iGuard[™] Seria LM

Instrukcja obsługi

Wersja 3.6.xxxx



Copyright © 2002 Lucky Technology Limited

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

Translation Copyright © DEEP BLUE BIOMETRICS Sp. z o.o.

Trade Name : iGuard Model No: FPS110 / LM



Copyright © 2002 Lucky Technology Limited

1.	INST	ALACJA	5
	1.1.1.	Szybka instalacia	5
	1.1.2.	Wymagania instalacvine:	5
	1.1.3.	Instalacja	5
	1.1.4.	Wymagania dotyczące zasilania	6
	1.1.5.	Decyzja o miejscu instalacji	6
	1.1.6.	** Ważne ** Dotyczy metalowej ramy montażowej	6
	1.1.7.	Podłaczenie – Zasilanie i zewnetrzne urządzenia	6
~			_
2.	KONI	-IGURACJA	/
	2.1.	Ustawianie daty i czasu	7
	2.2.	Ustawienie parametrów sieci i adresu TCP/IP	8
	2.3.	Kod firmy	8
	2.4.	Ustawienie hasła administratora	8
3.	OPEF	ACJE PODSTAWOWE (BASIC OPERATIONS)	9
	3 1	REJESTRACIA	o
	3.1.	REJESTRACIA ODCISKÓW PALCA	>
	3.1.1.	Właczenie trybu Automatch	10
	3.1.2.	Rejestracia z wykorzystaniem Smart Card (dla modeli wyposażonych w czytniki Smart Card)	10
	3.1.3.	Rejestracja istniejacej karty	11
	315	Wervfikacja na podstawie odcisku palca	11
	316	Weryfikacja w trybie Automtach	11
	317	Weryfikacja za pomoca Smart Card	12
	318	Wervfikacja za pomocą basła	12
	319	Tymcząsowe wstrzymanie dostenu	12
	3.1.2.	POZOSTAŁ F. FUNKCIE	12
	321	Kasowanie ID	12
	322	Wyłaczanie urzadzenia	13
	3.2.3	Procedura hezpieczeństwa	13
			11
4.	ADIVI		14
	4.1.	Używanie przeglądarki internetowej	14
	4.2.	Lista pracowników	15
	4.3.	Employee List – Add Employee	15
	4.4.	Departament – List	16
	4.5.	Deparment – Add Departament	18
	4.6.	Access Control – Quick Access	19
	4.7.	Admnistration – Terminal Status	19
	4.8.	Administration – Password Setup	20
	<i>4.9</i> .	Administration – Terminal Setup	21
	4.10.	Administration – Lock Setup	22
	4.11.	Administration – In / Out Trigger	22
	4.12.	Administration – Holiday Setup	23
	4.13.	Administration – Terminal list	24
	4.14.	Administration – Add Access Log	24
	4.15.	Tools – Export Employee	25
	4.16.	Tools – Backup & Restore	26
	4.17.	Tools – Web Camera	27
5.	RAPC	DRTOWANIE	28
	5.1.	Tools – Export (XLS)	28
	5.2	Tools - Export (TXT)	29
	5.3	Reports – Access Log	30
	54	Reports Attendance	32
	5.5	iServer	32
	5.51	MS Access	33
	5.5.2	SQL Server	34
	5.5.3.	Cracle	35

	5.5.4.	Tworzenie Data Source Name (DSN)	35
6.	MAS	TER/SLAVE	37
	6.1. 6.2. 6.3.	Master vs. Slave Ustawienie ID Terminalu Super Master	37 38 39
7.	POZO	DSTAŁE ELEMENTY SYSTEMU	40
	7.1. 7.2. 7.3. 7.4. 7.5. 7.6. 7.7. 7.8. 7.9. 7.10.	Zdalny sterownik przejścia. Różne tryby pracy funkcji IN/OUT. Wiegand 26 bitowy – wyjście. Bezpieczeństwo trybu Automatch. Konfiguracja kamery sieciowej. Język oprogramowania administracyjnego. Anti-Passback. Serwer czasu NTP. Bezpieczeństwo stron administracyjnej. Kasowanie danych z urządzenia.	
	7.11.	Tryb testowy	48
8.	ZAŁĄ	CZNIKI	49

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:
 - o Terminal #1 Uziemienie
 - o 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 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 <u>http://192.168.0.100</u>

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 wy ś wietlaczu:	
Opis	Wy ś wietlacz 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	Wy ś wietlacz LCD
Gdy czytnik jest w trybie oczekiwania wciśnij FUNC i wprowadź hasło	Enter Password: _
administratora:	
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	Date (M/D/Y)
terminalu a następnie wciśnij FUNC.	08/30/2004
Wpisz prawidłową godzinę na terminalu a następnie zatwierdź wciskając	Time: (H;M:S)
FUNC	13:45:23
Teraz system poprosi o podanie ID terminalu. Parametr ten jest istotny	Terminal ID:
jeśli w sieci znajduje się więcej urządzeń.	

