# iGuard™ Seria LM

## Instrukcja obsługi

Wersja 3.6.xxxx


 www.lucky-tech.com

**OŚWIADCZENIE DYSTRYBUTORA – DEEP BLUE BIOMETRICS**

Poniższa dokumentacja została przetłumaczona przez firmę DEEP BLUE BIOMETRICS Sp. z o.o. i nie jest dosłownym tłumaczeniem oryginalnej instrukcji producenta. Zawarty w niej tekst odpowiada jednak dokładne oryginalnej zawartości dokumentacji w języku angielskim. Niektóre opisy zostały uproszczone lub dostosowane do polskich warunków.

Wersja polskiej dokumentacji odpowiada numeracji przyjętej w oryginalnej wersji instrukcji.

Wszelkie uwagi dotyczące poniższego tekstu, tłumaczenia należy kierować na adres:

**DEEP BLUE BIOMETRICS Sp.z o.o.**
ul. Wilcza 44/5
00-678 Warszawa
Tel. +48 [0 22] 622 89 56, 625 77 98
Fax. +48 [0 22] 628 77 97



Trade Name : iGuard
Model No: FPS110 / LM

CE FC

# 1. INSTALACJA

## 1.1.1. Szybka instalacja

Przed instalacją iGuard należy zapoznać się z wymaganiami bezpieczeństwa dotyczącymi instalacji systemu zawartymi w „Wymaganiach instalacyjnych".

## 1.1.2. Wymagania instalacyjne:

- Terminal iGuard przeznaczony jest do montażu wewnątrz pomieszczeń. Jeśli urządzenie zostanie zamontowane na zewnątrz należy się liczyć z możliwością jego uszkodzenia w wyniku działania niskich temperatur, wilgoci lub bezpośredniego oddziaływania wody.
- W czasie instalacji musi być zapewnione uziemienie doprowadzone bezpośrednio do metalowego modułu instalacyjnego czytnika iGuard. Uziemienie chroni przed porażeniem prądem i uszkodzeniem terminalu.
- Dla celów bezpieczeństwa nie należy zasilać innych urządzeń z zasilacza przeznaczonego dla terminali iGuard.
- Dla zapewnienia należytego bezpieczeństwa nie wolno podłączać przycisku otwarcia drzwi bezpośrednio do iGuard. Przycisk powinien być podłączony bezpośrednio do zamka.
- Dla zapewnienia należytego bezpieczeństwa przekaźnik powinien być zainstalowany wewnątrz zabezpieczanego pomieszczenia i podłączony nie poprzez wyjście open collector ale poprzez dodatkowy moduł sterujący przekaźnika zapewniający szyfrowaną komunikację.
- Nie wolno instalować urządzeń w pobliżu źródeł ciepła, wystawiania na działanie promieni słonecznych lub dużego zapylenia otoczenia.
- Jeśli wykorzystywana jest funkcja czytania kart upewnij się, że kod firmy został wpisany w konfiguracji urządzenia.

## 1.1.3. Instalacja

- Określ lokalizację dla terminalu, zasilacza i przekaźnika sterującego przejściem.
- Zamocuj ramę montażową dla terminalu.
- Podłącz zasilanie, kabel od sieci LAN oraz sterowanie przekaźnikiem.
- Zainstaluj terminal na ramie montażowej i zablokuj za pomocą śruby od spodu czytnika.
- Schemat podłączeń terminalu:
    - Terminal #1 – Uziemienie
    - Terminal #2 – + 12V
    - Terminal #3/4 – Normalnie otwarte
    - Terminal #4/5 – Normalnie zamknięte
    - Terminal #6/7 – Czujnik drzwi (opcjonalnie)
    - Terminal #8/9 – Nie wykorzystane
    - Terminal #10/11 – Zewnętrzny alarm (opcja)
    - Wtyk – Sterowanie zewnętrznego przezaźnika (opcja)

iGuard może być bezpośrednio podłączony do sieci korporacyjnej poprzez łącze Ethernet RJ45 i protokół TCP/IP. Upewnij się, że twój komputer obsługuje połączenia protokołem TCP/IP.

iGuard można również podłączyć bezpośrednio do komputera za pośrednictwem kabla crossover Ethernet RJ45.

Konfiguracja adresu IP terminalu:

- Bezpośrednio na iGuard wciśnij **FUNC**, wpisz domyślne hasło administratora "123", naciśnij **FUNC**, naciśnij **5**.
- Wprowadź dane + **FUNC**.
- Wpisz czas + **FUNC**.

- Wpisz nazwę urządzenia + **FUNC** aby kontynuować.
- Wpisz adres IP (zależnie od adresacji w lokalnej sieci n.p. 192.168.0.101) + **FUNC** aby kontynuować.
- Wpisz maskę sieci (zależnie od adresacji w lokalnej sieci n.p. 255.255.255.0) + **FUNC** aby kontynuować.
- Wprowadź domyślną bramę + **FUNC** aby kontynuować.
- Wprowadź DNS (opcjonalnie) + **FUNC** aby kontynuować.
- Wybierz tryb pracy Master/Slave (1 dla **Master** lub 2 dla **Slave**).
- Wciśnij **1** aby zaakceptować wartości lub 2 aby anulować operację.

Aby sprawdzić czy terminal został prawidłowo skonfigurowany wykonaj program PING.

Na dowolnym komputerze w sieci z Menu startu (Windows) wybierz RUN a następnie Command

- Wpisz 'ipconfig " aby upewnić się że computer pracuje w tej samej sieci.to check the
- Ping adres IP iGuard, domyślny jest: 192.168.0.100.
- If the ping responds the following, the IP is set properly and you are ready to proceed:

  C:\>ping 192.168.0.100
  Pinging 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
  Reply from 192.168.0.100: bytes=32 time<10ms TTL=128
  Ping 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

- Uruchom w swoim komputerze dowolną przeglądarkę internetową i wpisz adres IP twojego iGuard'a. Jeśli wszystko poprawnie zostało skonfigurowane powinna otworzyć się strona startowa terminalu pod adresem http://192.168.0.100

## 1.1.4. Wymagania dotyczące zasilania

iGuard wymaga zasilania 12V/500mA z zasilacza impulsowego. Zasilacz ten nie powinien być wykorzystywany jednocześnie do zasilania innych urządzeń.

## 1.1.5. Decyzja o miejscu instalacji

iGuard jest przeznaczony do montażu na ścianie. Do tego celu służy specjalna, metalowa podstawa montażowa. Zaleca się aby urządzenie było montowane jak najbliżej drzwi którymi steruje w sposób przemyślany, umożliwiający wygodną obsługę. Szczególną uwagę należy zwrócić na:

- Zapewnienie odpowiedniej cyrkulacji powietrza aby urządzenie nie ulegało przegrzaniu.
- Nie wolno instalować urządzeń w pobliżu źródeł ciepła.
- Nie wolno instalować urządzeń w pomieszczeniach z o zanieczyszczonej atmosferze pyłami i w miejscach oddziaływania promieniowania słonecznego.

## 1.1.6. ** Ważne ** Dotyczy metalowej ramy montażowej

Metalowy panel przeznaczony do instalacji iGuard musi być uziemiony.

## 1.1.7. Podłączenie – Zasilanie i zewnętrzne urządzenia

iGuard umożliwia podłączenie zewnętrznego zasilania oraz zewnętrznych elementów wykonawczych, jak również sensorów montowanych w sterowanych przejściach.

**Zasilanie (12V DC):**

Terminal #1 (uziemienie), terminal #2 (+12V). Wymagane zasilanie 12V DC, 150mA, szczytowy prąd 500mA.

**Przekaźnik (Terminal 3 – 5)**
(3 – 4 normalnie otwarty, 4 – 5 normalnie zamknięty). Styki te można podłączyć bezpośrednio do przekaźnika wymagającego sterowania 12V DC i maks. 1A.
**Czujnik drzwi (opcjonalnie)**
Terminal 6 i 7 służy do podłączenia sensora otwarcia/zamknięcia drzwi. Jeśli drzwi będą otwarte dłużej niż 10 sekund włączy się alarm w czytniku iGard sterującym przejściem.

**Zewnętrzny alarm (opcja)**
Terminal 10 i 11 służy do podłączenia zewnętrznych urządzeń sygnalizujących przekroczenie dopuszczalnego czasu otwarcia przejścia.

**Zewnętrzny moduł sterujący przekaźnikiem (opcja)**
Pozwala na umieszczenie specjalnego modułu sterującego przekaźnikiem w strefie bezpiecznej i sterowanie nim zabezpieczonym protokołem komunikacyjnym. Zastosowanie tego modułu znacznie podnosi bezpieczeństwo w systemach kontroli dostępu.

**Włączenie zasilania**

Po włączeniu zasilania iGuard wykona autodiagnostykę:
***Opis komunikatów na wyświetlaczu:***

| **Opis** | **Wyświetlacz LCD** |
|---|---|
| po włączeniu zasilania wykonywany jest auto test | Initializing... |
| Po ok 10 sek. Urządzenie załaduje system operacyjny. program... | iGuard System Loading... |
| Po załadowaniu systemu iGuard przełączy się w tryb oczekiwania. | Monday 30 13:49 ID#: |

# 2. Konfiguracja

## 2.1. Ustawianie daty i czasu.

Aby informacje o rejestrowanych przejściach odzwierciedlały rzeczywisty czas zdarzenia należy prawidłowo ustawić zegar urządzenia.

| **Opis** | **Wyświetlacz LCD** |
|---|---|
| Gdy czytnik jest w trybie oczekiwania wciśnij FUNC i wprowadź hasło administratora: | Enter Password: _ |
| Wpisz hasło administratora (domyślne: 123) | Enter Password: _ *** |
| Wciśnij FUNC aby zatwierdzić | Press 1: Add/Update ID : Press 5: System Configuration ... |
| Wciśnij 5 aby przejść do konfiguracji systemu. Wpisz prawidłową datę terminalu a następnie wciśnij FUNC. | Date (M/D/Y) 08/30/2004 |
| Wpisz prawidłową godzinę na terminalu a następnie zatwierdź wciskając FUNC | Time: (H;M:S) 13:45:23 |
| Teraz system poprosi o podanie ID terminalu. Parametr ten jest istotny jeśli w sieci znajduje się więcej urządzeń. | Terminal ID: |

## 2.2. Ustawienie parametrów sieci i adresu TCP/IP

iGuard może być podłączony do sieci LAN bezpośrednio poprzez protokół TCP/IP. Dlatego też należy określić dla niego parametry takie jak adres IP lub DHCP, maska sieci, DNS.

| **Opis** | **Wyświetlacz LCD** |
|---|---|
| Wciśnij klawisz FUNC, wpisz hasło administratora a następnie zatwierdź ponownie wciskając FUNC. | Enter password:<br>_ |
| Wciśnij „5” aby ustawić konfigurację systemu. | Press 1:<br>Add/Update ID<br>:<br>Press 5: System<br>Configuration: |
| Wciśnij FUNC aby przejść do konfiguracji DHCP/Static IP. | |
| Wciśnij FUNC aby kontynuować a następnie wybierz „1” aby ustawić DHCP lub „2” aby ustawić statyczny adres IP. | DHCP/Static IP<br>(1/2) ? Static |
| Wciśnij FUNC aby kontynuować. Następnie system poprosi o podanie nowego adresu IP. Wpisz ponownie cały adres nawet jeśli chcesz zmienić tylko jedną cyfrę. | IP Address:<br>192.168.001.123 |
| Wciśnij FUNC a następnie wpisz nową maskę sieci. | Subnetmask:<br>255.255.255.000 |
| Wciśnij FUNC i wpisz nową bramę sieci. | DefaultGateway:<br>192.168.000.200 |
| Wciśnij FUNC aby podać nowy adres serwera DNS. | DNS:<br>192.168.000.200 |
| Wciśnij FUNC aby określić czy urządzenie jest Master czy Slave. Jeśli urządzenie pracuje samodzielnie zawsze ustaw je jako master. W przeciwnym razie system poprosi o podanie urządzenia Master. | Master/Slave<br>(1/2) ? Master |
| Wciśnij FUNC aby zakończyć konfigurację sieci. | Mon Aug 30 13:46<br>ID #:_ |

## 2.3. Kod firmy

Kod firmy jest parametrem ważnym, jeśli terminal wykorzystuje funkcje czytnika kart. Ustawienie tego kodu gwarantuje, że czytane są karty należące tylko do firmy. Karty z zapisanym innym kodem firmy będą ignorowane.

## 2.4. Ustawienie hasła administratora

iGuard wyposażony jest w trzy rodzaje haseł:
**System Administrator** – Konfiguracja i administracja systemem
**User Administrator** – do zarządzania kontami użytkowników
**The Door Access Password** – hasło służące do otwierania drzwi.

Procedura zmiany hasła:

| **Opis** | **Wyświetlacz LCD** |
|---|---|
| Gdy urządzenie jest w trybie oczekiwania wciśnij FUNC, podaj hasło administratora i zatwierdź ponownie wciskając FUNC. Wybierz „6” aby przejść do ustawiania hasła administratora. Gdy system zapyta się Admin/Personal (1/2) wybierz „1”. | System Admin:<br>123_ |
| Wciśnij ☐ aby wykasować stare hasło i wpisać nowe (np. AB456). Długość hasła ograniczona jest do 10 znaków w przedziale 0-9 oraz A i B. | System Admin:<br>AB456 |
| Wciśnij FUNC aby zaakceptować nowe hasło dla System Administrator. Teraz system poprosi o podanie nowego hasła dla User Administratora. | User Admin: _ |
| Wpisz nowe hasło (np. 7890AB) a następnie zatwierdź FUNC. | User Admin:<br>7890AB_ |
| Wciśnij FUNC aby zaakceptować. Teraz system poprosi o podanie nowego | Door Access: _ |

| | |
|---|---|
| hasła dla Door Access Password | |
| Wpisz nowe hasło (np. 9394AB709) a następnie zatwierdź FUNC | Door Access:<br>9394AB709_ |
| Po zatwierdzeniu FUNC terminal przełączy się w stan oczekiwania | Mon Aug 30 13:49<br>ID #:_ |

# 3. OPERACJE PODSTAWOWE (BASIC OPERATIONS)

## 3.1. REJESTRACJA

### 3.1.1. REJESTRACJA ODCISKÓW PALCA

Proces ten polega na zapisaniu wzorców biometrycznych odcisków palca wewnątrz urządzenia iGuard. Terminal wykorzystuje technologię DFX (Difficulty Fingerprint Extraction) zaprojektowaną przez laboratorium Bell Lab z USA. Technologia ta jest najbardziej dopasowaną technologią dla rejestrowania wzorców biometrycznych większości ludzi i charakteryzuje się bardzo niskim współczynnikiem niepożądanych odrzuceń poniżej 1%. W szczególnych przypadkach pojedyncze osoby mogą cię cechować szczególnie niską wilgotnością palca, dlatego mogą wystąpić problemy z rejestracją. Wynika to z faktu również, że system wymaga znacznie większej dokładności w procesie rejestracji niż wzorca niż podczas normalnego używania czytnika. Aby ograniczyć ten problem w procesie rejestracji należy nieco zwilżyć opuszki palców w celu ułatwienia rejestracji. Ta dodatkowa czynność wymagana może być jedynie w procesie rejestracji i nie jest konieczna w czasie normalnego używania terminala.

Osoby o znacznym uszkodzeniu powierzchni palców objętych rejestracją mogą być rejestrowane z obniżonym poziomem dokładności. Wpływa to jednak na obniżenie bezpieczeństwa indywidualnych wzorców.

W procesie rejestracji pobierane są wzorce z dwóch palców każdej osoby trzy razy. Jeśli zarejestrowany wzorzec nie jest dostatecznej jakości system poprosi o powtórną rejestrację wzorca.

Podczas rejestracji palec powinien być umieszczony centralnie na powierzchni sensora. Centralna część palca zawiera większość charakterystycznych elementów wykorzystywanych przez system w procesie tworzenia wzorca biometrycznego. Prawidłowo zarejestrowany palec wydatnie obniża poziom niepożądanych odrzuceń podczas codziennego stosowania.

W celu przeprowadzenia rejestracji wciśnij klawisz FUNC, wpisz hasło administratora a następnie zatwierdź ponownie wciskając klawisz FUNC.

| **Opis** | **Wyświetlacz LCD** |
|---|---|
| Wpis „1” aby uruchomić proces rejestracji | By Fingerprint/Passwd<br>(1/2)? |
| Wybierz 1 a następnie | Enter ID # and<br>Scan 1st Finger |
| podaj ID użytkownika i wciśnij klawisz FUNC | Enter ID# A01_ |
| Naciśnij klawisz FUNC po każdym zarejestrowaniu wzorca. Proces rejestracji będzie demonstrowany poziomą linią przesuwającą się wzdłuż wyświetlacza. Za każdym razem gdy chcemy umieścić nasz palec na czytniku musimy dokładnie odsunąć pokrywę ochronną sensora. | Scanning 1 of 3 ... |
| Gdy linia demonstrująca proces rejestracji przesunie się całkowicie do prawej strony zostaniesz poproszony o zdjęcie palca z czytnika | Analyzing. Pls remove finger ... |

| | |
|---|---|
| Gdy system wykryje że palec został odsunięty wówczas poprosi o wciśnięcie klawisza FUNC i powtórzenie rejestracji. | Press FUNC to scan 2 of 3 |
| Ponownie naciśnij FUNC aby jeszcze raz zarejestrować palec. | Press FUNC to scan 3 of 3 |
| Jeśli wszystko udało się wykonać bez problemu system poprosi o przyłożenie drugiego palca i cała procedura potrójnej rejestracji zostanie powtórzona. | Press FUNC to scan<br>2nd finger |
| Na zakończenie pozytywnie wykonanej operacji zostanie wyświetlony komunikat: | ID: A01 Added OK.! |
| System automatycznie przestawi się w tryb rejestracji kolejnej osoby | Enter ID # and<br>scan 1st Finger |
| Aby opuścić tryb rejestracji wciśnij klawisz ☐ | Mon 30 Aug 12:00<br>ID #: _ |
| W sytuacji gdy palec jest zbyt suchy pojawi się następujący komunikat | Scanning 1 of 3<br>=== To Dry !== |
| Jeśli mimo to kontynuujemy rejestrację na jej koniec system zaproponuje obniżenie poziomu bezpieczeństwa. Zaleca się obniżenie bezpieczeństwa jedynie dla systemów RCP | Set Security to<br>Low2 yes(1)/No(2) |

### 3.1.2. Włączenie trybu Automatch

Tryb ten umożliwia identyfikację osób bez uprzedniego podawania hasła lub zbliżania karty. W trybie automach pracownik jedynie musi unieść pokrywę ochronną czytnika a następnie przyłożyć palec. Graficzna instrukcja obsługi tej czynności jest załączana z każdym czytnikiem iGuard. Maksymalną ilość użytkowników objętych systemem automatch zaleca się ograniczyć do 30. wynika to z faktu, że ustawienie trybu automatach dla większej liczby pracowników skutkuje znacznym spowolnieniem procesu identyfikacji nawet do kilkudziesięciu sekund. Zamiast tego dla większej liczby użytkowników należy stosować mieszaną metodę opartą o PIN i palec lub KARTA i palec. Zaleca się aby tryb automatach uruchamiać dla ograniczonej liczby osób lub dla np.: zarządu. Włączenie tej opcji możliwe jest jedynie poprzez interfejs programu administracyjnego.

### 3.1.3. Rejestracja z wykorzystaniem Smart Card (dla modeli wyposażonych w czytniki Smart Card)

Użytkownik musi być zanim zostanie zarejestrowany w systemie za pomocą odcisku palca lub przydzielone zostanie hasło. Po zakończeniu rejestracji ID użytkownika zostanie zapisane w urządzeniu razem ze wzorcem biometrycznym w pamięci terminalu.

*Tylko jeden, główny wzorzec odcisku palca zapisywany jest na karcie.*

Poniższa procedura pokazuje jak zarejestrować użytkownika w systemie:

| **Opis** | **Wyświetlacz LCD** |
|---|---|
| Gdy urządzenie jest w trybie oczekiwania wciśnij FUNC. Wprowadź hasło administratora i potwierdź za pomocą FUNC. Naciśnij „9” i wybierz Issue/Import Card. Wciśnij „1” aby zapisać kartę. | Enter ID #: _ |
| Wpisz ID użytkownika, którego dane chcesz zapisać na karcie. | Enter ID #: A01 _ |
| Wciśnij FUNC aby potwierdzić. Teraz system poprosi o zbliżenie karty. | Writing for<br>SmartCard... |
| Zbliż kartę do klawiatury. Teraz system zapisze wzorzec na karcie. | Writing... |
| Po zapisaniu zostaniesz zapytany czy system ma usunąć zapisany w swojej pamięci wzorzec odcisku palca. Ta operacja nie jest zalecana. | Remove Fingerprint<br>Yes(1)/ No (2) ? |

| | |
|---|---|
| Teraz urządzenie przejdzie w tryb oczekiwania na podanie kolejnego ID. | Enter ID #: _ |
| Wciśnij klawisz ß lub poczekaj aż upłynie limit czasu oczekiwania aby powrócić do normalnego trybu oczekiwania. | Mon Aug 30 12:00<br>ID #: _ |

Powyższa procedura nadpisze poprzednio umieszczone dane na karcie.

