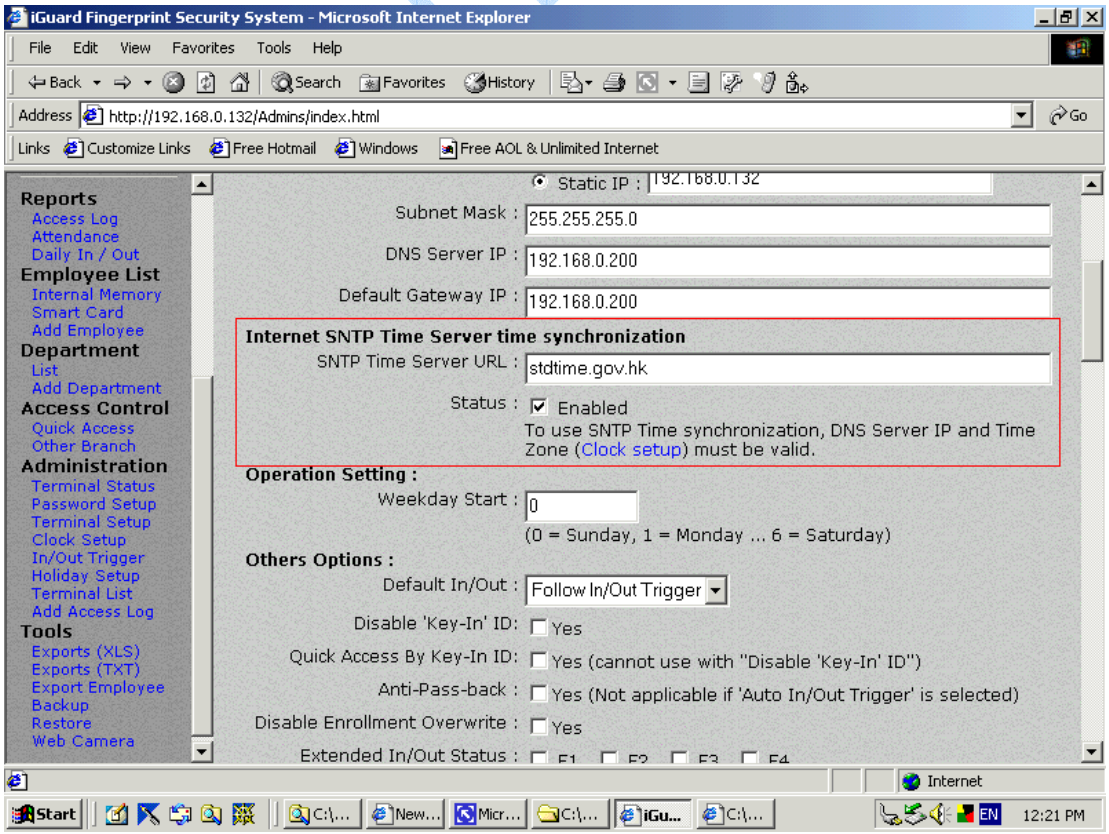
Anti-Passback	Quand permis, cette particularité empêche le même employé d'entrer deux fois dans les locaux s'il n'a pas vérifié sa sortie.