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.

Onis	Wy ś wietlacz I CD
Wciśnii klawisz FLINC, wpisz hasło administratora a nastepnie zatwierdź	Enter password
ponownie wciskając FUNC.	
Wciśnii 5" aby ustawić konfiguracie systemu	Press 1 [.]
	Add/Update ID
	·
	· Press 5· System
	Configuration:
Wciśnii FUNC aby przejść do konfiguracji DHCP/Static IP.	
Wciśnii FUNC aby kontynuować a nastepnie wybierz "1" aby ustawić	DHCP/Static IP
DHCP lub "2" aby ustawić statyczny adres IP.	(1/2) ? Static
Wciśnii FUNC aby kontynuować. Następnie system poprosi o podanie	IP Address:
nowego adresu IP. Wpisz ponownie cały adres nawet jeśli chcesz zmienić	192.168.001.123
tylko jedną cyfrę.	_
Wciśnij FUNC a następnie wpisz nową maskę sieci.	Subnetmask:
	<u>2</u> 55.255.255.000
Wciśnij FUNC i wpisz nową bramę sieci.	DefaultGateway:
	<u>1</u> 92.168.000.200
Wciśnij FUNC aby podać nowy adres serwera DNS.	DNS:
	<u>1</u> 92.168.000.200
Wciśnij FUNC aby określić czy urządzenie jest Master czy Slave. Jeśli	Master/Slave
urządzenie pracuje samodzielnie zawsze ustaw je jako master. W	(1/2) ? Master
przeciwnym razie system poprosi o podanie urządzenia Master.	
Wciśnij FUNC aby zakończyć konfigurację sieci.	Mon Aug 30 13:46
	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	Wy ś wietlacz LCD
Gdy urządzenie jest w trybie oczekiwania wciśnij FUNC, podaj hasło	System Admin:
administratora i zatwierdź ponownie wciskając FUNC. Wybierz "6" aby	123_
przejść do ustawiania hasła administratora. Gdy system zapyta się	
Admin/Personal (1/2) wybierz "1".	
Wciśnij 🗆 aby wykasować stare hasło i wpisać nowe (np. AB456).	System Admin:
Długość hasła ograniczona jest do 10 znaków w przedziale 0-9 oraz A i B.	AB456
Wciśnij FUNC aby zaakceptować nowe hasło dla System Administrator.	User Admin: _
Teraz system poprosi o podanie nowego hasła dla User Administratora.	
Wpisz nowe hasło (np. 7890AB) a następnie zatwierdź FUNC.	User Admin:
	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:
	9394AB709_
Po zatwierdzeniu FUNC terminal przełączy się w stan oczekiwania	Mon Aug 30 13:49
	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	Wy ś wietlacz LCD
Wpis "1" aby uruchomić proces rejestracji	By Fingerprint/Passwd
	(1/2)?
Wybierz 1 a następnie	Enter ID # and
	Scan 1st Finger
podaj ID użytkownika i wciśnij klawisz FUNC	Enter ID# A01_
Naciśnij klawisz FUNC po każdym zarejestrowaniu wzorca. Proces	Scanning 1 of 3
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.	
Gdy linia demonstrująca proces rejestracji przesunie się	Analyzing. Pls remove finger
całkowicie do prawej strony zostaniesz poproszony o zdjęcie	
palca z czytnika	

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

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

Teraz urządzenie przejdzie w tryb oczekiwania na podanie	Enter ID #: _
kolejnego ID.	
Wciśnij klawisz B lub poczekaj aż upłynie limit czasu oczekiwania	Mon Aug 30 12:00
aby powrócić do normalnego trybu oczekiwania.	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	Wy ś wietlacz LCD
Gdy terminal jest w trybie oczekiwania wciśnij FUNC, wpisz hasło administratora a następnie zatwierdź FUNC. Teraz wybierz "9"	Enter ID #: _
aby przejść do Issue/import Card. Wciśnij "2" aby importować	
kartę.	
Teraz system poprosi o zbliżenie karty	Wait for
	Smart Card
Zbliż kartę do klawiatury iGuard. Teraz system zapisze informację	Writing
zapisaną w karcie.	