## 3.1.4. Rejestracja istniejącej karty

Gdy pierwszy raz zostanie użyta karta ze zdalnym czytnikiem zainstalowanym w oddziale firmy użytkownik musi zarejestrować swoją kartę na danym czytniku. Dodatkowo po rejestracji administrator musi określić departament do którego jest przypisany dany użytkownik aby przypisać mu właściwe uprawnienia. Teraz użytkownik może normalnie używać karty.

Procedura rejestracji karty

| **Opis** | **Wyświetlacz LCD** |
|---|---|
| Gdy terminal jest w trybie oczekiwania wciśnij FUNC, wpisz hasło administratora a następnie zatwierdź FUNC. Teraz wybierz „9" aby przejść do Issue/import Card. Wciśnij „2" aby importować kartę. | Enter ID #: _ |
| Teraz system poprosi o zbliżenie karty | Wait for<br>Smart Card ... |
| Zbliż kartę do klawiatury iGuard. Teraz system zapisze informację zapisaną w karcie. | Writing ... |

## 3.1.5. Weryfikacja na podstawie odcisku palca

Urządzenie wykorzystuje zapisane wzorce w celu porównania tożsamości pracowników. Proces weryfikacji jest bardzo prosty co ilustruje poniższa procedura.

| **Opis** | **Wyświetlacz LCD** |
|---|---|
| Gdy urządzenie jest w trybie oczekiwania na klawiaturze wpisz swoje ID, przykładowo A01. | Mon Aug 30 13:49<br>A01 _ |
| Podnieś osłonę sensora i przytknij jeden z zarejestrowanych palców. Urządzenie automatycznie odczyta palec a następnie dokona weryfikacji. | Scanning ... A01_<br>:<br>:<br>Veryfying... |
| Jeśli tożsamość zostanie potwierdzona, urządzenia zasygnalizuje to komunikatem, oraz zapaleniem się zielonych lampek po obu stronach klawiatury a następnie powróci do trybu oczekiwania. | A01 Authorized!<br>:<br>Mon Aug 30 13:49<br>ID #: _ |

## 3.1.6. Weryfikacja w trybie Automtach

Identyfikacja w trybie automtach pozwala na identyfikację osoby bez konieczności podania ID użytkownika.

| **Opis** | **Wyświetlacz LCD** |
|---|---|
| Gdy urządzenie jest w trybie oczekiwania podnieś osłonę i połóż palec na sensor. Urządzenie automatycznie rozpocznie odczyt wzorca. | Mon Aug 30 13:49<br>== Automatach !==<br>:<br>Veryfying ... |
| Jeśli jesteś osobą upoważnioną system potwierdzi twoją | Mon Aug 30 13:49 |

| | |
|---|---|
| tożsamość i zasygnalizuje to. | Authorized ! |

### 3.1.7. Weryfikacja za pomocą Smart Card

| Opis | Wyświetlacz LCD |
|---|---|
| Gdy urządzenie jest w trybie oczekiwania zbliż kartę blisko klawiatury. Terminal odczyta kartę i jeśli jest ona zarejestrowana w systemie poprosi o przyłożenie palca | Jacky Hui<br>Waiting Finger |
| Jeśli wzorzec zapisany na karcie odpowiada wzorcowi palca na czytniku użytkownik uzyskuje dostęp | Jacky Hui<br>Authorized |

### 3.1.8. Weryfikacja za pomocą hasła

| Opis | Wyświetlacz LCD |
|---|---|
| Gdy terminal jest w trybie oczekiwania wpisz na klawiaturze ID użytkownika (np. A01) | Mon Aug 30 13:49<br>A01_ IN |
| Zamiast podnosić pokrywę czytnika wystuka ja klawiaturze hasło i naciśnij FUNC | Your password: |
| Wpisz hasło | Your password:<br>****** |
| Wciśnij FUNC ponownie aby potwierdzić. Jeśli hasło jest prawidłowe dostęp zostanie przyznany. | A01<br>Authorized |
| | |

### 3.1.9. Tymczasowe wstrzymanie dostępu

Istnieje możliwość tymczasowego zablokowania dostępu określonej osobie do systemu. Funkcja ta dostępna jest poprzez „Inactivate ID". Osobom którym odebrano czasowo dostęp można go przywrócić bez konieczności ponownej rejestracji.

| Opis | Wyświetlacz LCD |
|---|---|
| Gdy urządzenie jest w trybie oczekiwania wciśnij FUNC. Wprowadź hasło administratora i potwierdź za pomocą FUNC. Naciśnij „2" i wybierz „Inactivate ID". | Enter ID #: _ |
| Wpisz ID # użytkownika które chcesz zablokować | Enter ID: A01 |
| Wciśnij FUNC aby zatwierdzić. Teraz użytkownik z ID # A01 został zablokowany. | ID A01:<br>Inactivated ! |

## 3.2. POZOSTAŁE FUNKCJE

### 3.2.1. Kasowanie ID

Czynność ta polega na permanentnym usunięciu użytkownika z systemu.

| Opis | Wyświetlacz LCD |
|---|---|
| Gdy urządzenie jest w trybie oczekiwania wciśnij FUNC. Wprowadź hasło administratora i potwierdź za pomocą FUNC. Naciśnij „4" i wybierz „Delete ID". | ID to Delete: |
| Wpisz ID # użytkownika które chcesz usunąć | ID to Delete:<br>A01 |
| Wciśnij FUNC aby zatwierdzić. Teraz użytkownik z ID # A01 został usunięty. | ID #A01<br>Delete! |

Usunięcie ID użytkownika spowoduje usunięcie wszystkich informacji na jego temat.

### 3.2.2. Wyłączanie urządzenia

Urządzenie można wyłączać w prosty sposób poprzez odłączenie zasilania, jednak taki sposób nie jest zalecany. Ponieważ w czasie pracy przez pewien krótki czas niektóre informacje przechowywane są w pamięci ulotnej istnie ryzyko ich utraty. Producent zaleca wyłączanie urządzeń w sposób kontrolowany. Aby bezpiecznie wyłączyć urządzenie należy korzystając z funkcji FUNC 7 z menu.
Funkcja ta służy również do kasowania zapisanych danych w czytniku, dlatego należy dokładnie zapoznać się z komunikatami wyświetlanymi przez terminal przed ich akceptacją.

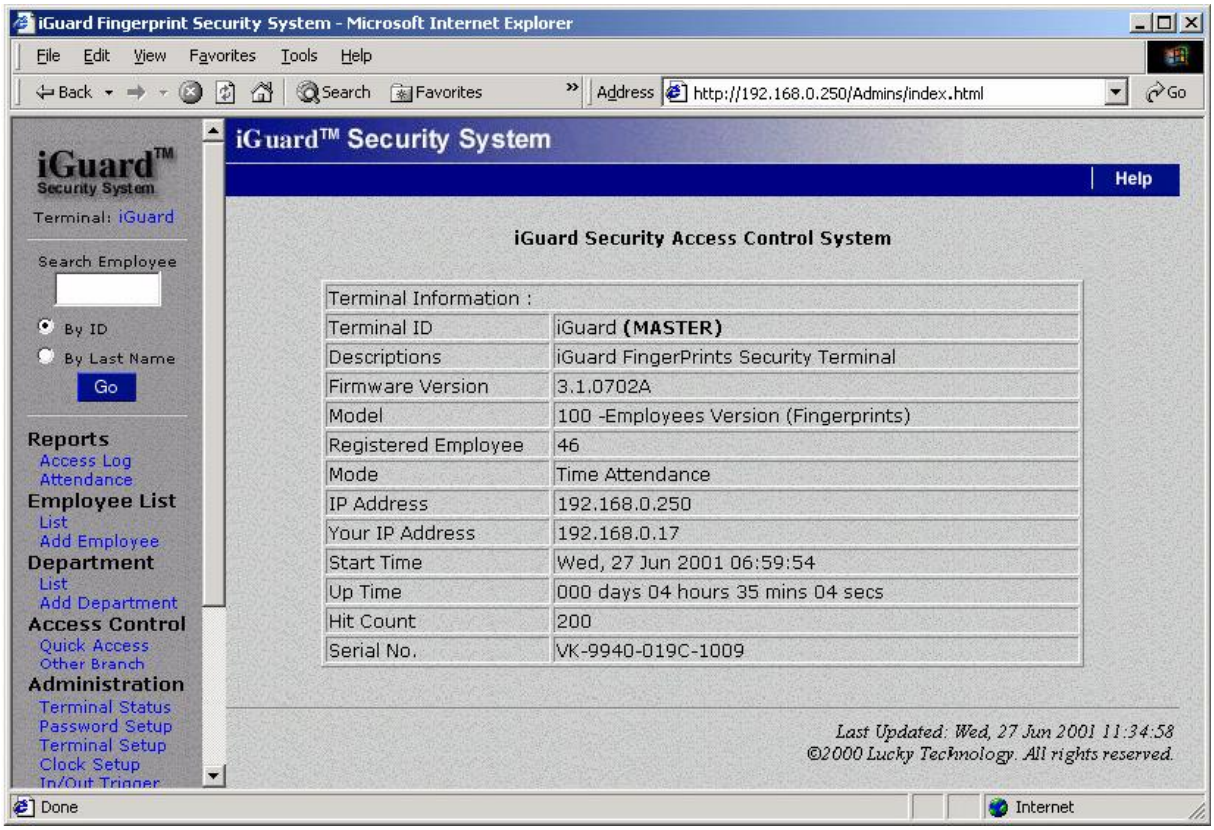
### 3.2.3. Procedura bezpieczeństwa

W sytuacji gdy urządzenie nie odpowiada istnieje możliwość awaryjnego otwarcia drzwi przez administratora. Polega to na wciśnięciu klawisza FUNC, wpisanie hasła administratora, ponownego wciśnięcia klawisza FUNC a następnie „B”. Taka operacja spowoduje awaryjne otwarcie przejścia.

# 4. ADMINSTRACJA

## 4.1. Używanie przeglądarki internetowej

Wbudowany serwer WWW pozwala na pełne zarządzanie urządzeniami iGuard. Z tego też powodu nie jest istotne jaki system operacyjny wykorzystywany jest do zarządzania siecią iGuard. Dostęp do wybranych urządzeń realizowany jest poprzez wpisanie adresu IP danego terminalu. Po wpisaniu adresu IP urządzenia w przeglądarce zgłosi się następujący ekran:




Strona domowa iGuard podzielona jest na dwie części, lewą jako menu nawigacyjne oraz prawą wyświetlającą dostępne opcje dla danej pozycji w menu.

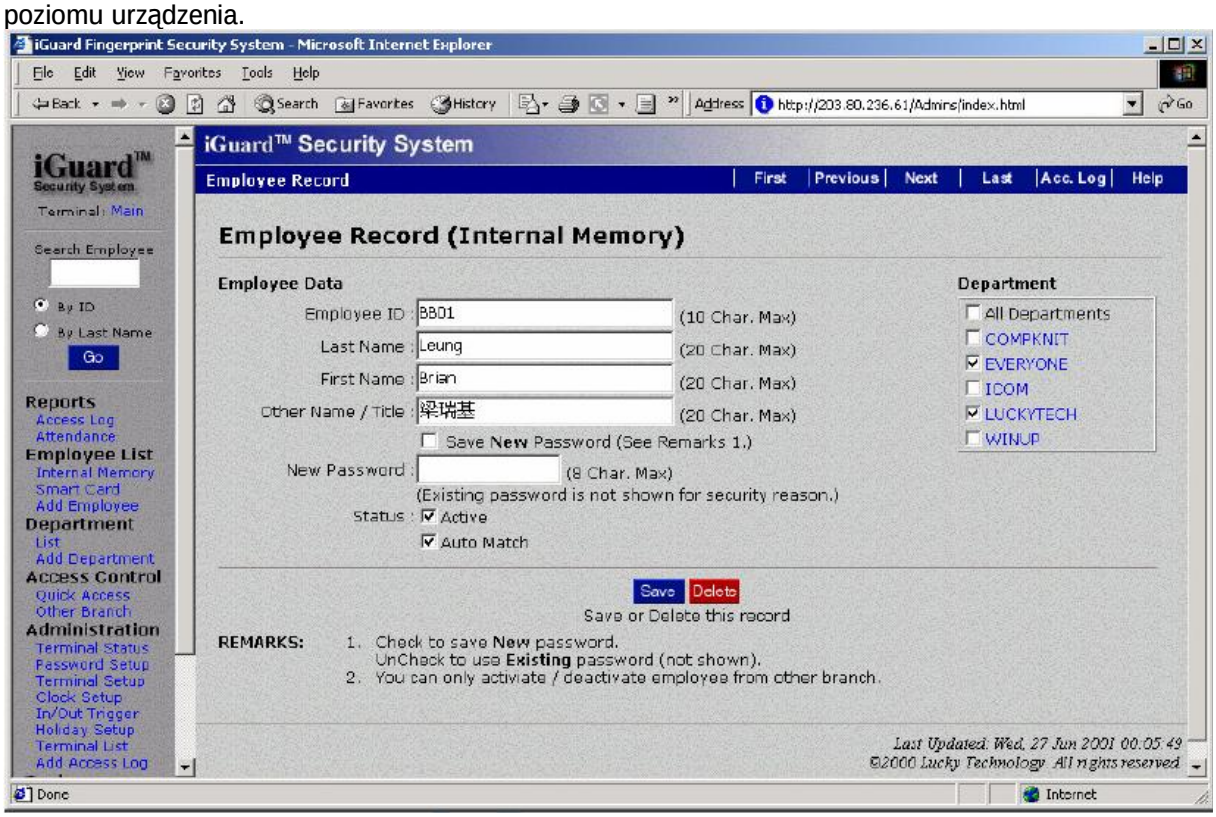
Uwaga: Strona rzeczywista iGuard może nieco odbiegać od tej prezentowanej w dokumentacji.

## 4.2. Lista pracowników

Kliknij na Employee List aby zobaczyć listę pracowników


## 4.3. Employee List – Add Employee

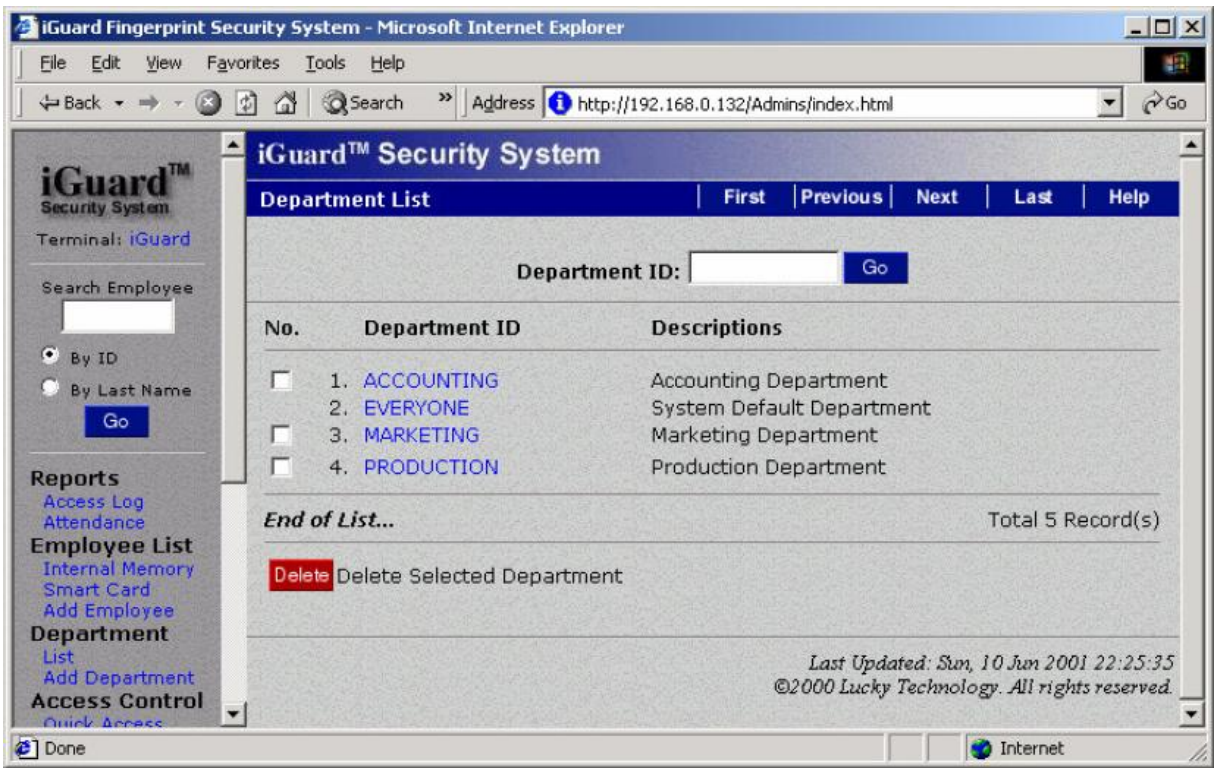
W tej części możemy dodawać nowych pracowników do list, znacznie łatwiej niż z poziomu urządzenia. Należy pamiętać jednak że rejestracja nowych osób w systemie możliwe jest jedynie z poziomu urządzenia.



## 4.4. Departament – List

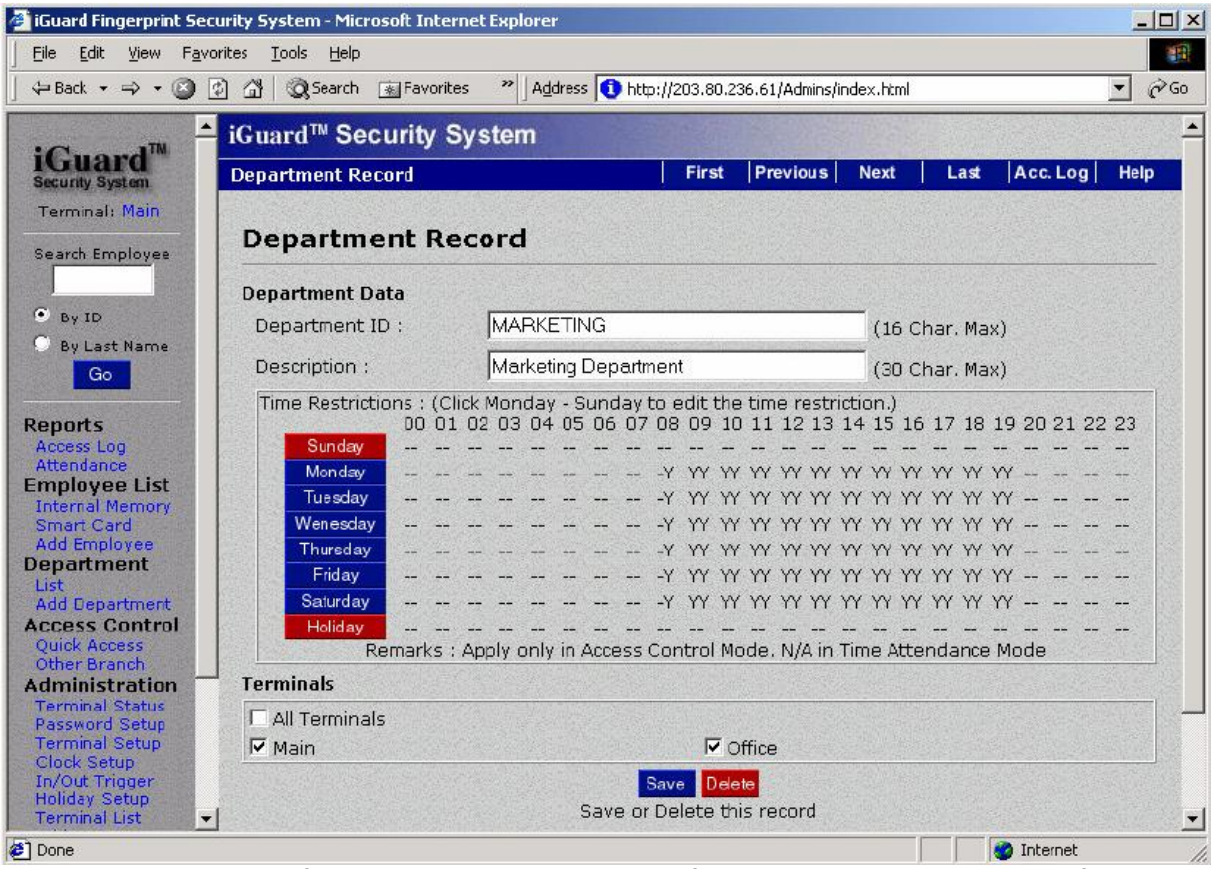
Departamenty pozwalają na grupowanie użytkowników. Każdy departament może mieć przypisaną własną strefę czasową określającą dostęp do systemu dla osób należących do danego departamentu. Jeśli w departamencie dostęp jest określony w godzinach 9:00 – 16:00 oznacza to że osoby należące do tego departamentu również uzyskują dostęp na zasadach określonych dla danego departamentu.