7.8 Serveur de Temps SNTP

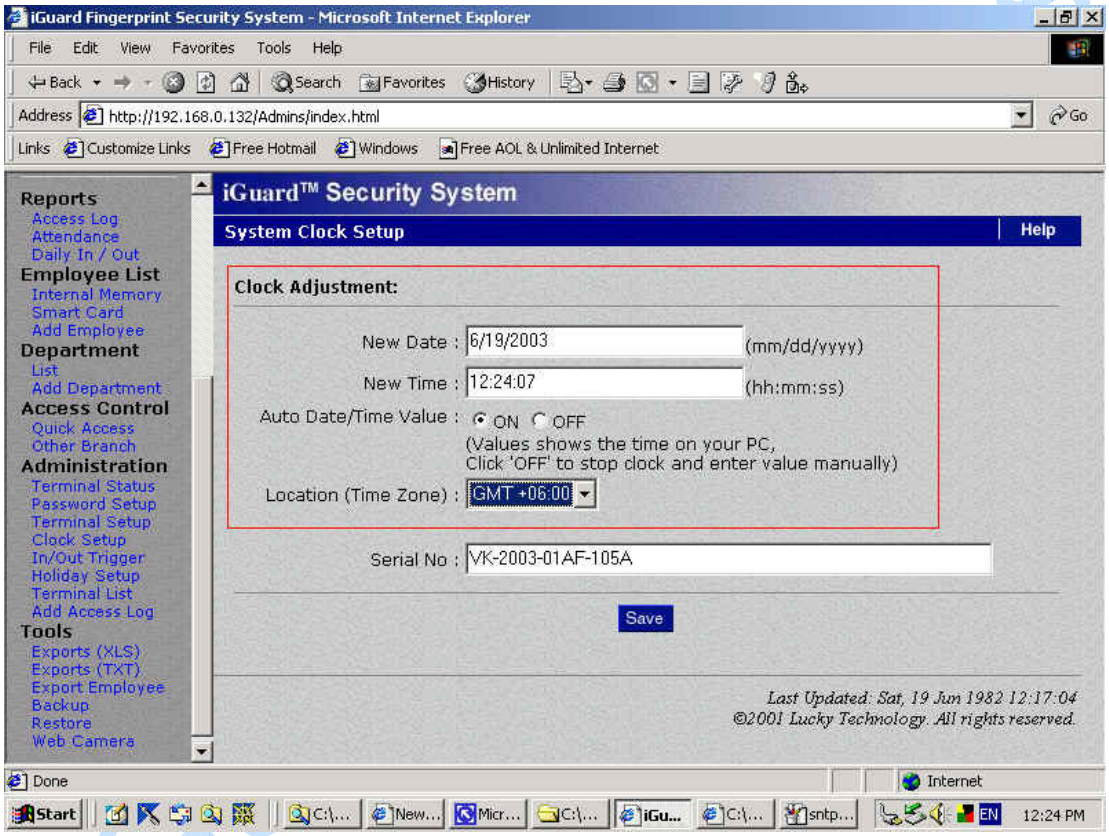
Serveur de Temps Internet SNTP de synchronisation de temps

Aller à: “Installation Terminal”:



Serveur de temps SNTP URL: Cela doit être mis au temps standard sur l'Internet. Il est représenté par l'heure de Greenwich. Pour le permettre vous devez cocher la case du Champ "Statut". Une fois que vous avez choisi cela, vous devez aller à l'Installation d'Horloge sous "Administration" et ajuster l'heure de Greenwich à votre heure locale par + /- par défaut GMT.