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

3.1.6. Weryfikacja w trybie Automtach

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

Opis	Wy ś wietlacz LCD						
Gdy urządzenie jest w trybie oczekiwania podnieś osłonę i połóż Mon Aug 30 13:49							
palec na sensor. Urządzenie automatycznie rozpocznie odczyt == Automatach !==							
wzorca.							
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	Wy ś wietlacz LCD
Gdy urządzenie jest w trybie oczekiwania zbliż kartę blisko	Jacky Hui
klawiatury. Terminal odczyta kartę i jeśli jest ona zarejestrowana	Waiting Finger
w systemie poprosi o przyłożenie palca	
Jeśli wzorzec zapisany na karcie odpowiada wzorcowi palca na	Jacky Hui
czytniku użytkownik uzyskuje dostęp	Authorized

3.1.8. Weryfikacja za pomocą hasła

Opis	Wy ś wietlacz LCD		
Gdy terminal jest w trybie oczekiwania wpisz na klawiaturze ID	Mon Aug 30 13:49		
użytkownika (np. A01)	A01_ IN		
Zamiast podnosić pokrywę czytnika wystuka ja klawiaturze hasło i	Your password:		
naciśnij FUNC			
Wpisz hasło	Your password: *****		
Wciśnij FUNC ponownie aby potwierdzić. Jeśli hasło jest	A01		
prawidłowe dostęp zostanie przyznany.	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	Wy ś wietlacz LCD
Gdy urządzenie jest w trybie oczekiwania wciśnij FUNC.	Enter ID #: _
Wprowadź hasło administratora i potwierdź za pomocą FUNC.	
Naciśnij "2" i wybierz "Inactivate ID".	
Wpisz ID # użytkownika które chcesz zablokować	Enter ID: A01
Wciśnij FUNC aby zatwierdzić. Teraz użytkownik z ID # A01	ID A01:
został zablokowany.	Inactivated !

3.2. POZOSTAŁE FUNKCJE

3.2.1. Kasowanie ID

Czynność ta polega na permanentnym usunięciu użytkownika z systemu.

Opis	Wy ś wietlacz LCD		
Gdy urządzenie jest w trybie oczekiwania wciśnij FUNC.	ID to Delete:		
Wprowadź hasło administratora i potwierdź za pomocą FUNC.			
Naciśnij "4" i wybierz "Delete ID".			
Wpisz ID # użytkownika które chcesz usunąć	ID to Delete:		
	A01		
Wciśnij FUNC aby zatwierdzić. Teraz użytkownik z ID # A01	ID #A01		
został usunięty.	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:

🚰 iGuard Fingerprint Security 🤉	System - Microsoft Internet Expl	orer	
<u>File Edit View Favorites</u>	<u>T</u> ools <u>H</u> elp		
🗍 ⇔Back • → • 🙆 🛃 🚮	🕴 🕅 Search 🛛 👔 Favorites	» Address 🙋 http://192.168.0.250/Admins/index.html	
iG1	uard [™] Security System	n	
iGuard Security System			Help
Terminal: iGuard			
Casuel Facalaura	iGi	uard Security Access Control System	
Search Employee	Terminal Information		
Bu ID	Terminal ID	iGuard (MASTER)	
O By Last Name	Descriptions	iGuard FingerPrints Security Terminal	
Go	Firmware Version	3.1.0702A	
	Model	100 -Employees Version (Fingerprints)	
Reports	Registered Employee	46	
Access Log Attendance	Mode	Time Attendance	
Employee List	IP Address	192.168.0.250	
Add Employee	Your IP Address	192.168.0.17	
Department	Start Time	Wed, 27 Jun 2001 06:59:54	
List Add Department	Up Time	000 days 04 hours 35 mins 04 secs	
Access Control	Hit Count	200	
Quick Access	Serial No.	VK-9940-019C-1009	
Administration			
Terminal Status Password Setup Terminal Setup Clock Setup Tn/Out Trigner		Last Updated: Wed, 27 Jr ©2000 Lucky Technology. A	m 2001 11:34:58 Il rights reserved.
Done Done		📄 🖉 Int	ernet //,