Maksymalna ilość departamentów – 32




Departament o nazwie EVERYONE jest domyślnym departamentem systemowym i nie może być usunięty. Można jednak po wcześniejszym utworzeniu nowych departamentów usunąć z jego listy wszystkich użytkowników systemu.
Usuwanie departamentów polega na zaznaczeniu odpowiedniego kwadracika a następnie kliknięcie klawisza DELETE.

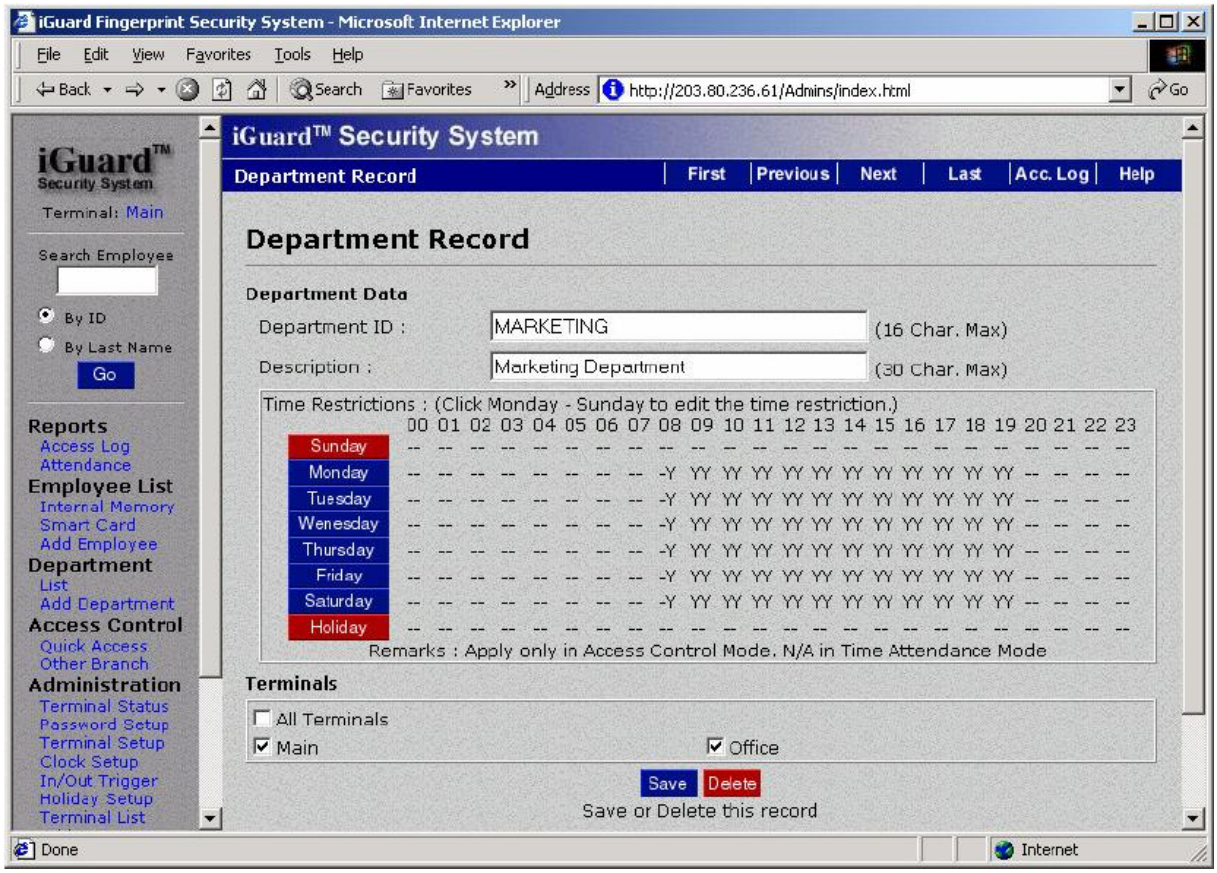
Aby zmienić parametry strefy czasowej dla danego departamentu należy kliknąć na nazwie departamentu.



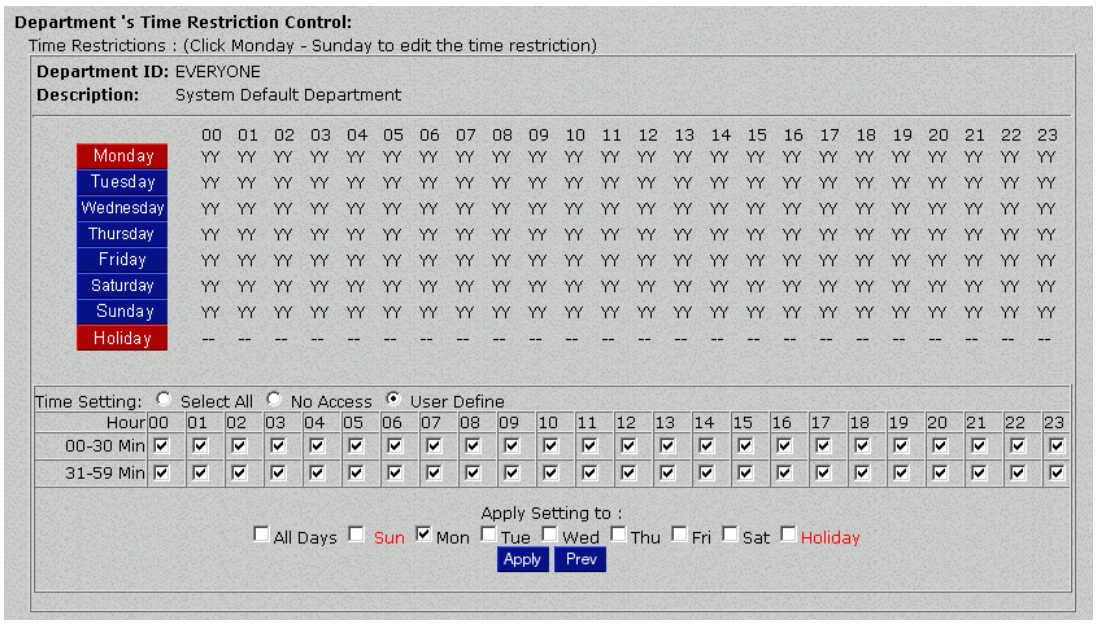

System pozwala na określenie praw dostępu z dokładnością do 30 minut na każdy dzień tygodnia. Dodatkowo wprowadzone są ułatwienia polegające na możliwości automatycznego powielania ustawień z jednego dnia dla wszystkich pozostałych, oraz określenie zasad dostępu dla osób przebywających na urlopach.

## 4.5. Deparment – Add Departament

Aby dodać nowy departament kliknij na link Add Departament . Maksymalna ilość znaków w nazwie departamentu wynosi 32.




Należy wpisać ID i opis departamentu. Następnym etapem jest określenie zasady funkcjonowania strefy czasowej. W tym celu należy określić dla jakich dni ma obowiązywać strefa a następnie zaznaczyć godziny dostępu. Całą operację należy zatwierdzić klawiszem Apply.

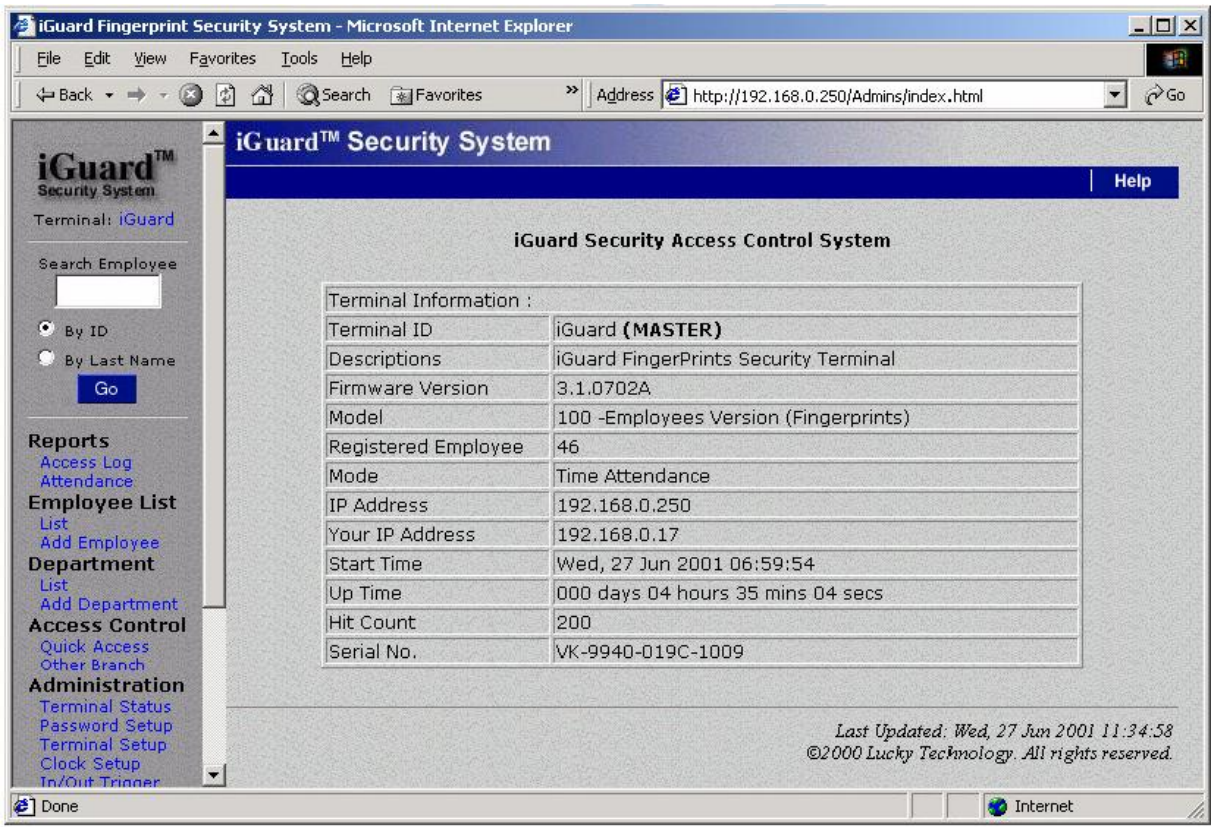


## 4.6. Access Control – Quick Access

Quick Access służy do omijania konieczności weryfikacji za pomocą odcisku palca. Zamiast tego użytkownik może wykorzystać hasło lub kartę w celu uzyskania dostępu. Konfiguracja jest wykonywana tak samo jak przy departamentach.

## 4.7. Admnistration – Terminal Status

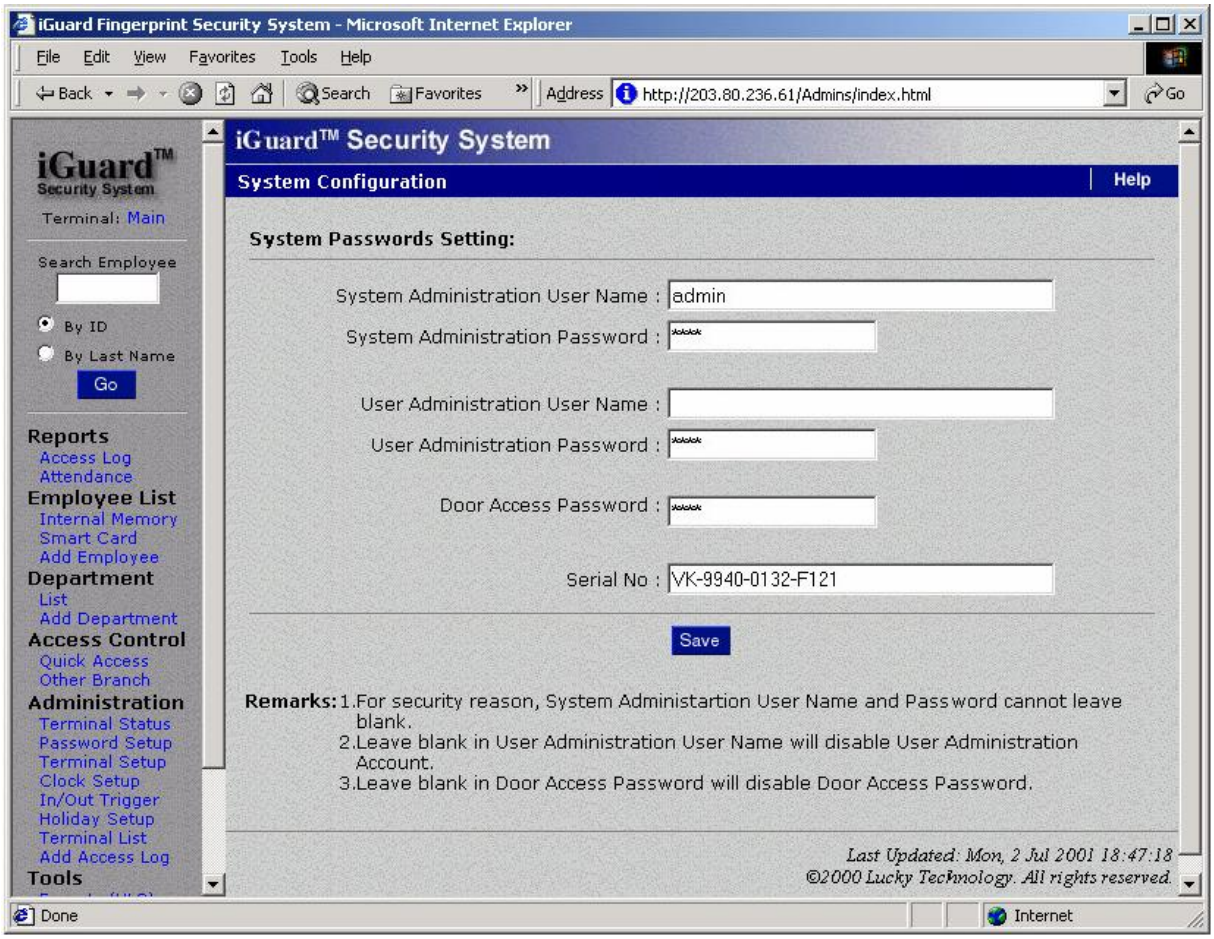
Poniższa strona domowa terminalu pokazuje wszystkie główne parametry urządzenia włączając w to numer seryjny.



## 4.8. Administration – Password Setup

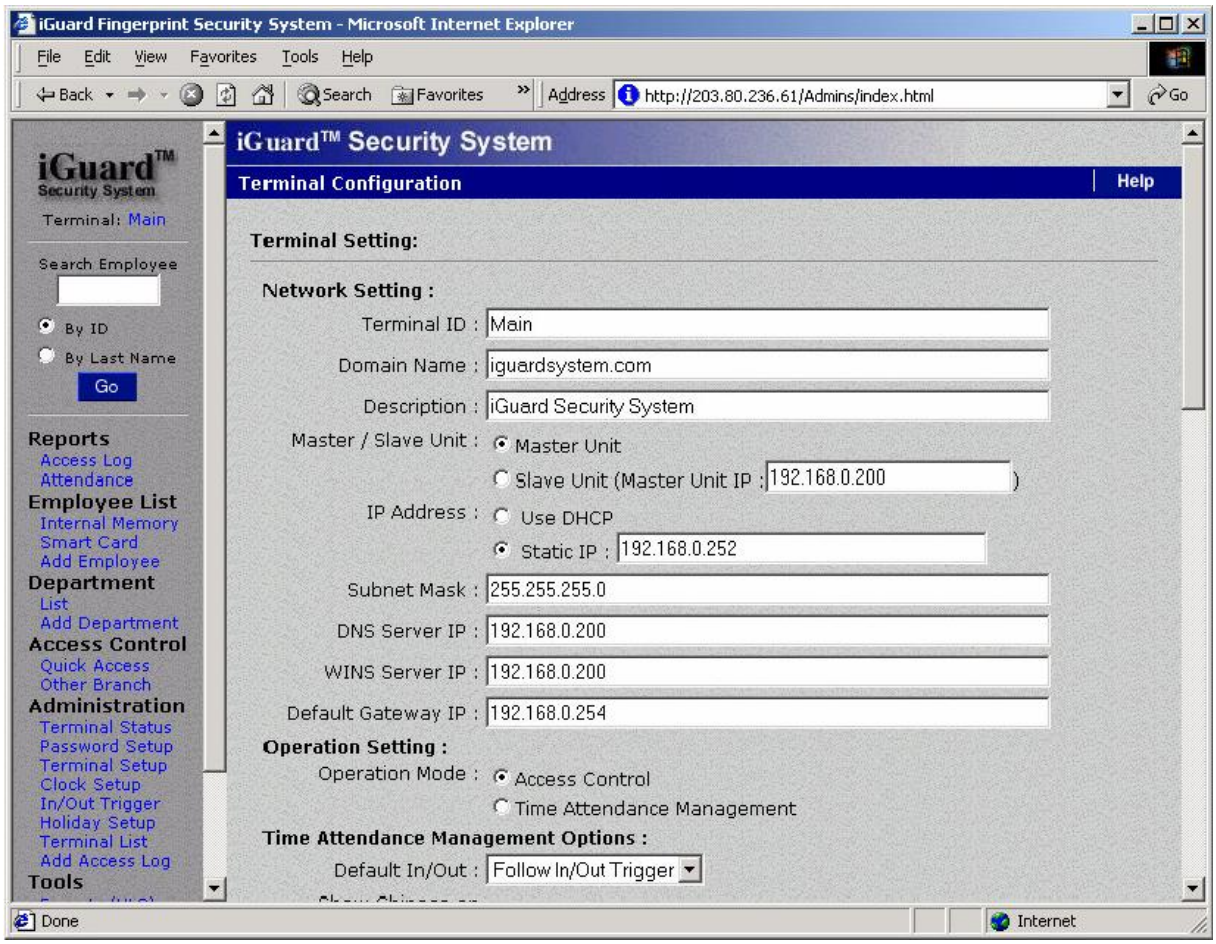
Ustawianie hasła Administratora i Door Access Password:

- System Administrator – ustawienie hasła dla administratora systemu
- User Administrator – Podobne prawa dostępu jak System Administrator z tym, że nie może konfigurować urządzenia.
- Door Access Password – Hasło otwarcia drzwi stosowane w czasie dużego natężenia ruchu kiedy wymogi wysokie go bezpieczeństwa nie są konieczne.



## 4.9. Administration – Terminal Setup

Wybierz Terminal Setup:



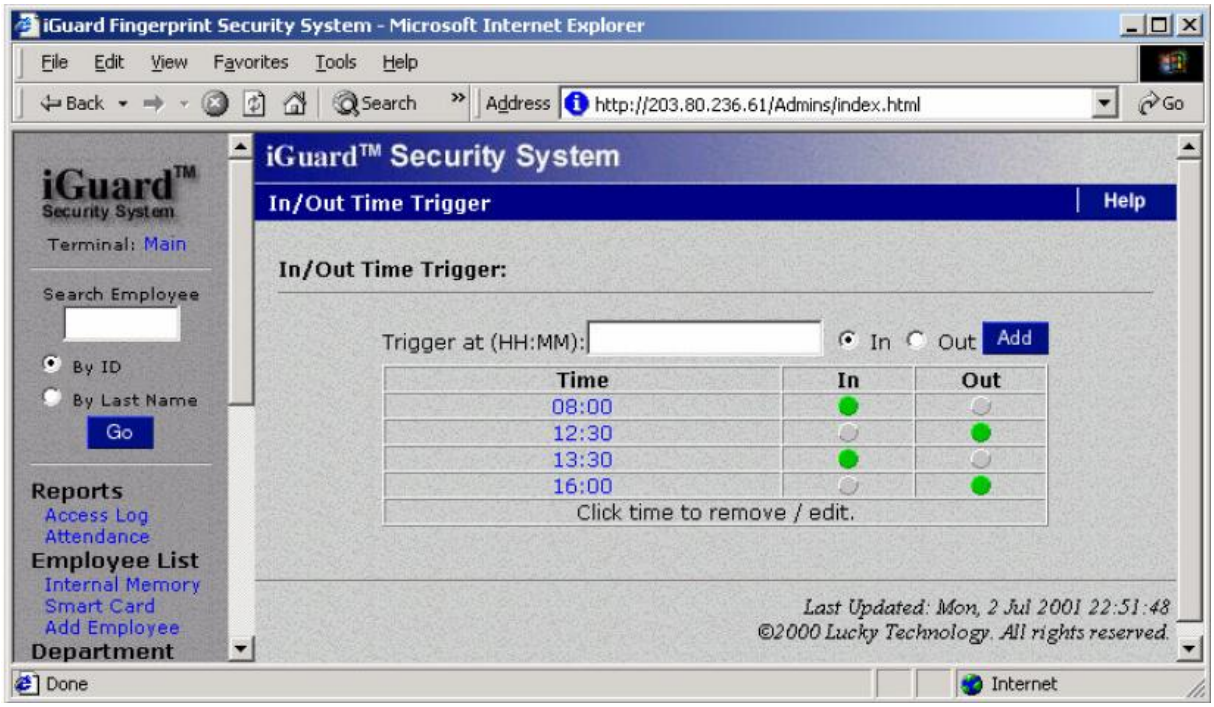
## 4.10. Administration – Lock Setup

Auto Date/Time: Automatycznie ustawia synchronizację czasu dla iGuard z komputerem.
Location (Time Zone): Strefa czasowa dla regionu w jakim zainstalowany jest iGuard.
Serial No.: Unikalny numer seryjny urządzenia.