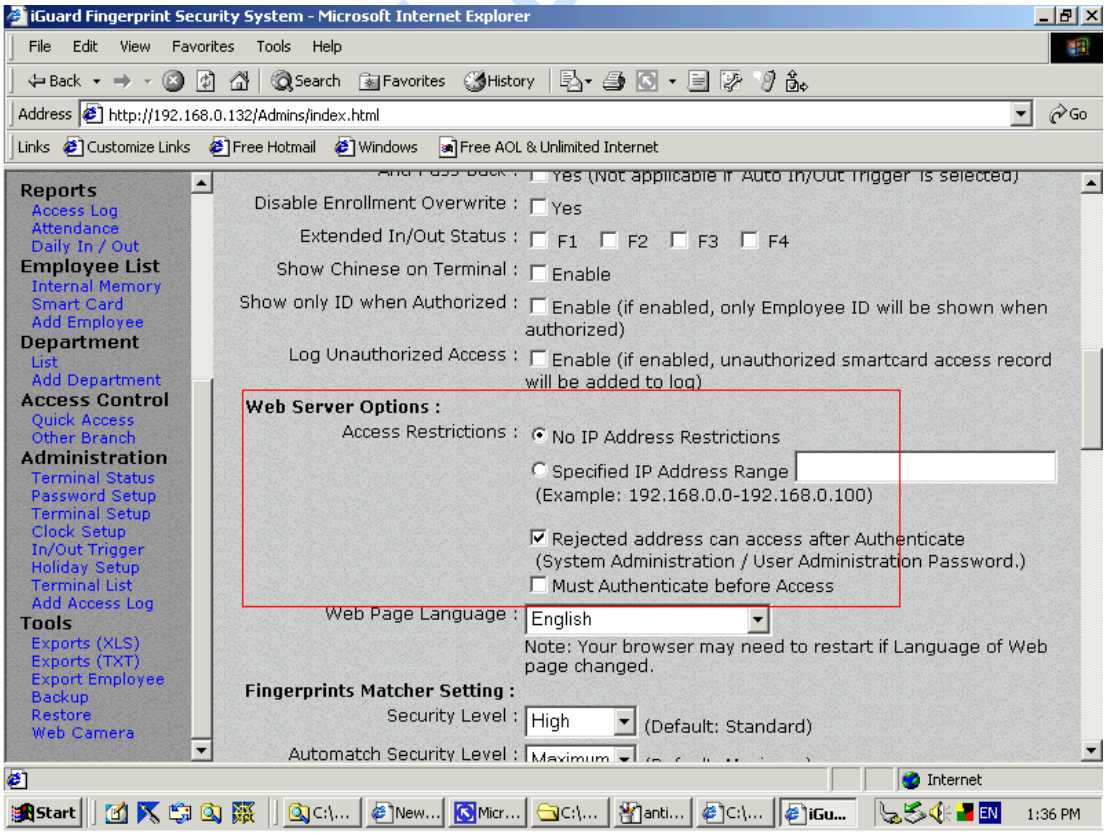
Statuts: Pour permettre le serveur de temps SNTP, vous devez vérifier cette boîte et vous assurer de paramétrer le Serveur de DNS et l'IP du Fuseau horaire sous "Installation Horloge" convenablement.



7.9 Sécurité pour Accès au Web

Installation de Sécurité pour l'Administration d'Accès au Web

Pas de restrictions d'adresse IP	Il n'y a aucune restriction pour avoir accès à la page d'administration Web de n'importe quel PC ou par n'importe quel utilisateur.
Restriction Accès	Une adresse IP ou une gamme d'adresse IP peuvent être mis avec un droit d'avoir accès à la page d'administration web. Par exemple 203.80.62.2-203.80.62.8. Le PC avec l'adresse IP différent de l'adresse IP ou la gamme d'adresses IP ne sera pas capable d'avoir accès à la page d'administration de tissu.
L'adresse rejetée peut avoir accès après authentification	Contrôlez cette case si vous voulez toujours permettre aux étrangers d'avoir accès au dispositif même si l'adresse IP est hors de la gamme indiquée comme discutée ci-dessus. Le dispositif demandera le mot de passe d'administrateur pour accorder l'accès. Il est utile si vous voulez avoir accès au dispositif à distance (comme d'un autre pays).
Doit être authentifié avant Accès	Normalement seules les pages qui impliquent le changement de la configuration et l'information des utilisateurs exigent le mot de passe. Cochez cette boîte si vous voulez configurer le dispositif pour demander le mot de passe pour toutes les pages.



7.10 Remise à zéro Dispositif

Si vous voulez effacer toute les informations d'utilisateurs et les rapports d'accès stockés dans la mémoire interne d'iGuard et remettre tous les paramètres par défaut d'usine, vous pouvez exécuter la fonction "Remise à zéro Système" pour purifier toutes les données stockées. Il y a deux bases de données à l'intérieur de l'iGuard : Base de données d'Utilisateur et Base de données d'Accès. La Base de données d'Utilisateur stocke les informations d'utilisateur, incluant les données d'empreinte digitale et les droits d'accès. Il stocke aussi l'information de département. La Base de données d'Accès stocke seulement les accès enregistrés. Il ne contient pas d'information d'utilisateur.
Vous pouvez sélectivement supprimer quelqu'un ou les deux bases de données. Cela se fait en choisissant "la Fonction 7" dans le menu Installation, comme indiqué en suivant :-