Na żądanie dostępne jest oprogramowanie specjalne przeznaczone do synchronizacji zegara z terminalu z komputerem. Jeśli urządzenia pracują w sieci master/slave wszystkie terminale slave automatycznie są aktualizowane z urządzenia master.

## 4.11. Administration – In / Out Trigger

Automatyczny „spust" dla IN i OUT pozwala na ustawienie Kidy system automatycznie będzie się przełączać w tryb rejestracji IN i OUT.




Spust IN/OUT ma zastosowanie jedynie w systemach rejestracji czasu pracy. Powyższy rysunek pokazuje, że system od 8:00 automatycznie będzie zliczać czas jako IN, a od 12:30 jako OUT itd.

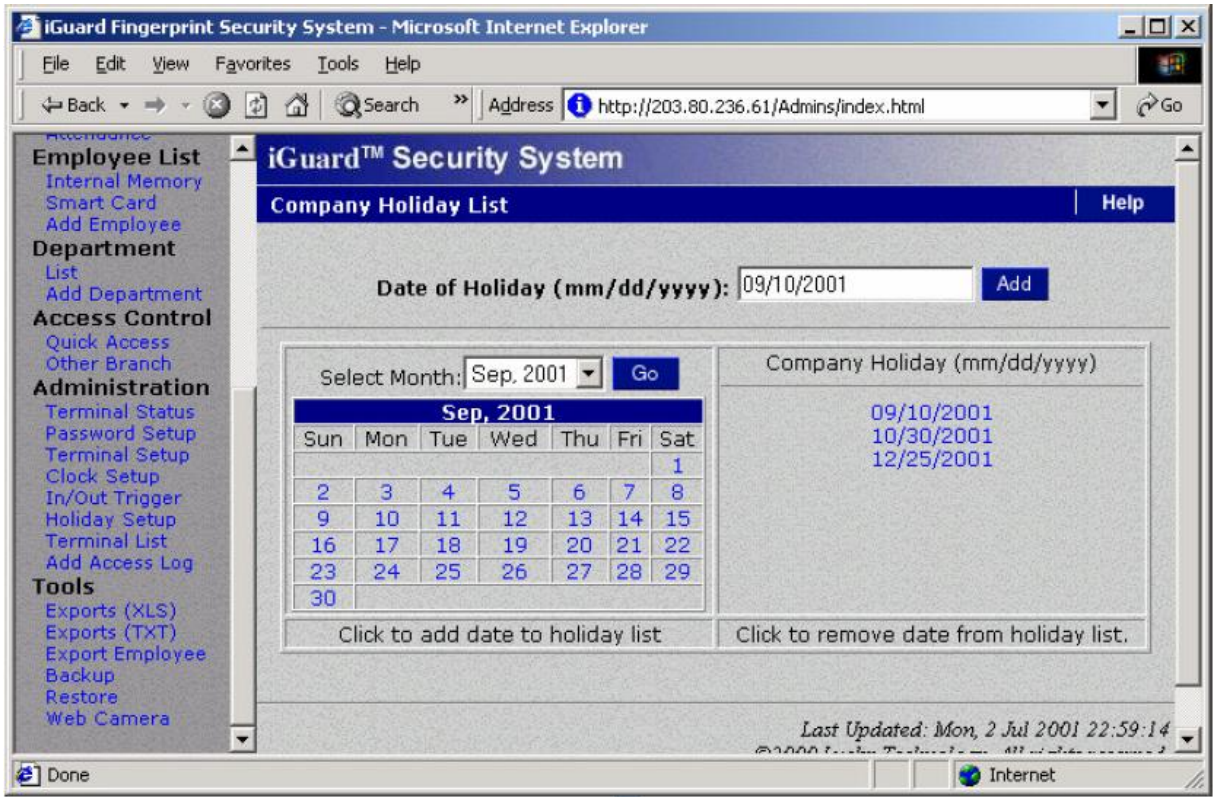
Wyświetlanie zaliczanego czasu pracy na urządzeniu

| **Opis** | **Wyświetlacz LCD** |
|---|---|
| Domyślnie IN (standardowe przy rejestracji czasu pracy na wejście) | Monady 30 13:49<br>ID#_ IN |
| Domyślnie OUT (standardowe przy rejestracji czasu pracy na wyjście) | Monady 30 13:49<br>ID#_ OUT |

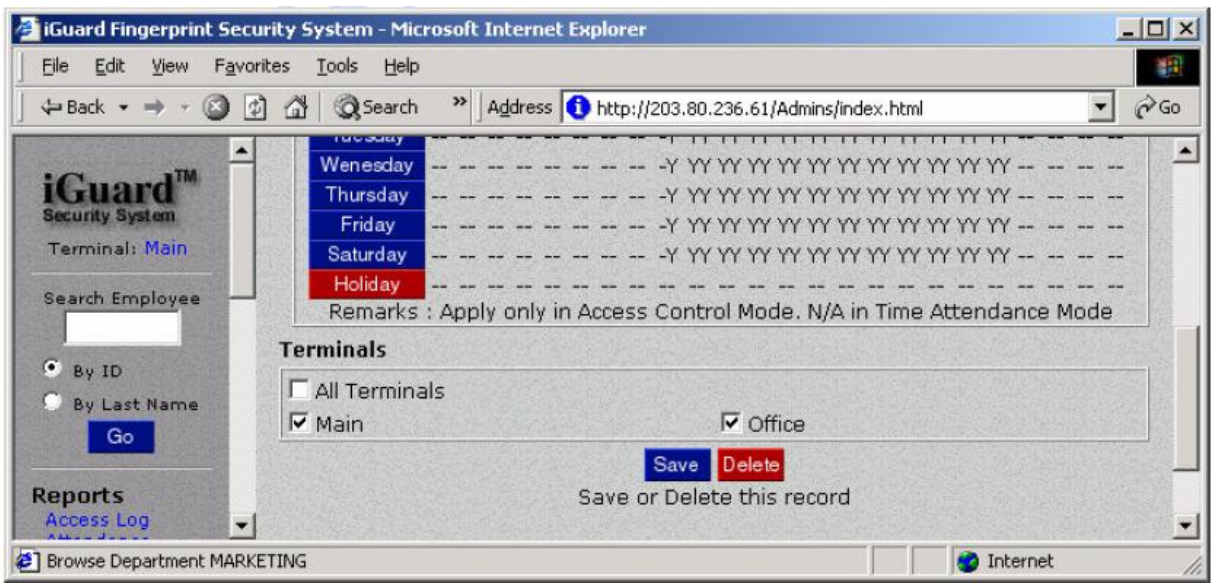
Ustawioną domyślną wartość można zmienić wciskając za każdym razem klawisz backspace.

## 4.12. Administration – Holiday Setup

W poniższym oknie wyświetlane są wpisane do systemu wolne dni.

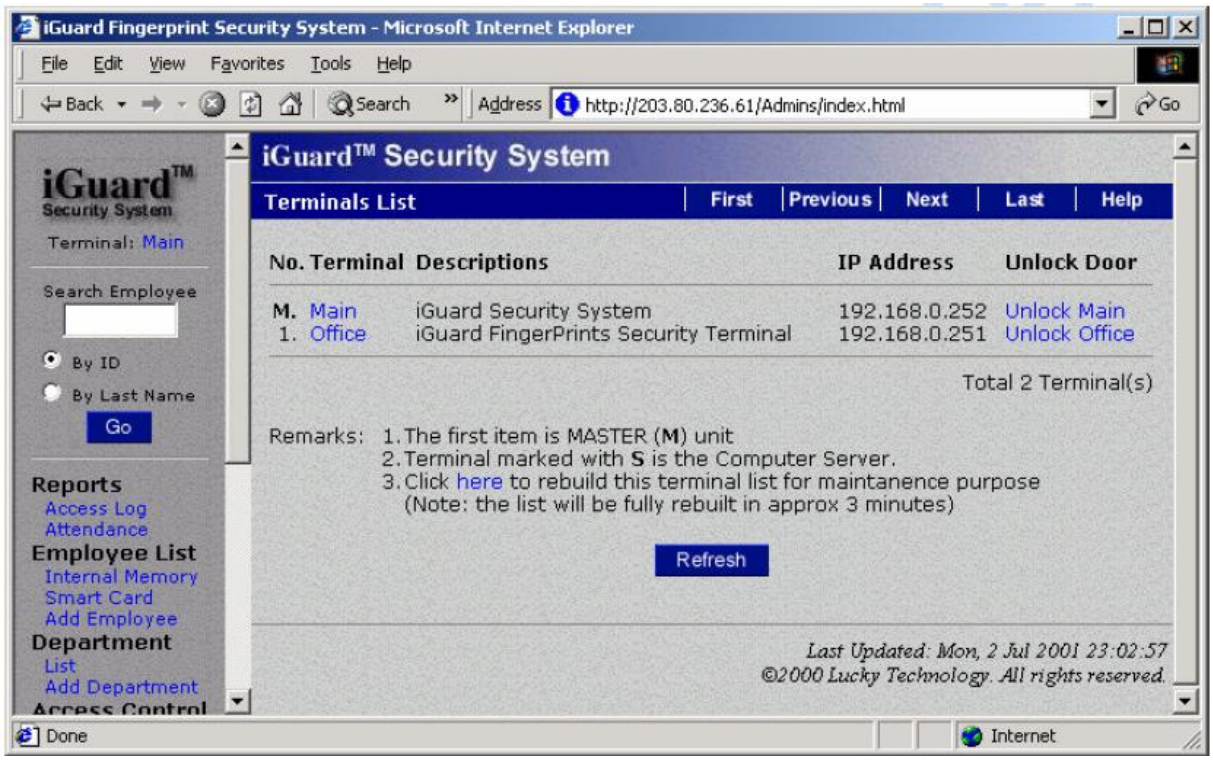



Konsekwencją tych ustawień będzie zabroniony dostęp do systemu dla członków grupy Office.
Zapoznaj się z sekcją Depatment - List



## 4.13. Administration – Terminal list

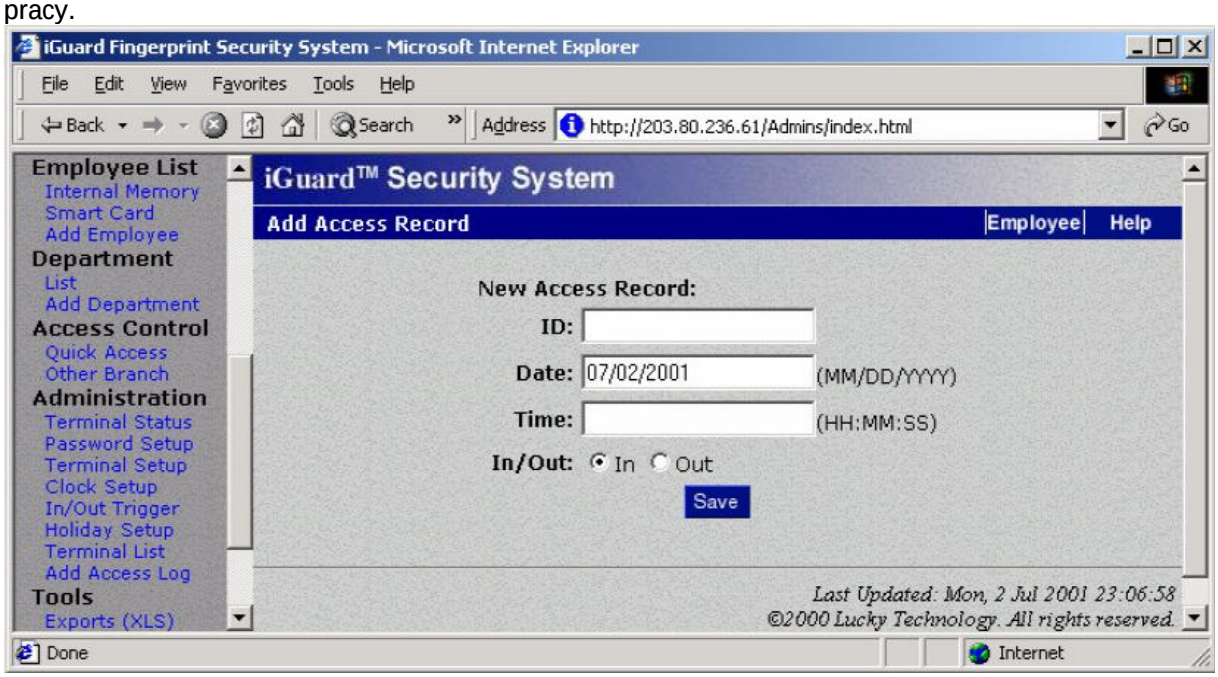
Poniższa strona pokazuje listę urządzeń slave oraz urządzenie master.



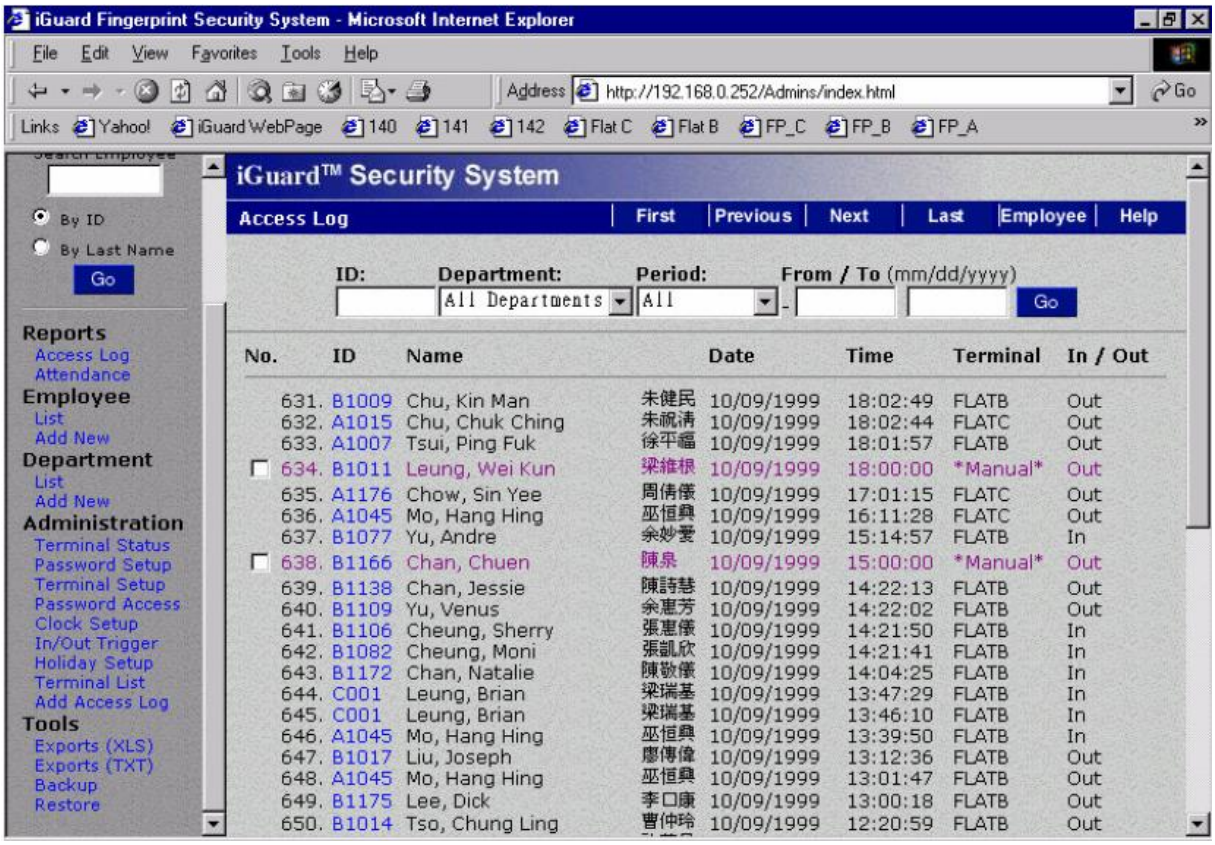

Urządzenie master oznaczone jest literką „M". Dodatkowo pokazany jest także adres IP każdego urządzenia. Jeśli istnieje taka potrzeba można wydać zdalne polecenie otwarcia drzwi klikając na link Unlock Main, Unlock Office, itp.
Terminale można też zresetować klikając na link Reset przy każdym terminalu.

## 4.14. Administration – Add Access Log

W szczególnych przypadkach administrator może sam dopisać w systemie odpowiednie zdarzeń zakwalifikowane jao wejście (IN) lub wyjście (OUT). Stosowane jest to do celów rejestracji czasu pracy.



Rekordy dopisane ręcznie są zaznaczone innym kolorem, mogą też być usuwane w przeciwieństwie do standardowych rekordów zarejestrowanych przez czytniki.

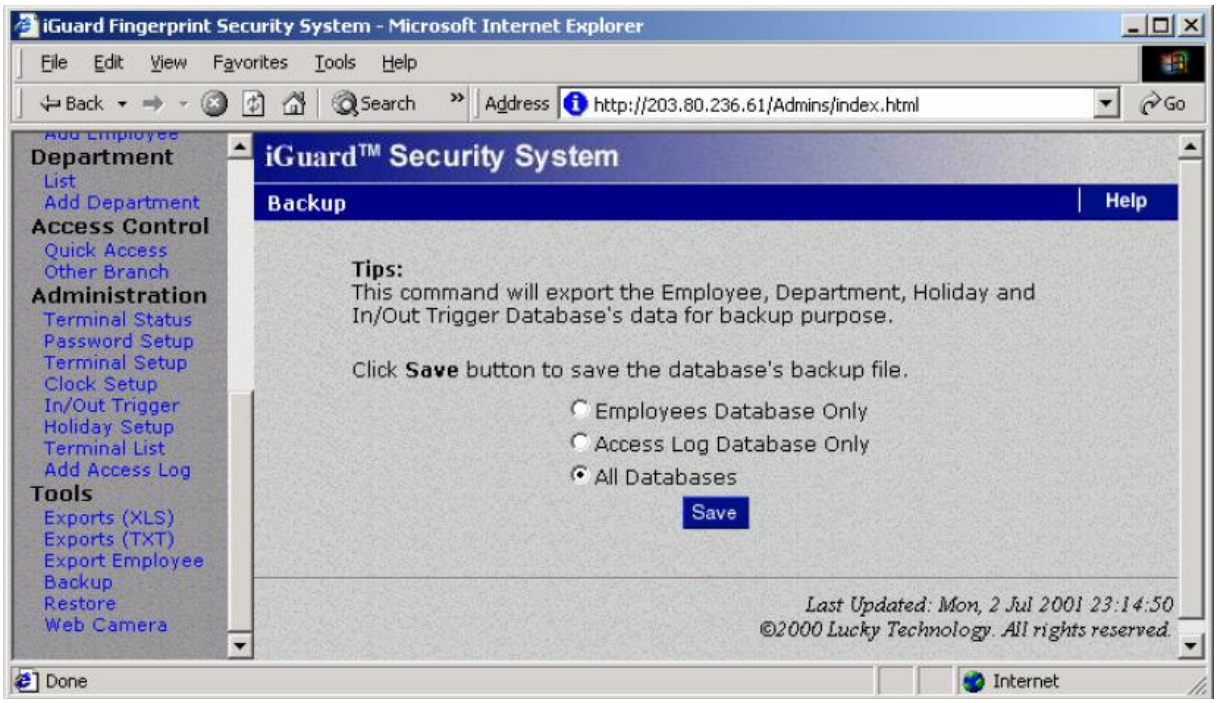



## 4.15. Tools – Export Employee

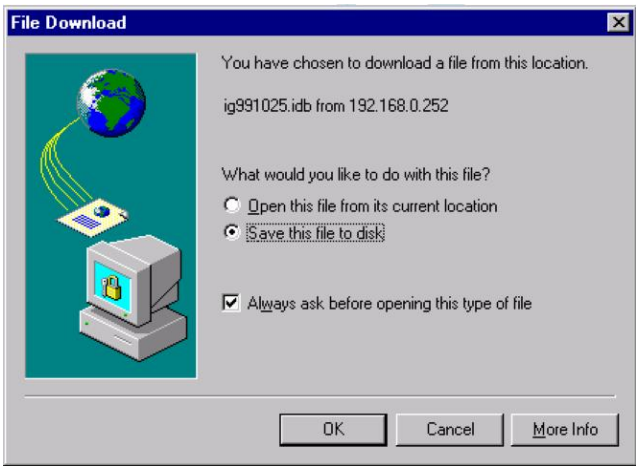
Wybierz Export aby wyeksportować określonych użytkowników lub ich grupę.