Description	***Affichage Ecran***
En mode Stand by, presser la touche Func pour entrer dans le menu Installation. Vous serez invite à entrer le Mot de Passe Administrateur (par défaut: 123) comme montré	`Entrer Mot de Passe`
Presser la touche **Func** pour continuer, Puis sélectionner la **Fonction 7** pour entrer dans le menu « remise à zéro Système ».	`Presser 7: Remise à zéro Système`
Il vous sera demandé si vous voulez effacer la base de données Utilisateurs. Entrer **1** si vous voulez effacer toutes les informations utilisateur existantes ou presser **2** pour conserver ces informations.	`Remise à zéro base Utilisateurs Oui/Non (1/2)? _`
Ensuite il vous sera demandé si vous voulez effacer la base de données d'accès. Entrer **1** si vous voulez effacer les rapports, entrer **2** si vous voulez les conserver.	`Remise à zéro rapports Accès Oui/Non (1/2)? _`
Finalement, on vous demandera alors si vous voulez remettre les paramètres par défaut d'usine. Entrez 1 si vous voulez remettre le dispositif aux paramètres par défaut d'usine (comme la réinitialisation de l'adresse IP au défaut 192.168.0.200).	`Paramètres Usine Oui/Non (1/2)? _`
Le système exécutera une remise à zéro et ensuite il retournera en mode stand-by (il prend d'habitude autour de 20 secondes).	`Lun 30 Dec 13:49 ID #:_`

Note:

Dans l'éventualité improbable ou IGuard ne fonctionne pas correctement pour des raisons inconnues, vous pouvez également employer la fonction" Remise à zéro Système » pour récupérer les rapports existants dans la machine.

7.11 Mode Test

En fonctionnement normal, iGuard enregistre toutes les transactions d'utilisateur dans ses mouvements d'Accès. Cependant, vous pouvez mettre la machine en mode Test et il mettra provisoirement hors de service la possibilité d'enregistrer les transactions. Cette particularité est utile quand vous avez fini une nouvelle inscription sur un nouvel utilisateur et vous voulez que le nouvel utilisateur pratique avec le dispositif.

Employez la "Fonction A" dans le menu Installation pour basculer entre le Mode Test et le Mode Normal comme illustré dans les étapes suivantes :

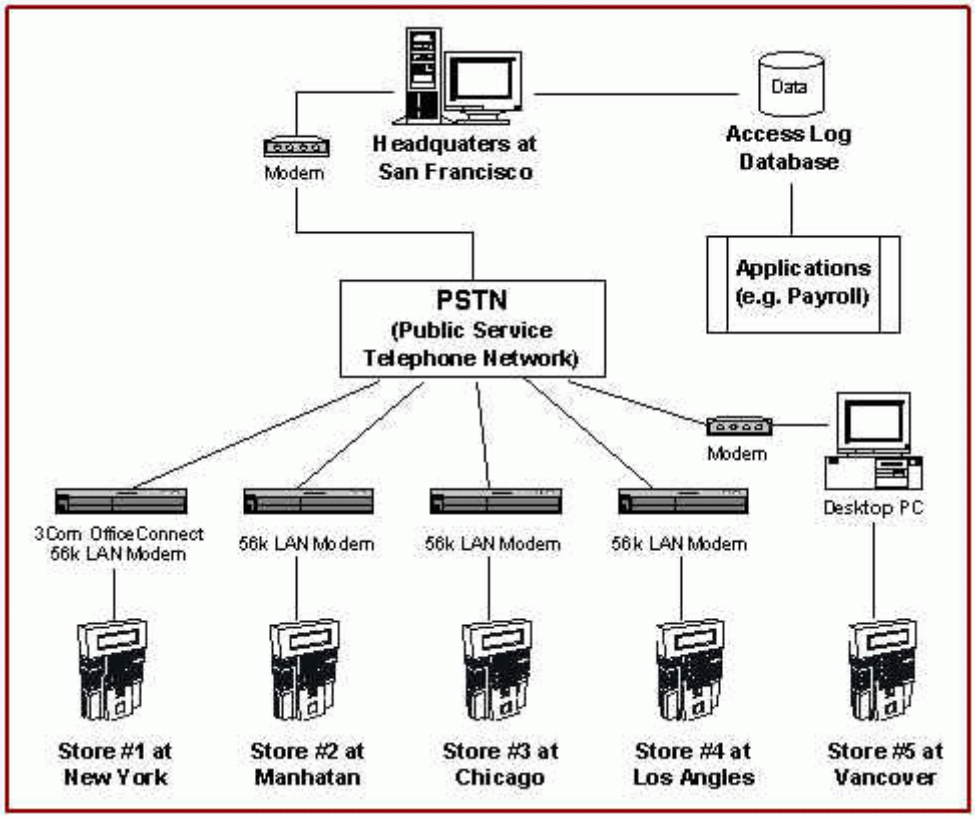
Description	***Affichage Ecran***
En mode stand-by, presser la touche **Func** pour entrer dans le menu Installation. Entrer le mot de passe Administrateur (défaut 123) Comme montré.	`Entrer Mot de Passe: _`
Presser la touche **Func**, puis presser "**A**" pour passer la machine en Mode Test. L'écran affichera le statut Mode Test comme montré. Vous pouvez maintenant demander aux nouveaux utilisateurs de s'exercer et aucune transaction ne sera enregistrée.	`== Mode Test! == ID #:_`
Répéter la procédure ci-dessus et presser "A" de nouveau dans le menu Installation pour remettre la machine en Mode Normal	`Lun 30 Dec 13:49 ID #:_`