## 4.16. Tools – Backup & Restore

Zaleca się aby dane z czytników były archiwizowane okresowo, szczególnie po zmianie użytkowników oraz w celu zabezpieczenia zapisanych zdarzeń. W sytuacji awarii nowe urządzenie może szybko zastąpić uszkodzone bez konieczności ręcznego odtwarzania jego konfiguracji.

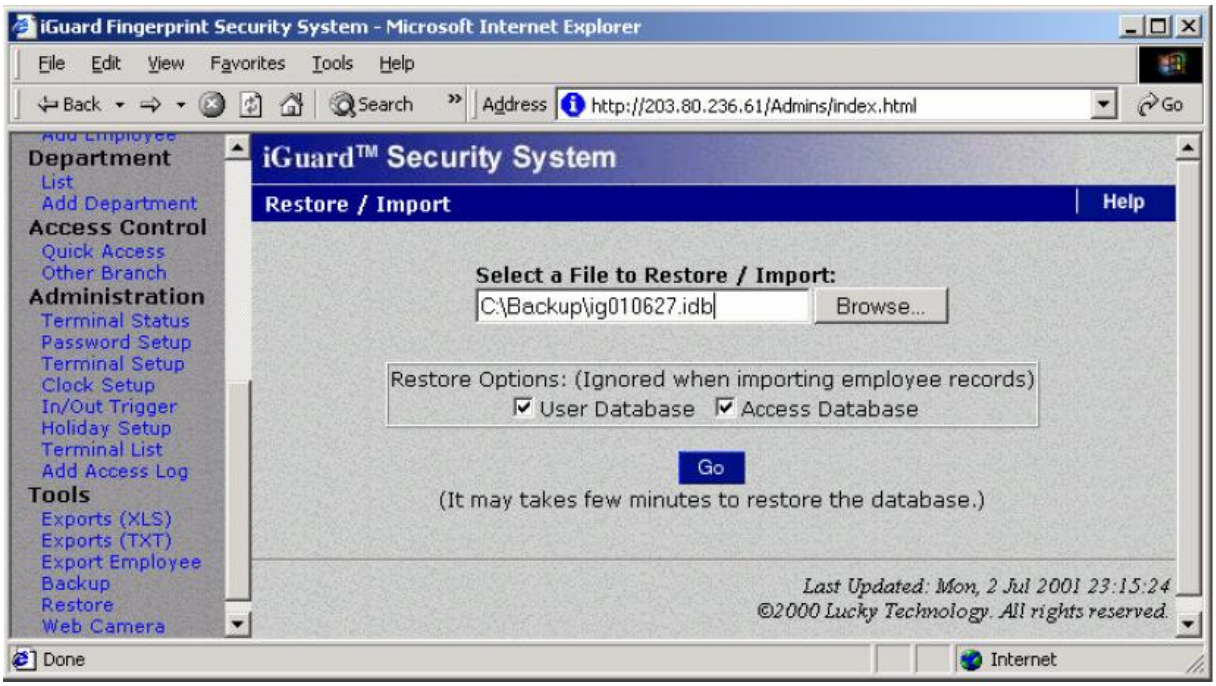



Wybierz save aby pojawiło się poniższe okno dialogowe.



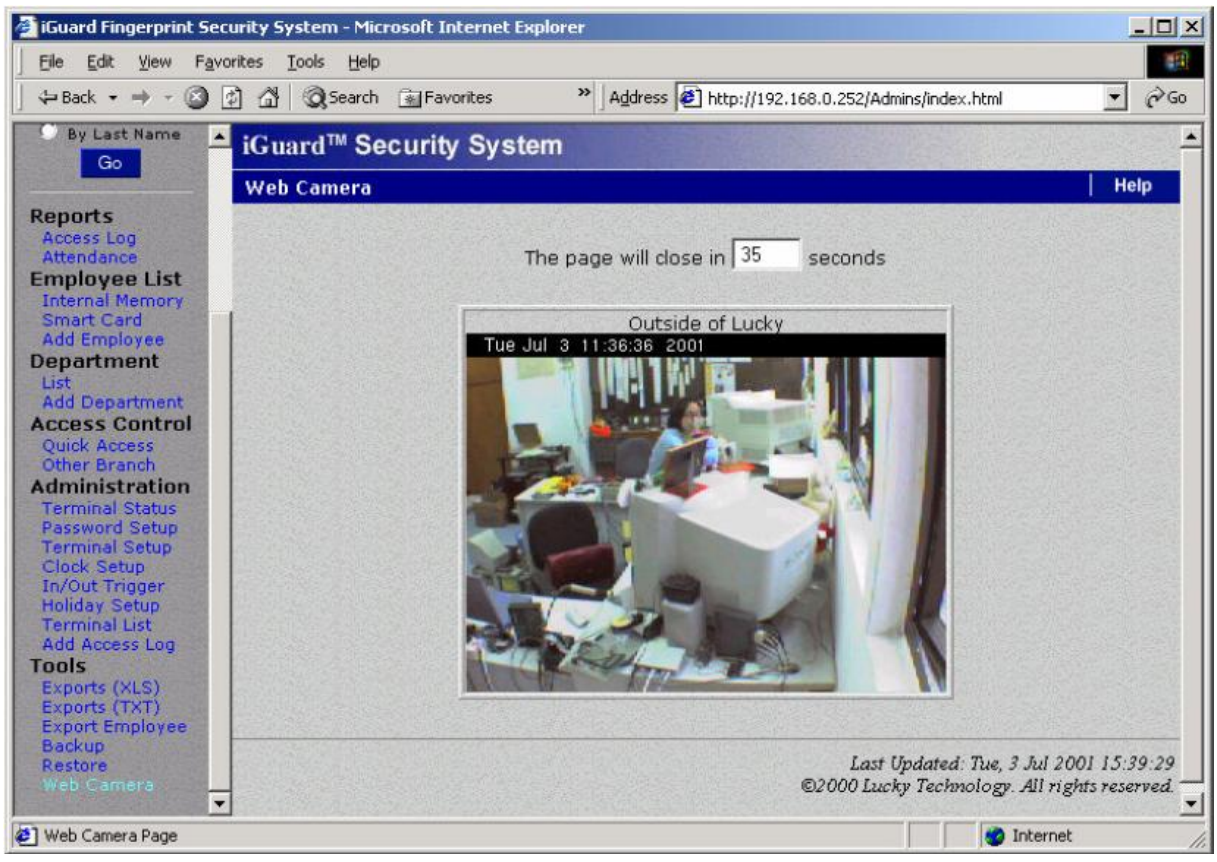

Kliknij OK. aby zapisać plik danych zarchiwizowanych.

Jeśli istnieje konieczność odtworzenia danych można to zrobić za pomocą Tools – Restore a następnie wskazać plik z archiwum. Wybierz jaką część archiwum chcesz odtworzyć a następnie zatwierdź klikając „Go”.




## 4.17. Tools – Web Camera

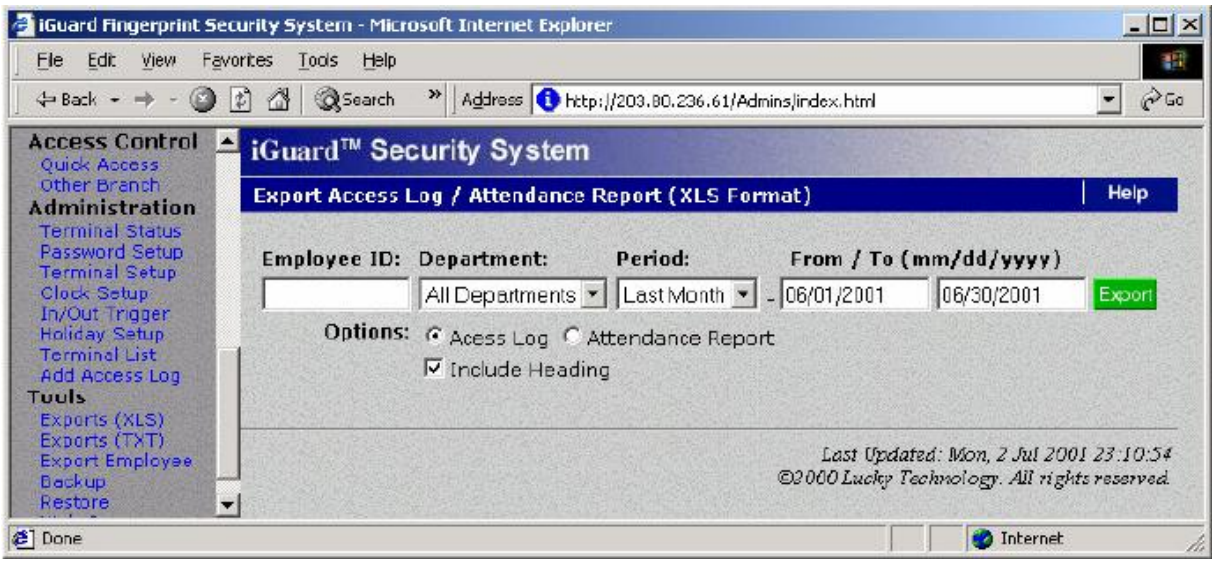
iGuard umożliwia podłączenie sieciowej kamery IP w celu obserwacji obrazu z otoczenia czytnika. Można podłączyć do pojedynczego do 4 kamer.



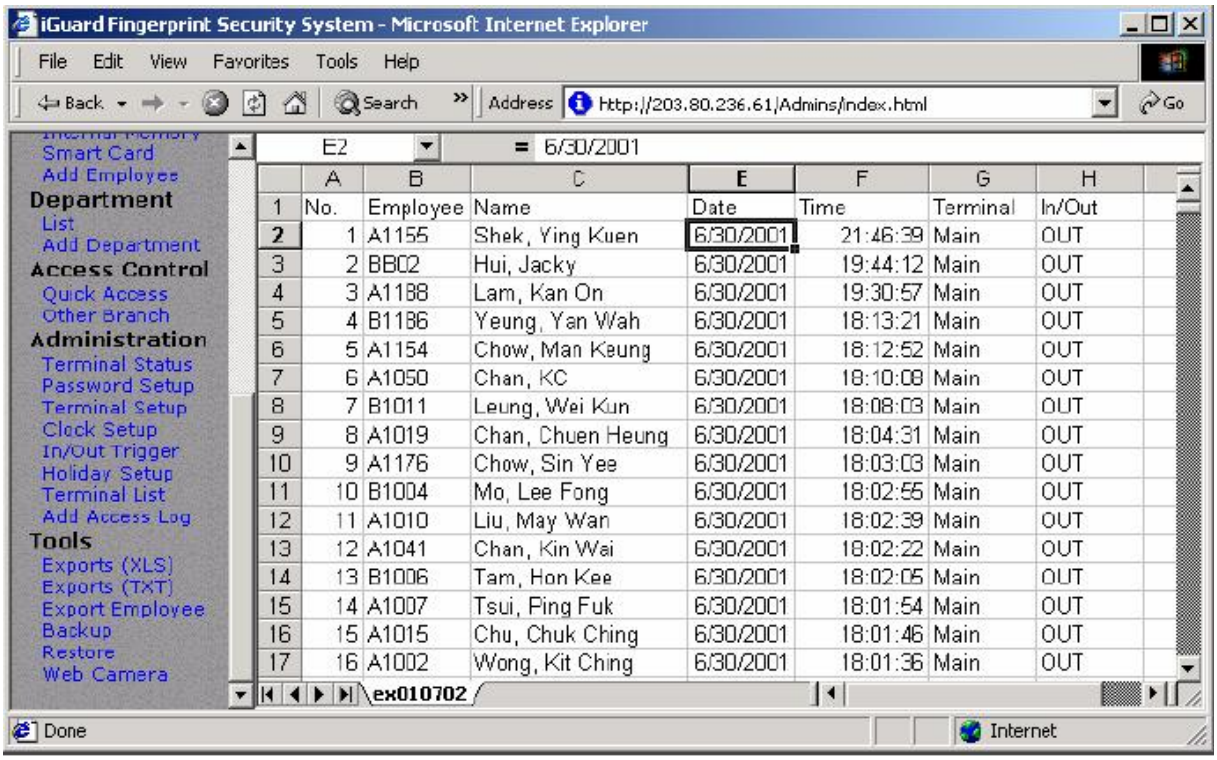
# 5. RAPORTOWANIE

## 5.1. Tools – Export (XLS)

Raporty (włączając w to raporty obecności I kontroli dostępu) mogą być eksportowane bezpośrednio do popularnych formatów takich jak XLS który umożliwia łatwą integrację z pakietem MS Office i programem MS Excel. Na podstawie standardowych formularzy łatwo można wygenerować inne raporty za pomocą pakietu Office.




Poniże prezentowany jest przykładowy raport wygenerowany w standardu MS Excel 5.0



## 5.2. Tools – Export (TXT)

Plik tekstowey przydaje się do exksportowania danych dla krogramów kadrowo płacowych.

Format pliku tekstowego jest następujący:

"Item","Employee ID","Name","Other Name","Date","Time","Terminal","In/Out"

"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. Reports – Access Log

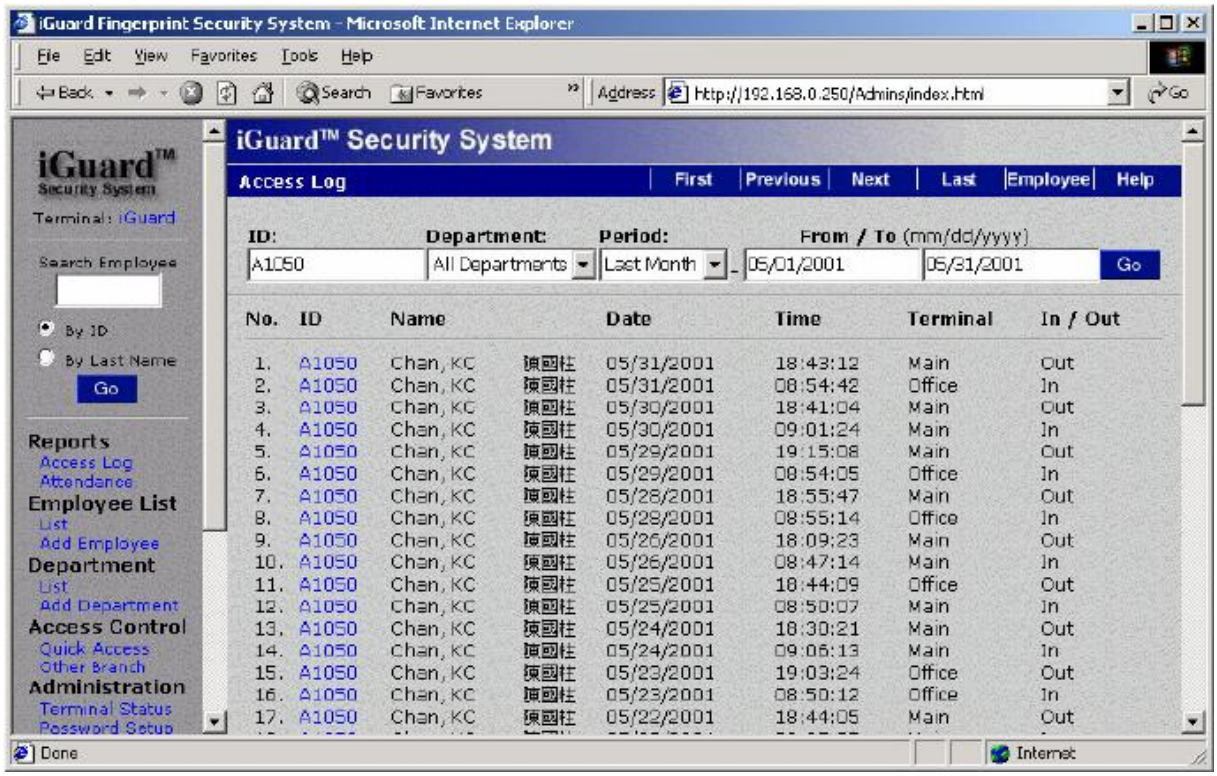
Kliknij na link Access Log w prawym panelu a na ekranie pojawi się strona podobna do poniższej.


Powyższa strona pokazuje rekordy kontroli dostępu. Jeśli chcesz zobaczyć rekordy dotyczące tylko jednej osoby (np. C001) wpisz ID tej osoby w polu edycji ID: a następnie kliknij klawisz Go. Przeglądarka wyświetli tylko rekordy należące do określonej osoby.

Dodatkowo można też określić departament, przedział czasowy według listy wyboru Perod lub poprzez podanie konkretnych dat.

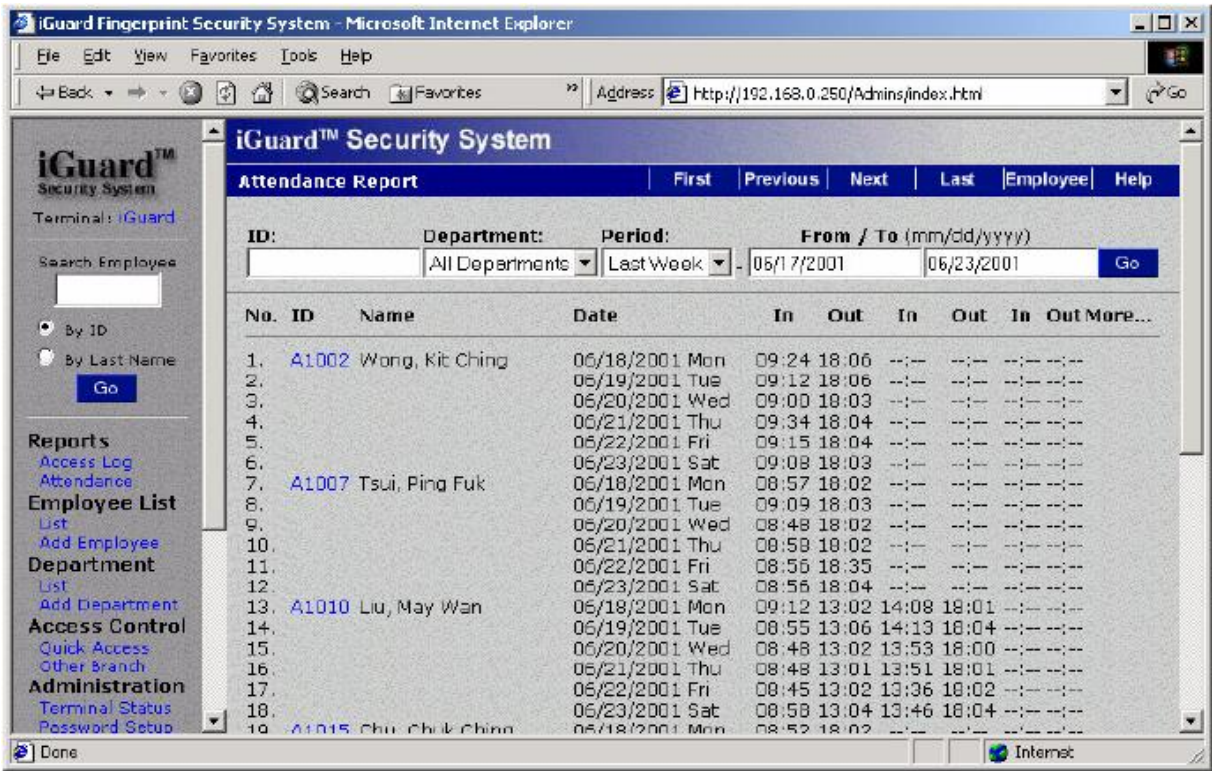
Jeśli mimo to ilość rekordów według określonego kryterium przekracza jeden ekran dodatkowo mamy do dyspozycji klawisze nawigacyjne pozwalające na przełączanie się pomiędzy poszczególnymi ekranami.

Poniższy rysunek pokazuje rekordy dotyczące określonej osoby (ID: A1050) w poprzedzającym miesiącu:



## 5.4. Reports Attendance

Raporty obecności pokazują skonsolidowane zestawienia na temat obecności pracowników wpracy:

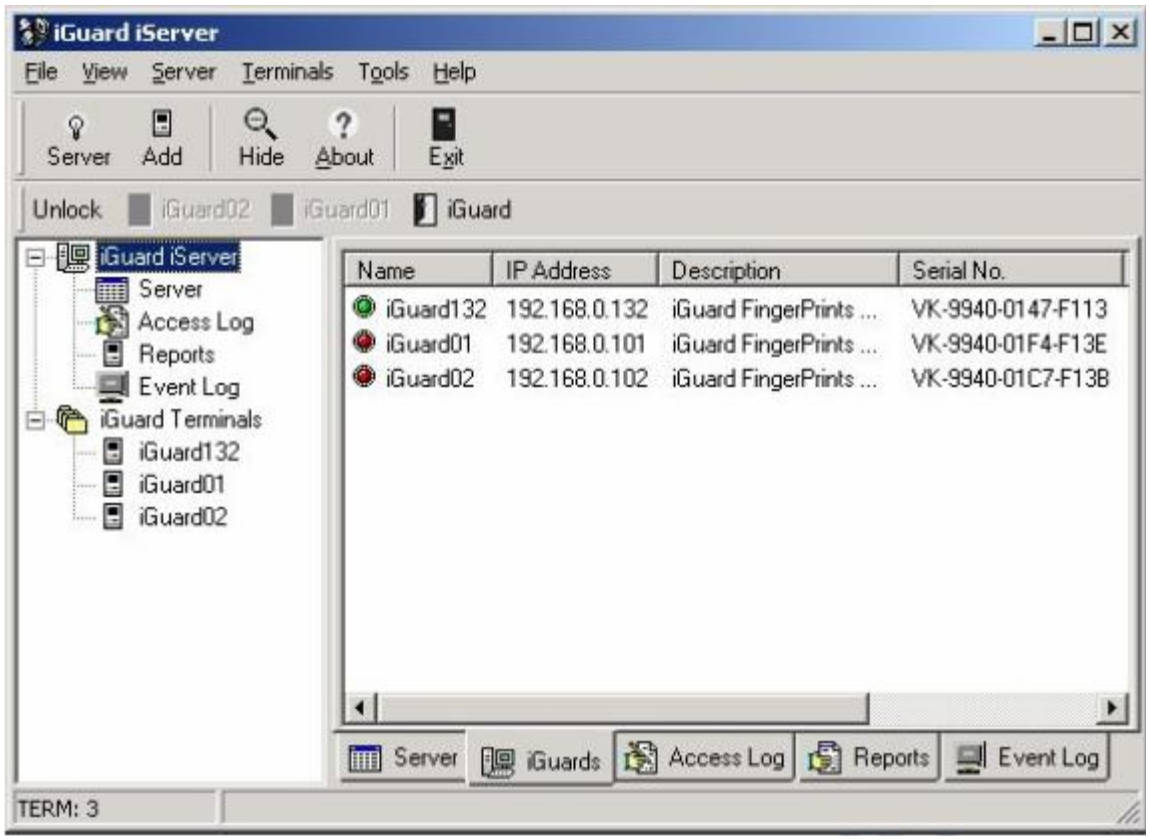



Raporty obecności wykorzystuje system kadrowo płacowy. Podobnie jak w raportach z kontroli dostępu można je określić co do osoby, czasu i departamentu.

## 5.5. iServer

iServer jest aplikacją Windows służącą do zapisywania na oddzielnym serwerze zdarzeń rejestrowanych przez terminale iGuard. Dodatkowo iServer jest aplikacją dzięki której poprzez łatwy do obsługi interfejs ODBC można przesyłać lub wymieniać dane z innymi systemami np. kadrowo płacowymi lub rejestracji czasu pracy.

Jeśli chcemy korzystać z zalet ODBC i zapisywać dane w bazie o formacie innym niż MS Access kolejne kroki pokażą jak należy skonfigurować iServer aby było to możliwe.




**Tworzenia Bazy Danych**
Trzeba utworzyć bazę danych oraz jej dwie tabele. Dla ułatwienia poniżej prezentujemy format konfiguracji tabel i pól dla bazy serwera iServer.

## 5.5.1. MS Access

**Tabela: AccessLog**

RCDID Int AUTO_INCREMENT,

EmployeeID char(16),

LogDate char(10),

LogTime char(10),

TerminalID char(20),

InOut Int,

Primary Key(RCDID, EmployeeID, LogDate, LogTime, TerminalID)

**Tabela: Employee**

EmployeeID char(16),

LastName char(40),

FirstName char(40),

OtherName char(40),

Password char(16),

EmpStatus Int,

NumMinutiae1 Int,

NumMinutiae2 Int,

PhotoFile char(40),

Minutiae1 image,

Minutiae2 image,

Photo image,

Department char(50),

Primary Key(EmployeeID)

Należy pamiętać że Istnieją pewne różnice w formatowaniu pól dla bazy zależnie od serwera SQL. Poniższe parametry są wyjściowymi dla serwerów SQL.

## 5.5.2. SQL Server

**Tabela AccessLog:**

RCDID Int IDENTITY yes,

EmployeeID char(16),

LogDate char(10),

LogTime char(10),

TerminalID char(20),

InOut Int,

Primary Key(RCDID, EmployeeID, LogDate, LogTime, TerminalID)

**Tabela Employee:**

Taka sama jak w MS Access

Dla baza danych opartych na serwerze SQL koniczne jest stworzenie odpowiedniego DSN aby umożliwić programowi dostęp do serwera.

## 5.5.3. Oracle

**Tabela: AccessLog**

RCDID Number(38) Not Null, <- Contraint – Auto Increment field

EmployeeID Char(16) Not Null,

LogDate Char(10) Not Null,

LogTime Char(10) Not Null,

TerminalID Char(20) Not Null,

InOut Number(38)

**Tabela: Employee**

EmployeeID Char(16) Not Null,

LastName Char(40),

FirstName Char(40),

OtherName Char(40),

Password Char(40),

EmpStatus Number(38),

NumMinutiae1 Number(38),

NumMinutiae2 Number(38),

PhotoFile Char(40),

Minutiae1 BLOB,

Minutiae2 BLOB,

Photo BLOB,

Department Varchar2(50)

Istnieje kilka sposobów utworzenia tabel na serwerze Oracle oraz pól typu autoincrement (RCDID). Poniższa metoda jest najpopularniejsza:

1. Aby utworzyć tabelę:
    - § Za pomocą narzędzi administracyjnych w Oracle do tworzenia tabel (w Oracle 8 lub wyżej)
    - § Za pomocą komend SQL do tworzenia tabel w SQL Plus lub SQL Worksheet
2. Aby utworzyć pole auto_increment (RCDID)
    - § To create a sequence and add a constriant to a field, or ;
    - § Create a trigger to increment the field.

Tak samo jak w innych serwerach SQL należy utworzyć login I hasło dostępu do bazy. Konto powinno umożliwiać dostęp do obu tabel bazy z prawem INSERT.

Testowanie (Opcja)

1. Użyj SQL Plus aby się zalogować jako użytkownik dla iServer'a
2. Spróbuj wykonać komendę SELECT i INSERT na obu tabelach bazy.

## 5.5.4. Tworzenie Data Source Name (DSN)

Panel Sterowania → Narzędzia Administracyjne → ODBC → System DSN →Dodaj

Dla serwerów SQL i baz Oracle procedura jest identyczna.
Proszę wpisać nazwę dla DSN jako „Server”.
W przypadku serwerów SQL można użyć loginu „sa” który posiada największe uprawnienia w systemie.

# 6. MASTER/SLAVE

## 6.1. Master vs. Slave

W wieloczynnikowym systemie złożonym z terminali iGuard zawsze jeden z nich pełni rolę Master, pozostałe zaś pracują jako slave.

Zanim dana osoba zostanie zweryfikowana przez czytnik najpierw musi zapisać swój wzorzec w systemie. Operacja ta może być wykonana z dowolnego urządzenia. Innymi słowy osoba raz zarejestrowana na dowolnym czytniku może być zweryfikowana automatycznie na wszystkich pozostałych bez konieczności rejestracji na każdym z nich indywidualnie. Ssytem automatycznie replikuje wzorce na pozostałe czytniki. Użytkownik automatycznie uzyskuje w ten sposób dostęp do przejść określonych w programie konfiguracyjnym.

Analogicznie do wzorców wszystkie zdarzenia rejestrowane na czytnikach (IN/OUT) połączonych w sieć są automatycznie przesyłane do urządzenia Master. Tak więc urządzenie master zawiera wszystkie informacje o przejściach. Dlatego aby uzyskać pełną informację o pracy systemu jak dokonać nowych rejestracji, czy zarządzać dostępem wystarczy podłączyć się do urządzenia master i za pomocą przeglądarki internetowej dokonać niezbędnych zmian, które system samodzielnie roześle do pozostałych urządzeń typu slave.

Urządzenia Master i Slave mogą być połączone logicznie poprzez sieć Ethernet protokołem TCP/IP. Za pomocą kabla RJ45 urządzenia podłącza się do sieci korporacyjnej. Aby uzyskać prawidłowe połączenie z siecią LAN w pierwszej kolejności należy skonfigurować adres IP urządzenia oraz określić czy urządzenie pełni rolę master czy slave.

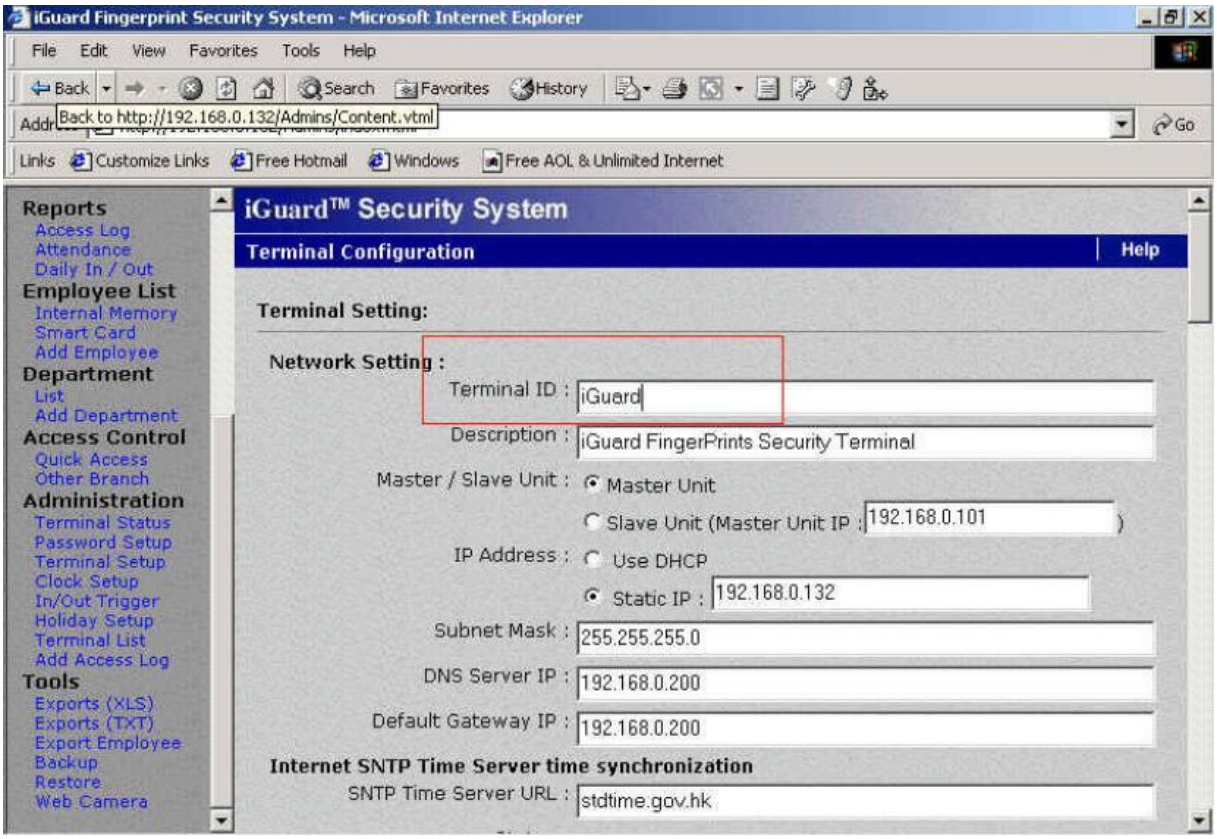
Tworząc użytkowników i dodając ich do określonych czytników nadaje się im jednocześnie prawa dostępu do określonych przejść. Oznacza to, że dostęp określony jest do konkretnych przejść sterowanych przez ściśle określone urządzenia. Operację tą wykonuje się poprzez powiązanie grup użytkowników – Departamentów z określonymi czytnikami. Osoby przypisywane pewnej grupie automatycznie uzyskują dostęp do przejść powiązanych z daną grupą.

W celu synchronizacji zegara czasu musisz skonfigurować urządzenia w układzie master/slave.

UWAGA: Urządzenia serii LM nie mogą być mieszane w sieci master/slave z urządzeniami starego typu serii FPS110.

## 6.2. Ustawienie ID Terminalu

Nazwa każdego terminalu powinna być zmieniona, domyślna jest iGuard. Zmiana nazwy jest Terminal ID jest konieczna dla prawidłowej pracy urządzeń w sieci. Zmiany parametru Terminal ID musi być wykonana na wszystkich urządzeniach.



## 6.3. Super Master

Super Master to urządzenie służące do budowy systemów oparty o większą liczbę użytkowników niż tylko 1000 osób wykorzystujących urządzenia serii LM w układzie master/slave. Z urządzeniem SuperMaster terminale serii LM pracują w trybie cache slave co oznacza że w ich pamięci znajduje się tylko do 1000 ostatnio używanych wzorców/kont.

# 7. POZOSTAŁE ELEMENTY SYSTEMU

## 7.1. Zdalny sterownik przejścia.

Zdalny sterownik służy do absolutnie bezpiecznego sterowania przejściem. W tym przypadku nie jest wykorzystywane zwykłe wyjście open collector dostępne w iGuard. Zamiast tego wykorzystuje się połączenie RS485. Zdalny sterownik montowany jest wewnątrz strefy bezpiecznej a komunikacja z terminalem jest zabezpieczona.

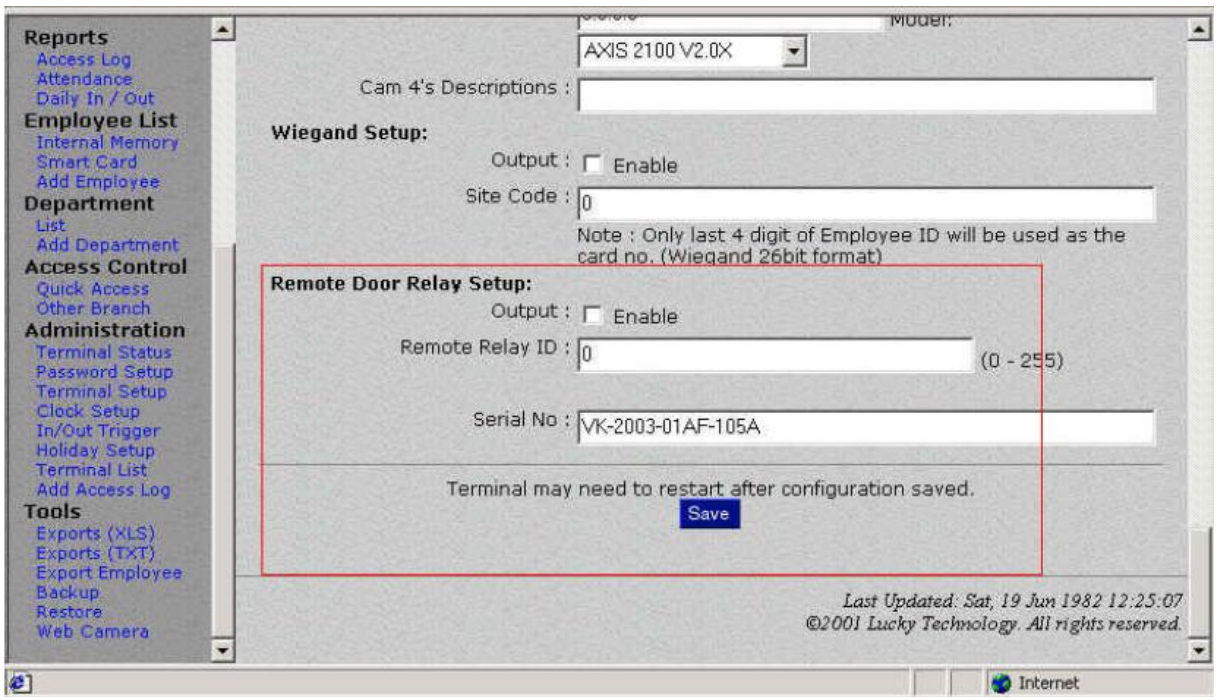
Opis wyjść sterownika:

| | |
|---|---|
| **NO** | **Przekaźnik drzwi normalnie otwarte** |
| **COM** | **Przekaźnik drzwi masa** |
| **NC** | **Przekaźnik drzwi normalnie zamknięte** |
| **DOOR SW** | **Przełącznik drzwi** |
| **DOOR SW** | **Przełącznik drzwi** |
| **A-RS485** | **Podłączenie do iGuard** |
| **B-RS485** | **Podłączenie do iGuard** |
| **+12VDC** | **Zasilanie +12V** |
| **GND** | **Uziemienie** |

Ustawienia przełączników (DIP Switch)
Ustaw osiem przełączników kontrolera aby określić odpowiednie ID. Każdy z przełączników reprezentuje sobą odpowiednią wartość tak aby ich suma dawała odpowiednią liczbę określoną w konfiguracji iGuard w przedziale od 0 – 255.

| Switch | Numer | Wymagania |
|---|---|---|
| 1 | 1 | W celu poprawnego skonfigurowania połączenia wymagane są dodatkowe ustawienia na terminalu iGuard. |
| 2 | 2 | 1. Wersja Firmware: 3.2.9987A lub wyżej (można wykonać aktualizację) |
| 3 | 4 | |
| 4 | 8 | 2. W oknie konfiguracji Terminalu iGuard należy zaznaczyć checkbox output w Remote Door Relay Setup |
| 5 | 16 | |
| 6 | 32 | 3. Jeśli to nie pomoże należy skontaktować się z serwisem w celu otrzymania uaktualnienia firmware |
| 7 | 64 | |
| 8 | 128 | |

Uaktywnienie komunikacji w konfiguracji terminala

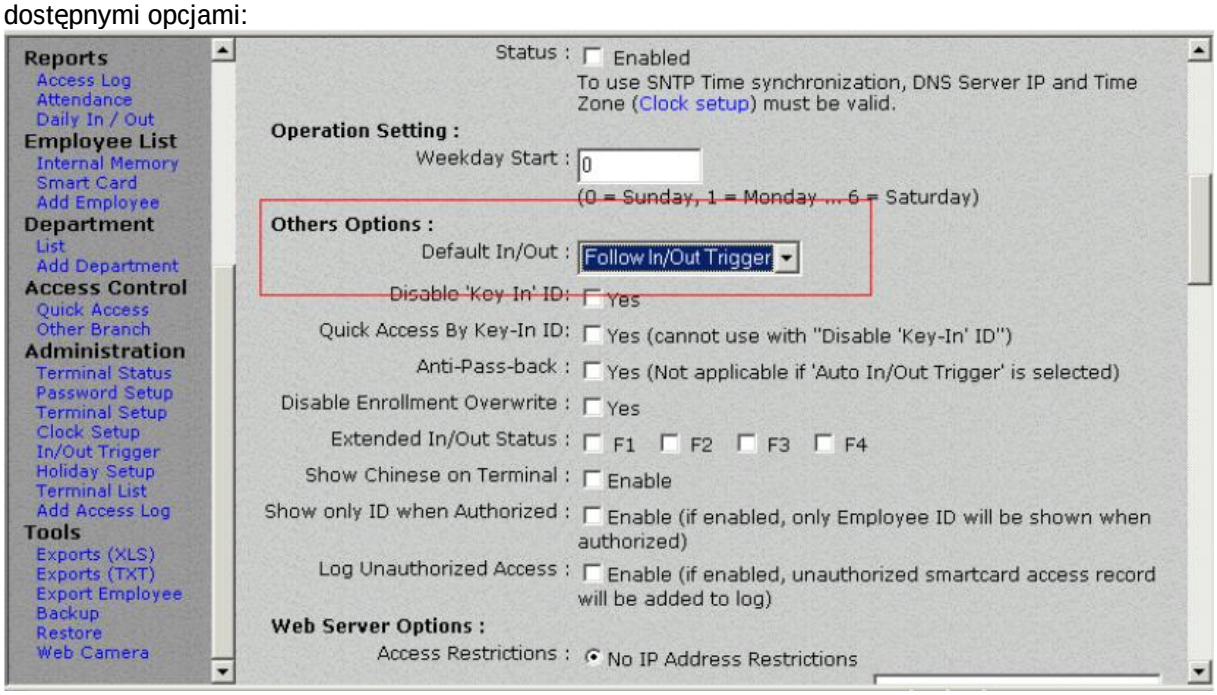


## 7.2. Różne tryby pracy funkcji IN/OUT.

**Opisane poniżej funkcje nie są zawarte w standardowej wersji urządzeń serii LM. W celu ich aktywacji należy się skontaktować ze sprzedawcą.**