Note:
Notez que vous devez ramener la machine en Mode Normal, ou bien les rapports des mouvements d'accès deviendront invalides.

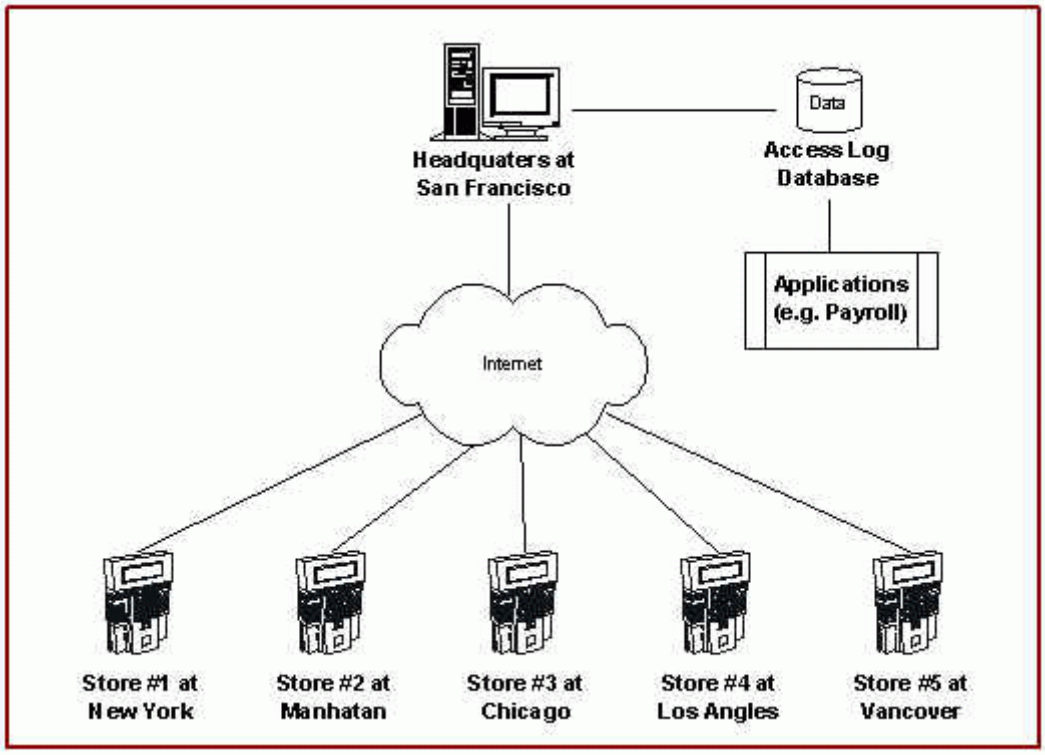
8 Annexe

Connexion Réseau

1. Connexion avec PSTN (Service Public de Réseau Téléphonique)