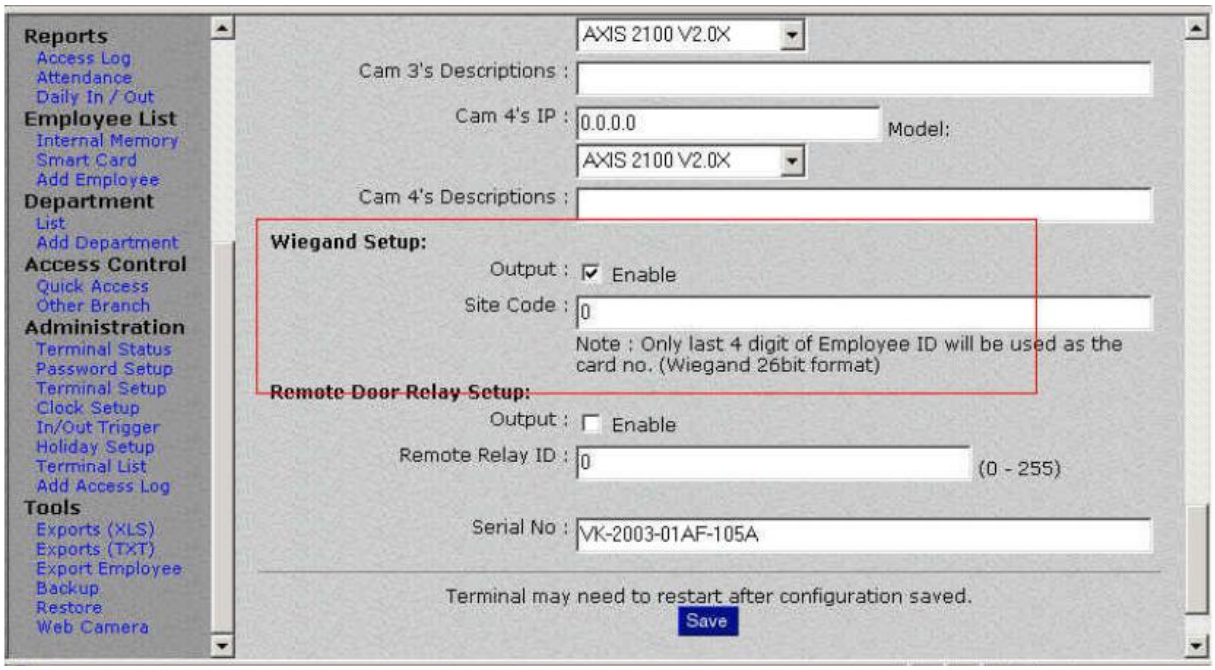
| Tryby pracy | Opis |
|---|---|
| Follow IN/OUT Trigger (domyślny) | Jeśli wybrna jest wartość domyślna tego parametru ustawienia przełącznika IN/OUT są ustawiane w In/Out Trigger Setup (patrz sekcja Administracja – IN/OUT Trigger) |
| Always OUT | To ustawienie powoduje zaliczanie każdej weryfikacji jako OUT |
| Always IN | To ustawienie powoduje zaliczanie każdej weryfikacji jako IN |
| Don't Show | To ustawienie powoduje zaliczanie każdej weryfikacji jako IN |
| Auto IN/OUT Trigger | Powoduje automatyczne przełączanie pomiędzy IN I OUT |
| Extended IN/OUT Status | Dodatkowo poza IN I OUT dostępne są oznaczenia F1, F2, F3, F4 które należy ręcznie wybierać za pomocą przycisku return (←) z klawiatury terminalu. Odpowiednie zapisy zostaną również umieszczone w systemie logów. Stosownie do wymagań oznaczenia F1 – F4 mogą być przypisane określonym czynościm. |

Wybierz Terminal setup, Domyślne ustawienie „Default In/Out może być ustawione zgodnie z dostępnymi opcjami:



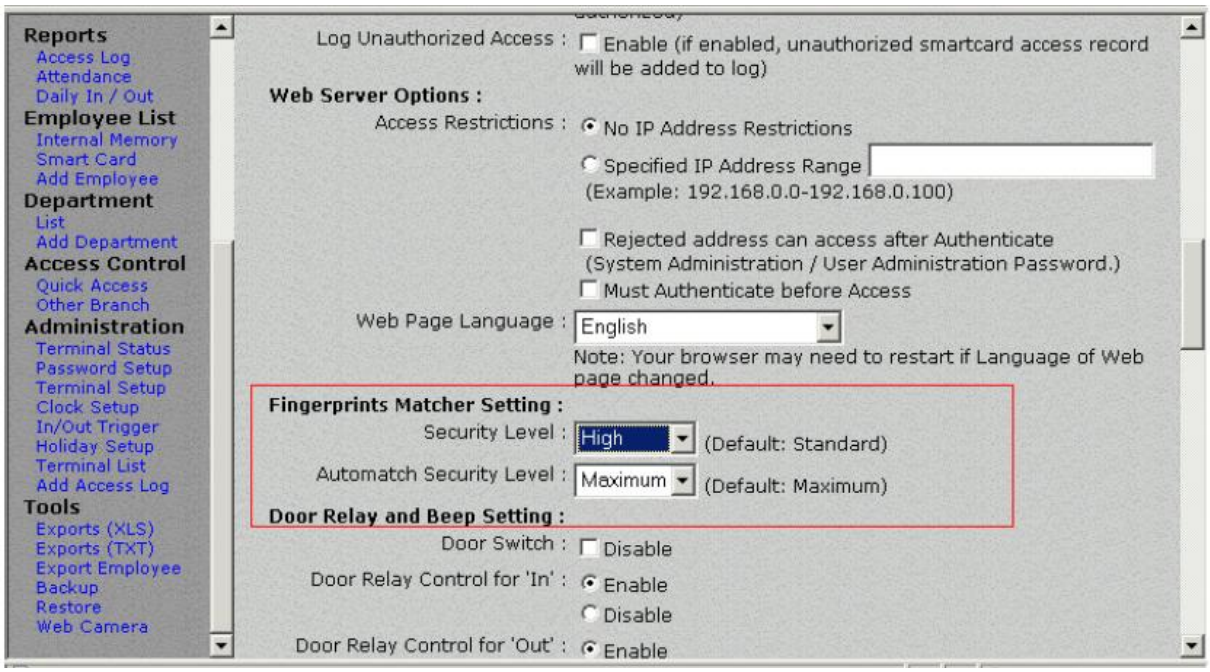

## 7.3. Wiegand 26 bitowy – wyjście.

Terminal posiada możliwość podłączenia urządzeń komunikujących się poprzez interfejs WIEGAND w formacie 26bit.



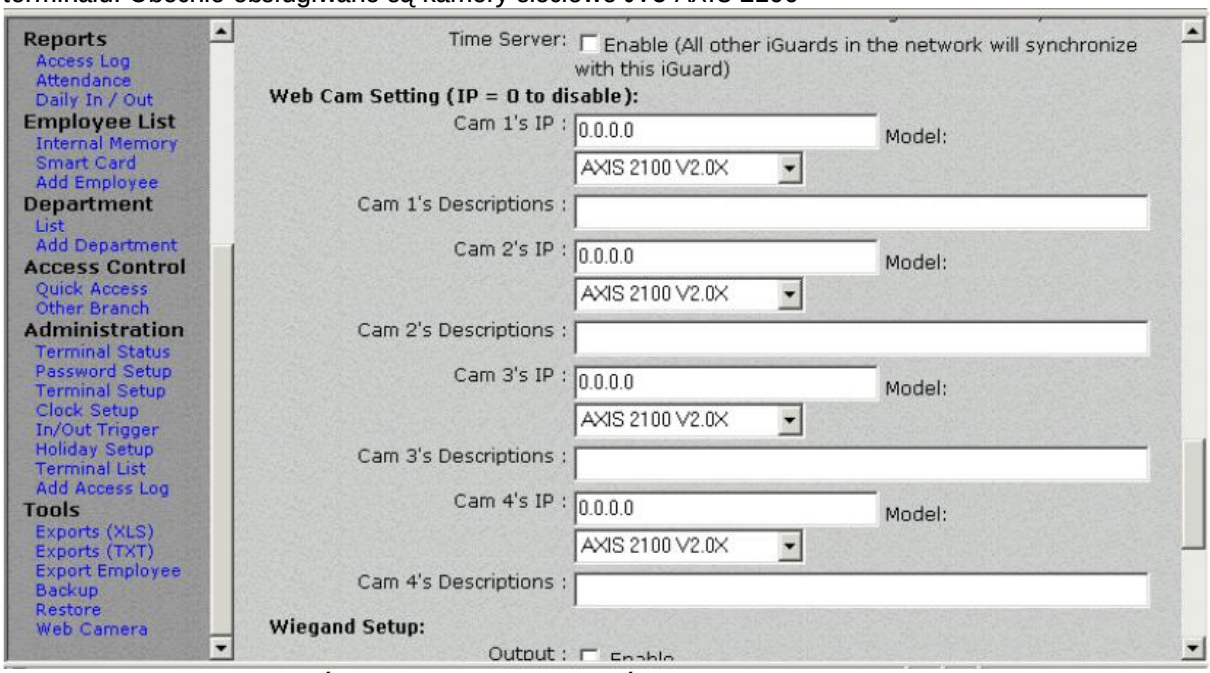

## 7.4. Bezpieczeństwo trybu Automatch.

Opcja ta pozwala administratorowi określić poziom bezpieczeństwa dla systemu. Przy zwykłych zastosowaniach powinno ustawiać się ten parametr na Low. W zastosowaniach gdzie wymagane jest wysokie bezpieczeństwo zaleca ustawić ten parametr na poziomie High. Ustawienie poziomu na wysoki może skutkować zwiększoną liczbą niepożądanych odrzuceń. Parametr ten ustawiasię w oknie terminal setup.



## 7.5. Konfiguracja kamery sieciowej.

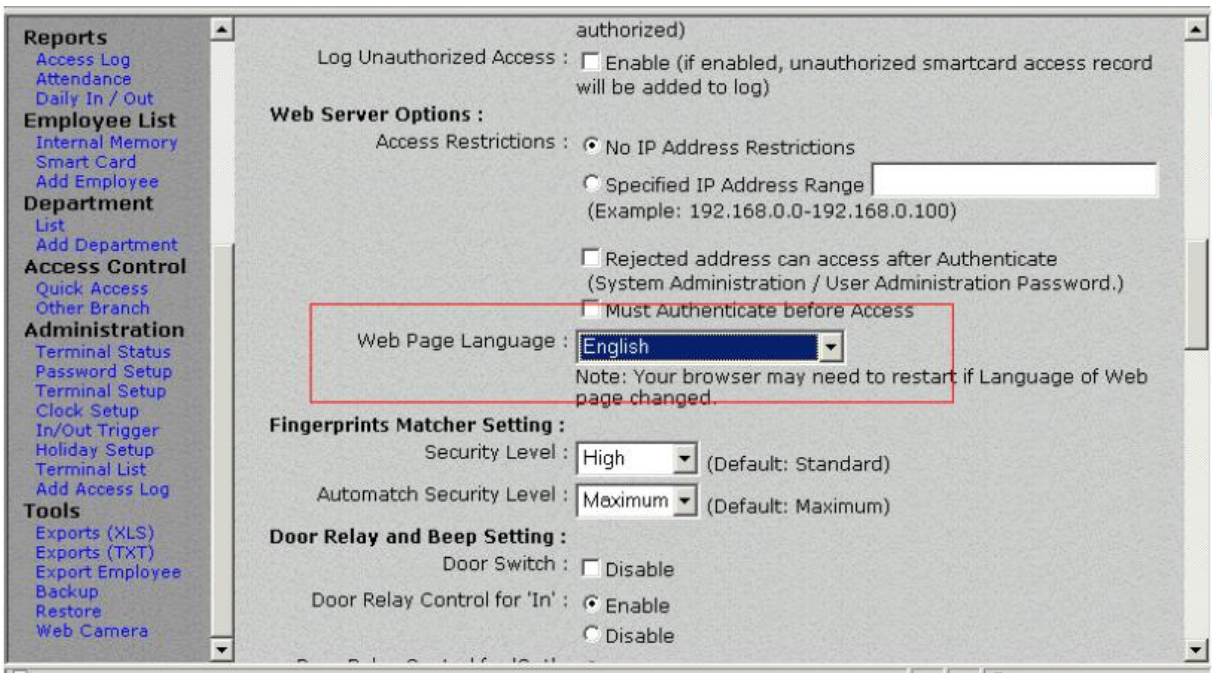
Urządzenia mogą być tak skonfigurowane, aby kierować sygnał z kamery IP w okno apletu w terminalu. Obecnie obsługiwane są kamery sieciowe JVC AXIS 2100




W konfiguracji należy podać adres IP kamery i wpisać jej numer modelu.

## 7.6. Język oprogramowania administracyjnego

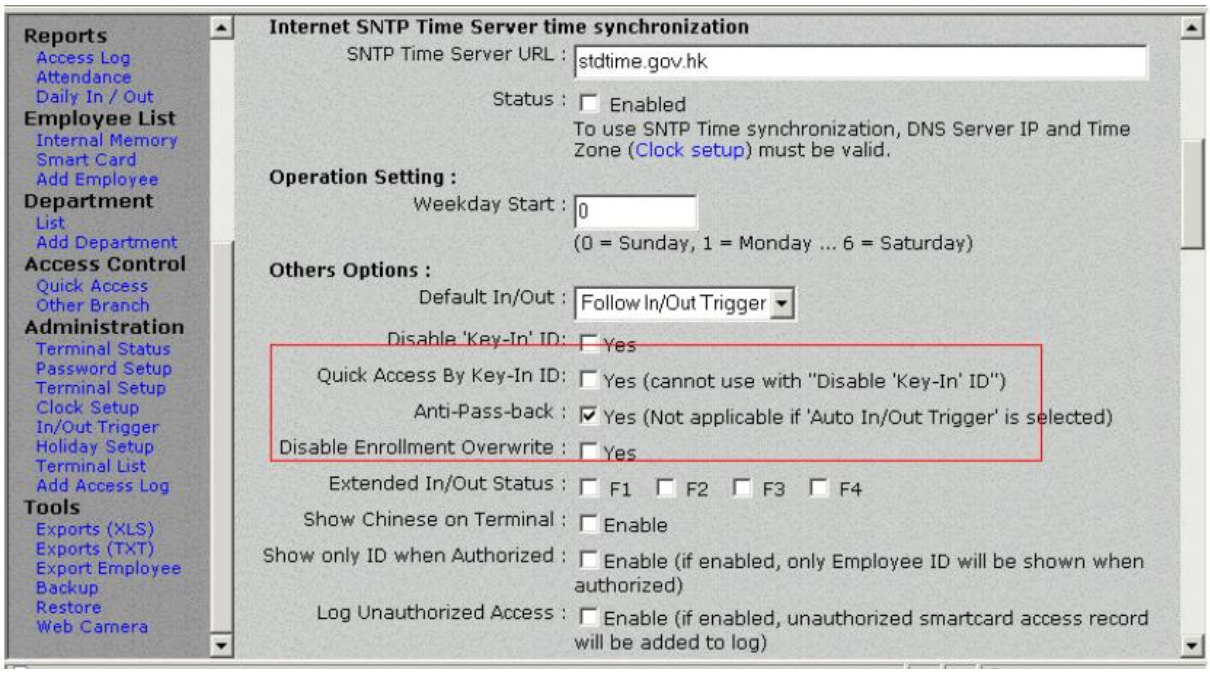
W systemie można wybrać domyślny język oprogramowania spośród kilku języków dostępnych w systemie. Dostępne są: Angielski, Hiszpański, Włoski, Prosty Chiński, Tradycyjny Chiński, Japoński. Istnieje możliwość dodania innych języków, w tym celu skontaktuj się z suportem.



## 7.7. Anti-Passback

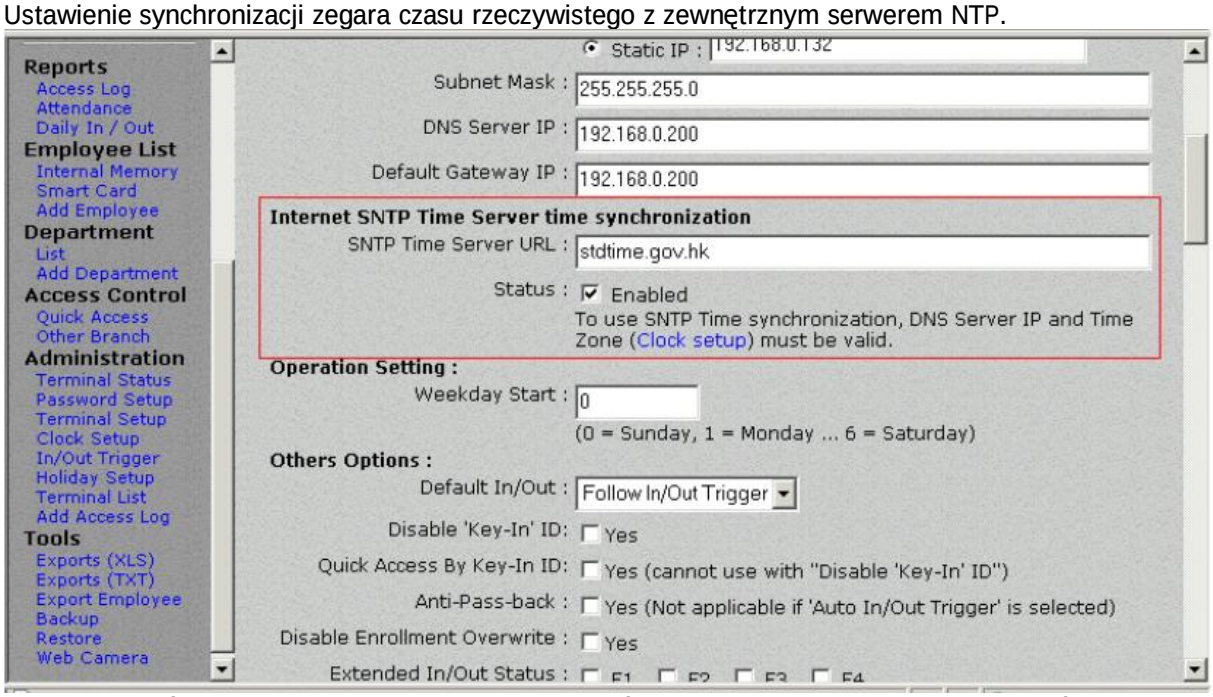
Ta funkcja nie jest dostępna w wersji standardowej urządzeń serii LM.

| | |
|---|---|
| Anti-Passback | Funkcja ta blokuje możliwość ponownego wejścia do pomieszczeń dla osoby, która wcześniej już zarejestrowała swoje wejście. Aby ponownie wejść osoba ta powinna wyjść. |



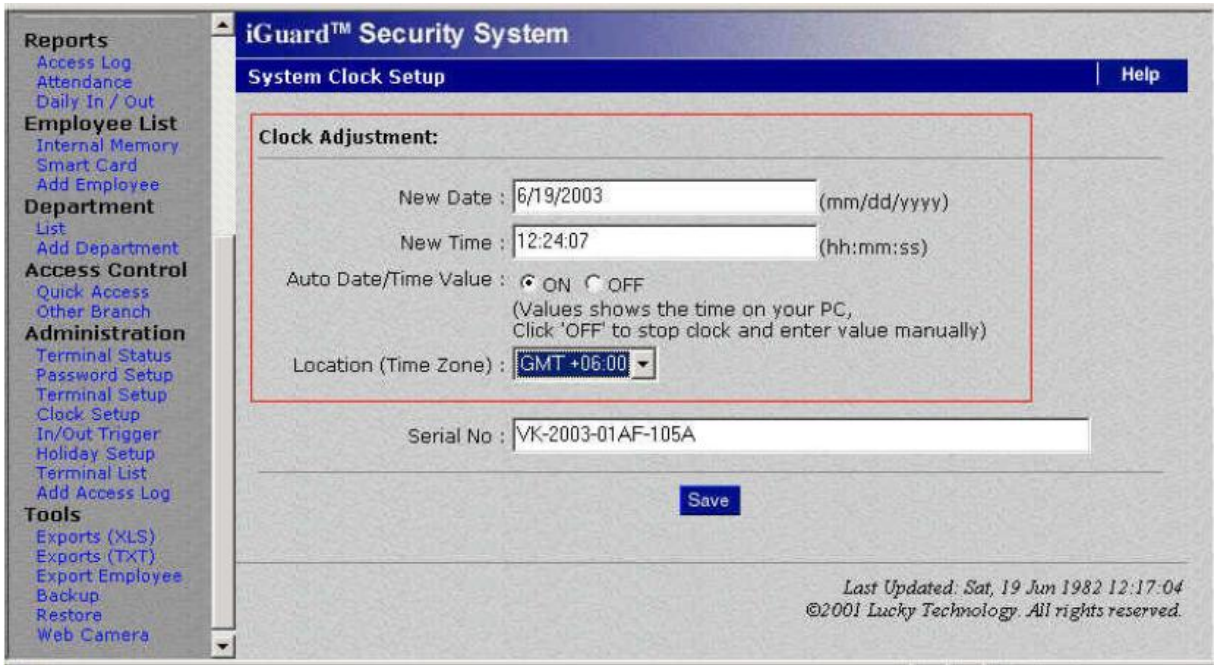

## 7.8. Serwer czasu NTP

Ustawienie synchronizacji zegara czasu rzeczywistego z zewnętrznym serwerem NTP.



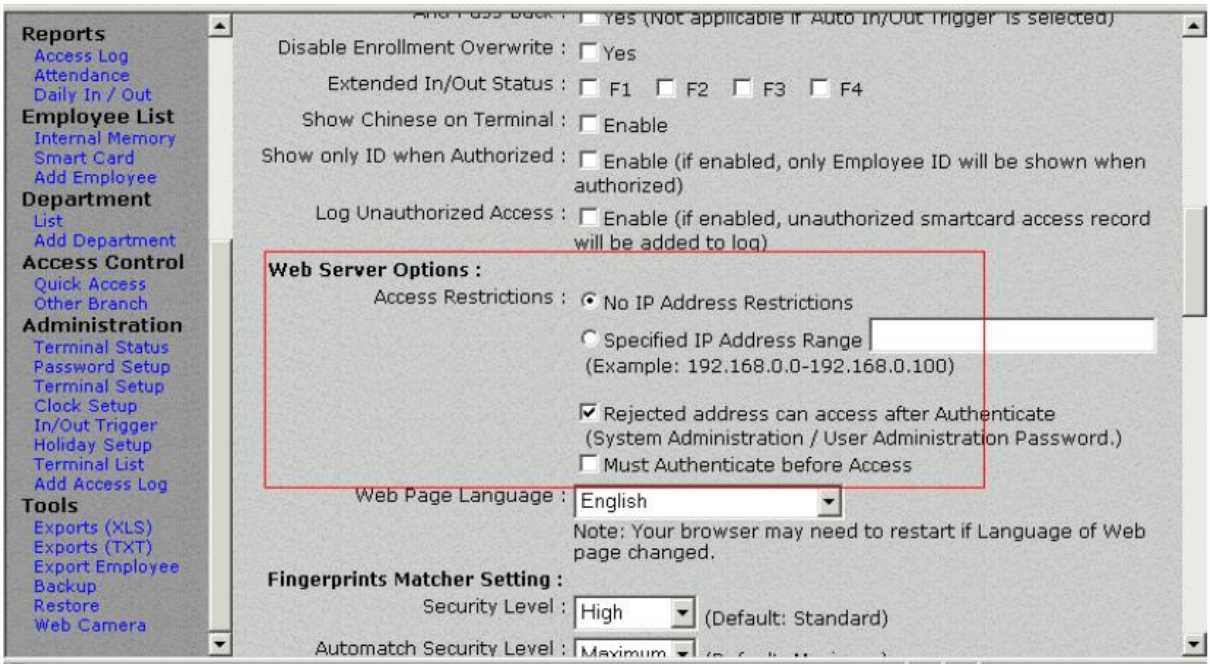

Aby uaktywnić tą funkcję należy najpierw zaznaczyć Status: enabled a następnie wpisać prawidłowy adres serwera. Dodatkowo w sekcji Clock Setup należy określić relację strefy czasowej w stosunku do czasu GMT +/-.

Status: Aby uaktywnić synchronizację SNTP upewnij się że adres serwera DNS i strefa czasowa ustawione są w sekcji Clock Setup.



## 7.9. Bezpieczeństwo stron administracyjnej

| | |
|---|---|
| No IP Address Restriction | Brak ograniczeń co do dostępu do urządzenia w sieci IP. |
| Access Restriction | Wpisz zakres adresów IP upoważnionych do dostępu do urządzenia. |
| Rejected address can Access after Authenticate | Działa podobnie jak poprzednia opcja jednak przed dostaniem się do urządzenia wymaga zalogowania się z hasłem administratora. Zezwala na z adresów spoza uprawnionej listy. Dostęp szczególnie przydatne przy zdalnym zarządzaniu. |
| Must Authenticate before Access | Wymaga podania hasła za każdym razem gdy się logujemy do systemu. |




## 7.10. Kasowanie danych z urządzenia

W uzasadnionych przypadkach istnieje możliwość wykasowania wszystkich danych i ustawień z urządzenia. Kasowane mogą być: baza danych użytkowników, baza logów przejść, wszystkie zarejestrowane wzorce biometryczne i prawa dostępu.

| **Opis** | **Wyświetlacz LCD** |
|---|---|
| W czasie gdy urządzenie jest w trybie oczekiwania wciśnij FUNC i wpisz hasło administratora. | Enter Password: _ |
| Wciśnij FUNC aby potwierdzić a następnie wybierz opcję 7 „System Shutdown/Reset | Press 7: System Shutdown/Reset |
| Teraz system poprosi Cię o podanie czy chcesz usunąć bazę danych użytkowników. Wybierz 1 aby to zrobić lub 2 aby ominąć | Reset User Dbase Yes/No (1/2)? _ |
| Teraz system poprosi Cię o podanie czy chcesz usunąć bazę zapisanych logów przejść. Wybierz 1 aby to zrobić lub 2 aby ominąć | Reset User Access Log Yes/No (1/2)? _ |
| Teraz system poprosi Cię o podanie czy chcesz przywrócić domyślne ustawienia urządzenia. Wybierz 1 aby to zrobić lub 2 aby ominąć. | Factory Default Yes/No (1/2)? _ |
| System wykonuje procedurę resetu a następnie powraca do trybu oczekiwania. | Mon Aug 30 13:46 ID #:_ |

## 7.11. Tryb testowy

W tym trybie dla celów przetestowania pracy urządzenia istnieje możliwość czasowego wyłączenia rejestracji logów. Służy do tego tryb testowy. Ma to zastosowanie szczególnie gdy po rejestracji nowych użytkowników chcesz zademonstrować sposób pracy urządzenia oraz przeprowadzić szkolenie z obsługi.

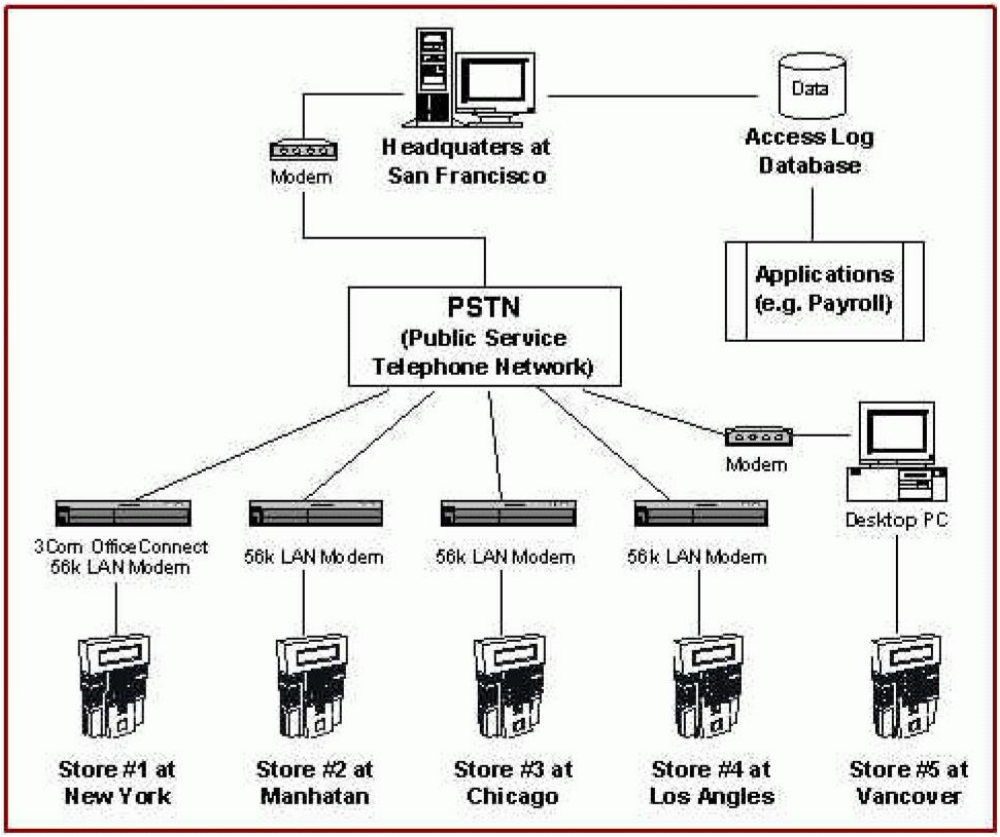
| **Opis** | **Wyświetlacz LCD** |
|---|---|
| W czasie gdy urządzenie jest w trybie oczekiwania wciśnij FUNC i wpisz hasło administratora. | Enter Password: _ |
| Ponownie wciśnij FUNC aby potwierdzić a następnie naciśnij klawisz „A". Na wyświetlaczu pojawi się napis „Test Mode". Tera możesz testować wzorce i szkolić pracowników. | == Test Mode! ==<br>ID #:_ |
| Według tej same powyższej procedury ponowne wciśnięcie klawisza „A" spowoduje opuszczenie trybu testowego. | Mon 30 Dec 13:49<br>ID #:_ |

**UWAGA:**
Pamiętaj o wyłączeniu trybu testowego aby zdarzenia rejestrowane przez urządzenie zostały zapisane w systemie logów.

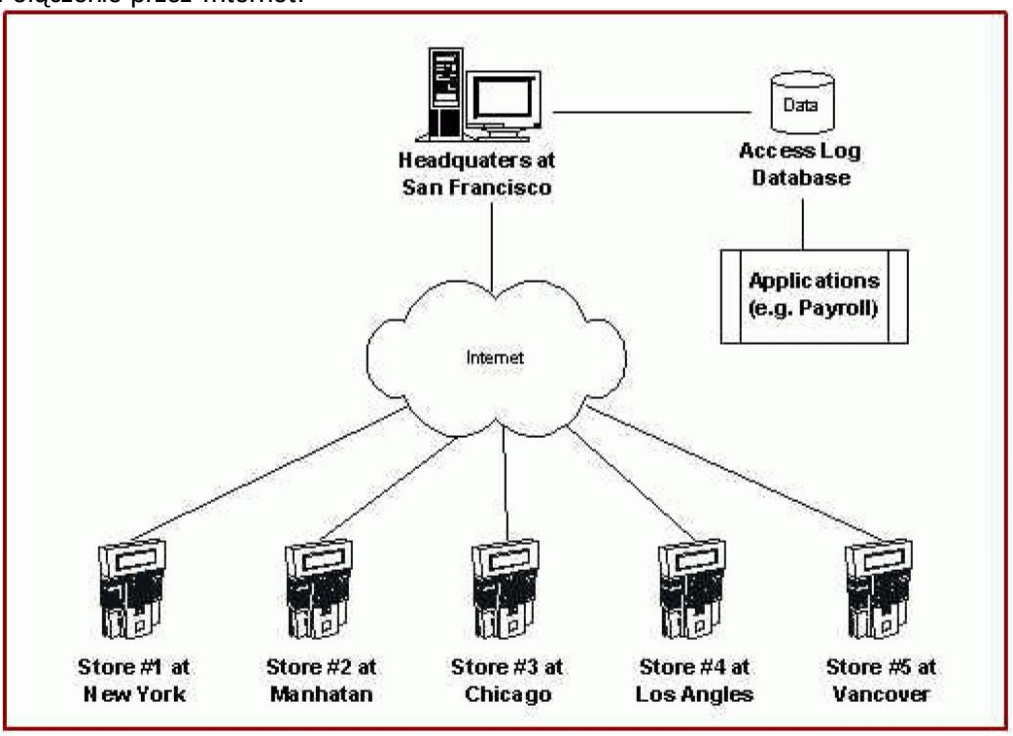
# 8. ZAŁĄCZNIKI

## Połączenia sieciowe

1. Połączenie przez sieć telefoniczną:

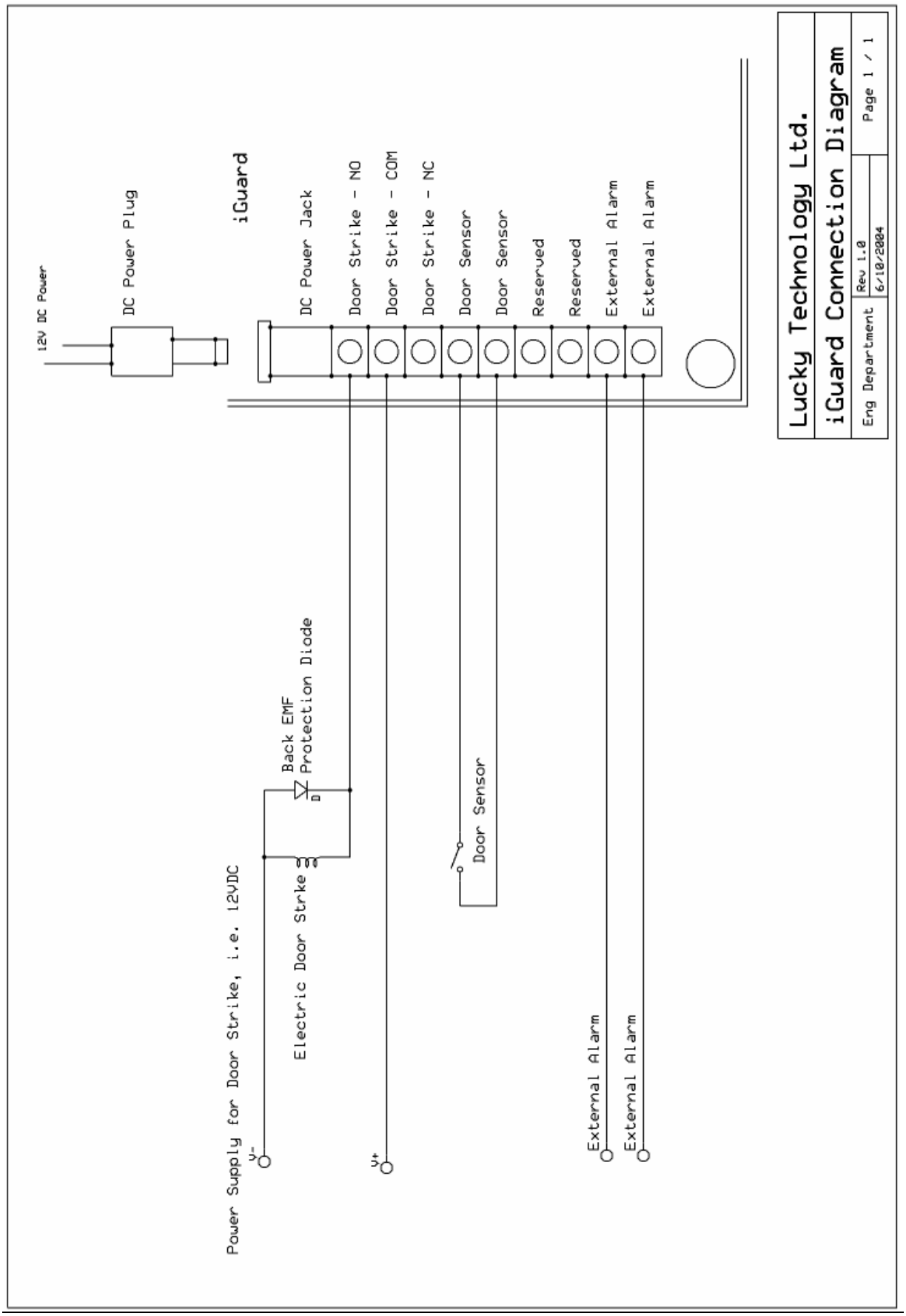



2. Połączenie przez Internet:

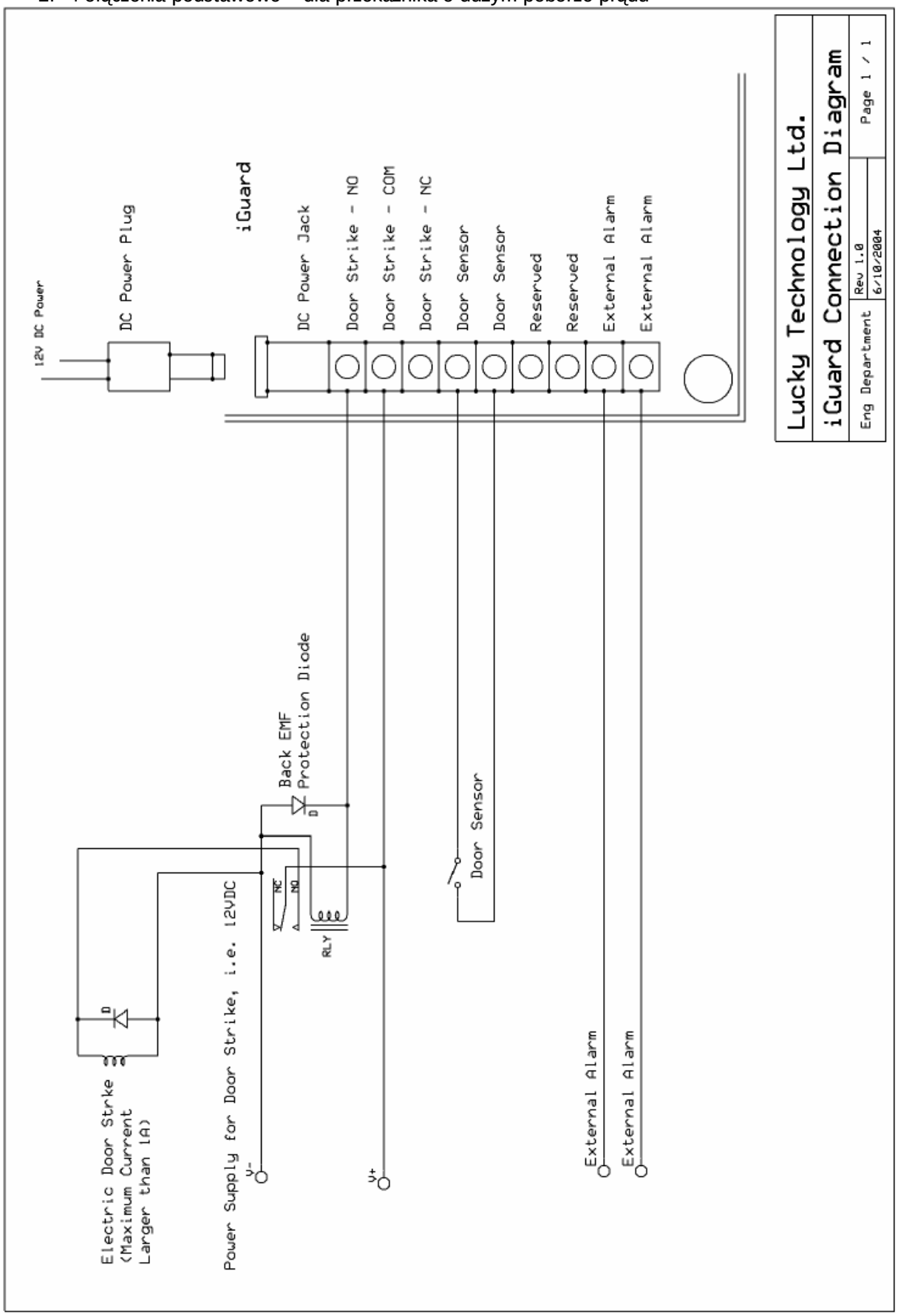


## Schemat połączeń

1. Połączenia podstawowe



2. Połączenia podstawowe – dla przekaźnika o dużym poborze prądu



3. Schemat podłączeń – zdalny przekaźnik