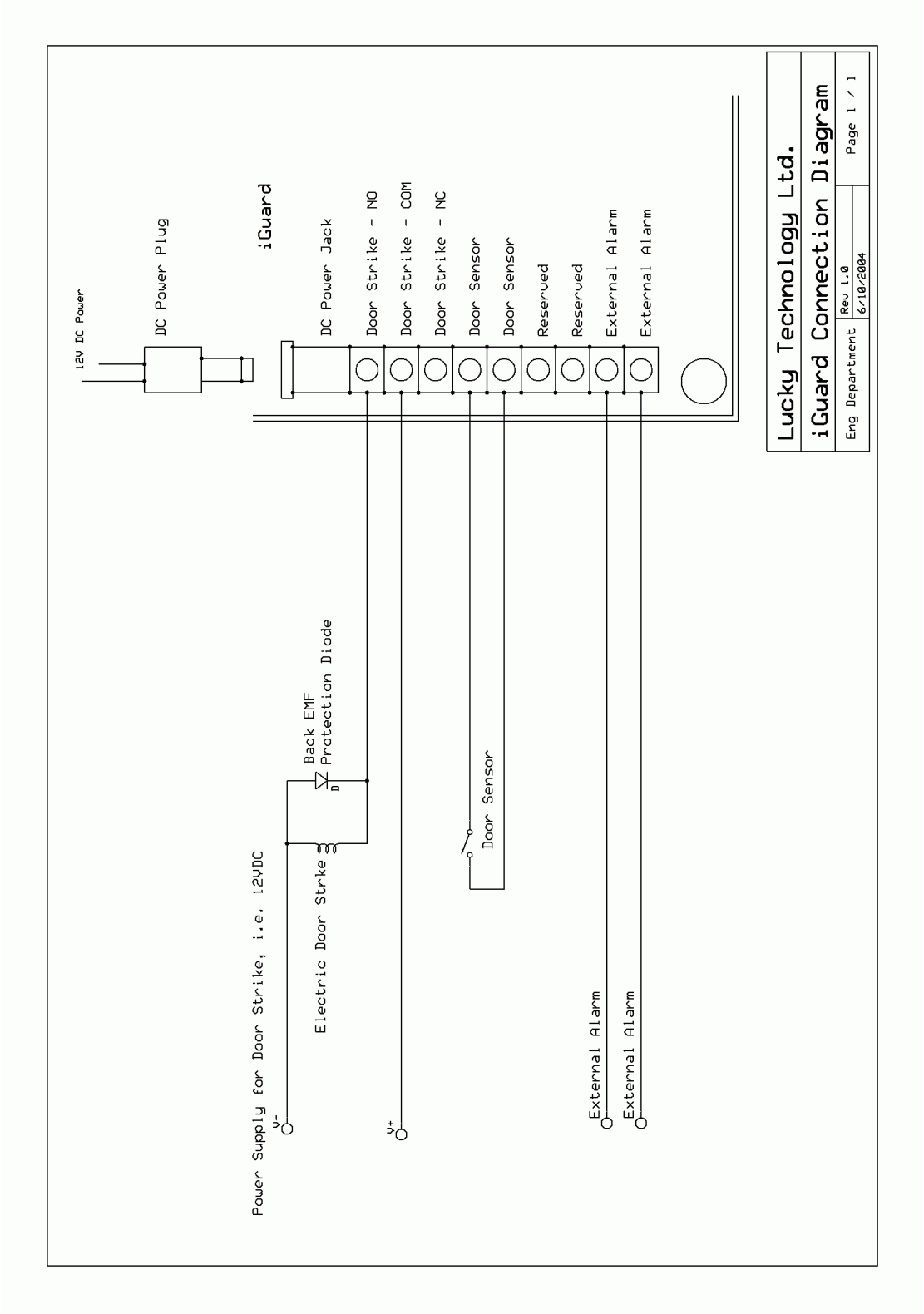


2. Connexion avec Internet

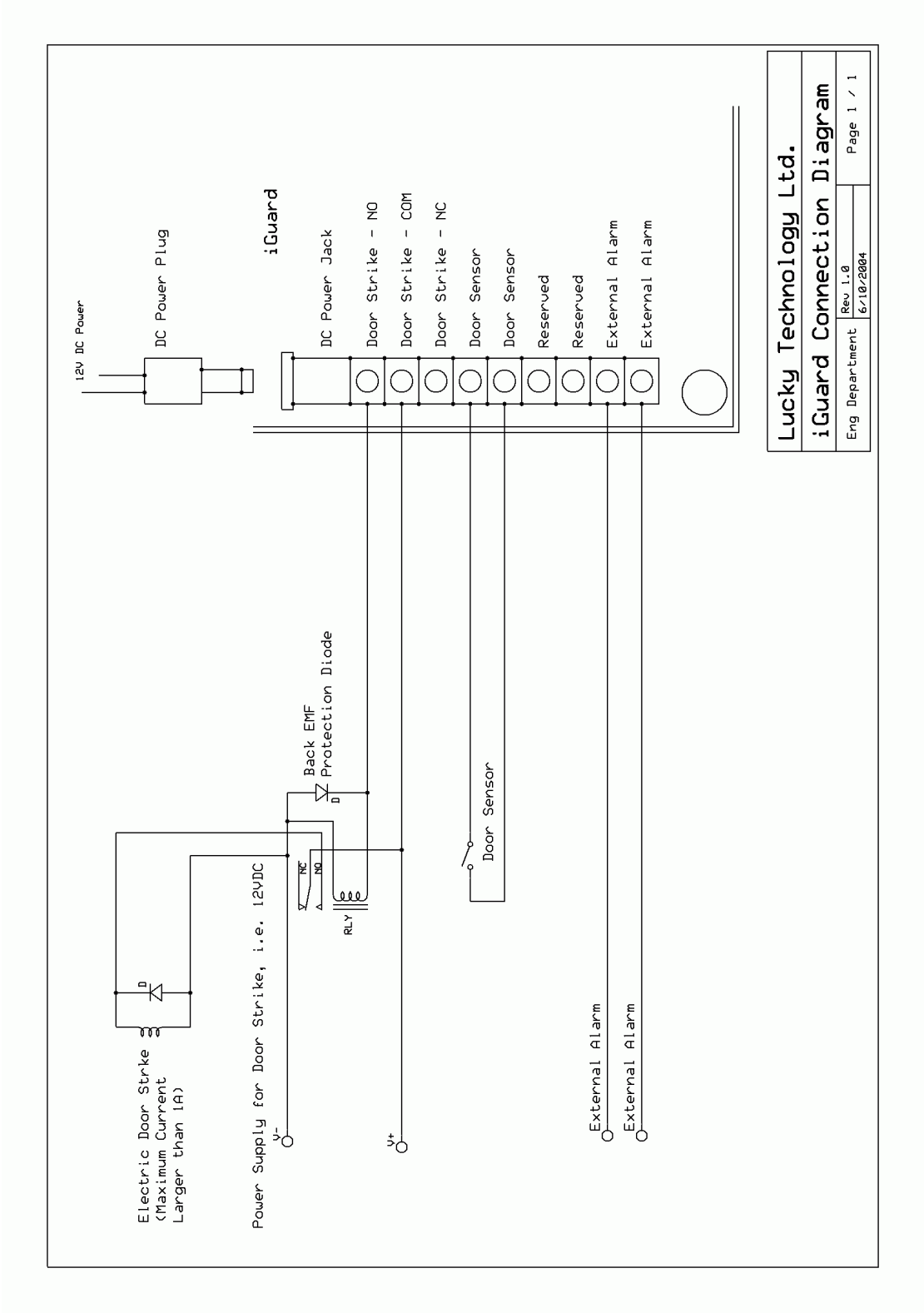


Diagrammes de Connexion

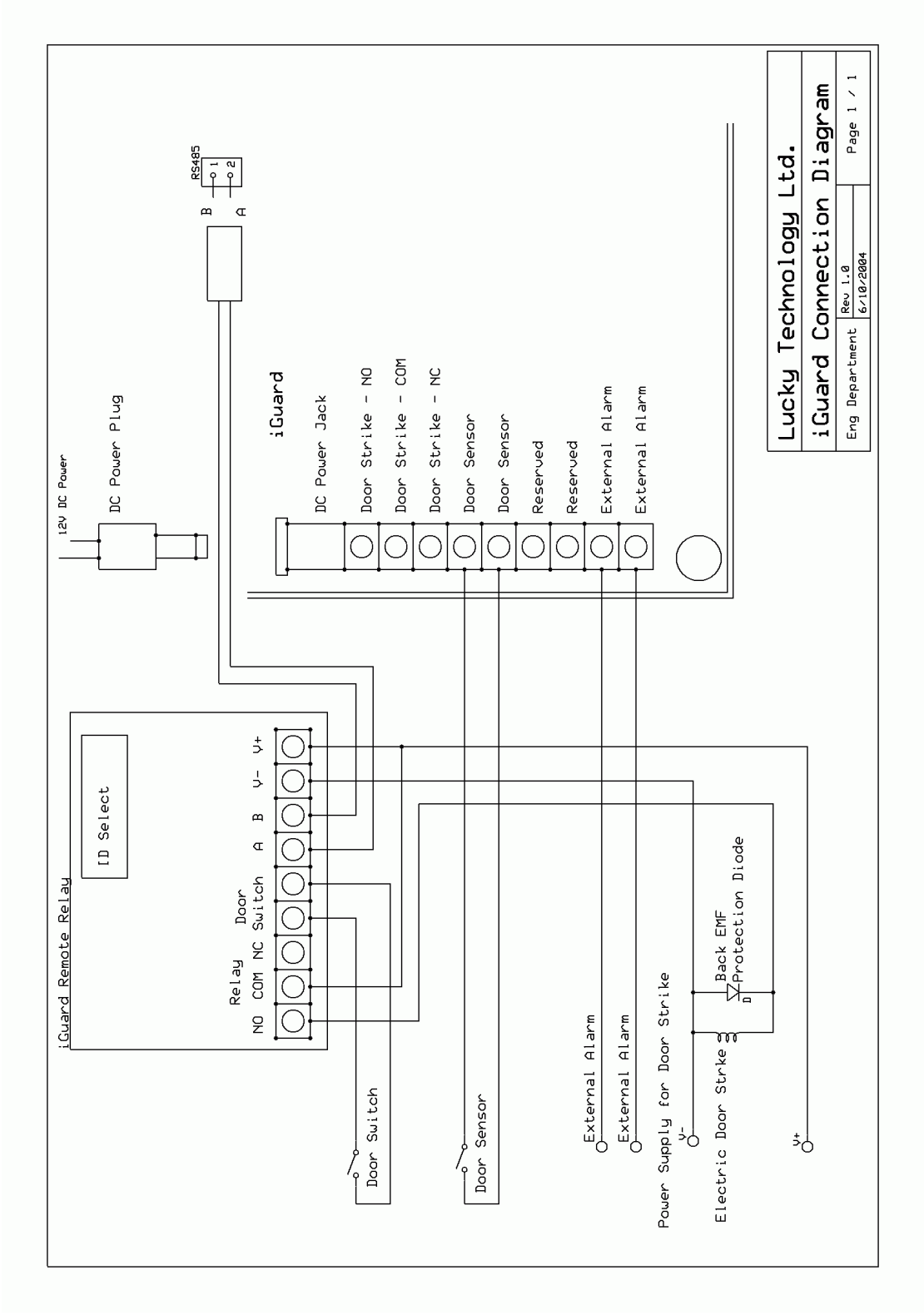
1. Connexions Basiques



2. Connexion Basique (Grande Charge)



3. Diagramme de Connexion – Relais de porte éloignée



FIN