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

<u>File E</u> dit <u>V</u> iew F <u>a</u> v	orites <u>T</u> oo	ls <u>H</u> elp							1
🕁 Back 🔹 🔿 👻 🎑) (<u>)</u>	Search 💽 Favo	orites >	> 🛛 Address 🕖 http)://192.168.0	.250/Admins/inde	ex.html		▼ 🖗 G
	iGuar	d [™] Securitv	System		2				
iGuard™ Security System	Employ	ee List			First	Previous	Next	La	st Help
Terminal: iGuard	Allerton			Rect Provenie				il de	
Carauch Caralanaa		First Nan	ne Last Nan	ne Status	I	Department		-	
Search Employee		The state of the s	Security Contraction	All	<u> </u>	All Departmen	ts 🗾	Go	
• By ID	No	Employee ID	Last Name	First Name		Active FP	PSW	A/M	IN/OUT
🗢 By Last Name		A1002	Wona	Kit China	苦潔貞	10 0	0	0	IN 09:06
Go	Γ2.	A1007	Tsui	Ping Fuk	徐平福		0	0	IN 09:19
Penorts	Гз.	A1010	Liu	May Wan	廖美雲			0	IN 08:53
Access Log	□ 4.	A1015	Chu	Chuk Ching	朱祝淸		0	0	IN 08:39
Attendance	□ 5.	A1019	Chan	Chuen Heung	陳泉香	• •	0	0	IN 09:32
List	6.	A1041	Chan	Kin Wai	陳建威		0	0	IN 09:10
Add Employee	□ 7.	A1045	Мо	Hang Hing	巫恒興		0	0	
list	Г 8.	A1050	Chan	кс	陳國柱		0		IN 09:00
Add Department	Γ9.	A1073	Ng Luk	Mui Mui	吳陸妹妹		0	0	IN 08:43
ccess Control	□ 10.	A1154	Chow	Man Keung	周交強		* O	0	IN 09:15
Other Branch	Γ 11.	A1155	Shek	Ying Kuen	石英櫂		0	0	IN 09:56
dministration	□ 12	A1162	Chan	Tai Wan	陳帶穩		0	0	OUT 08:03
the second se	the second se			THE REPORT OF	The second s	The second s	AND DECKSTONES	Contraction of the local division of the loc	A STATE OF A STATE OF A STATE OF A STATE

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.

🚈 iGuard Fingerprint Secu	urity System - Microsoft Intern	et Explorer					<u> </u>	
Eile Edit Yiew Favor	rites <u>T</u> oals <u>H</u> elp						1	
] 🗇 Back 🔹 🔿 😴 [🖞 🛱 🥘 Search 📓 Favorites	③History 🔄 - 🗃 💽 - 📃 "	Address 🚺 http	p://203.80.236	.61/Admin	s/inde×.html	▼ (r ² 60	
A	iGuard [™] Security Sy	rstem					- -	
iGuard ""	Employee Record		First	Previous	Next	Last Acc.	Log Help	
Terminal: Main	Employee Reco	rd (Internal Memory)	1					
	Employee Data					Department		
• By ID	Employee ID :	BBD1	(10 Char. Max)			All Departm	ients	
Go By Last Name	Last Name :	Leung	(20 Char. Max)					
	First Name :	Brian	(20 Char, Max)			I ICOM		
Access Log	Other Name / Title :	梁瑞基	(20 Char. Max)				1	
Employee List		Save New Password (See Re	marks 1.)					
Internal Memory Smart Card	New Password :	(8 Char. Max) (Existing password is not shown	for security rea	ison.)				
Add Employee Department	Status :	I▼ Active						
List Add Department	V Auto Match							
Access Control Quick Access		Savo	Delete					
Other Branch Administration		Save or Del	ete this record					
Terminal Status	REMARKS: 1. Chec UnCh	REMARKS: 1. Check to save New password. UnCheck to use Existing password (not shown).						
Terminal Setup Clock Setup	2. You t	an only activiate / deactivate emp	oloyee from oth	er branch.				
In/Out Trigger Holiday Setup							2002 00 05 10 -	
Add Access Log 🚽				©12	000 Luck	y Technology All	nghts reserved 🚽	
Done						🕘 Inte	rnet //	

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.

iGuard Fingerprint Second iGuard Fingerprint Second	urity Sys	tem - Microsoft Internet Exp	lorer					
Eile Edit View Favo	rites <u>T</u> o	ools <u>H</u> elp						1
] ⇔ Back → → - 🙆 🧕	1 4	🐼 Search 🛛 👋 🛛 Address 🚺	http://192.168.0).132/Adn	nins/index.html			• @Go
·	iGua	rd™ Security Syste	m					<u> </u>
IGUARD Security System	Depar	tment List	I,	First	Previous	Next	Last	Help
Terminal: iGuard		Depar	tment ID:		Go			
By ID By Last Name Go	No.	Department ID	Desci	riptions				
		1. ACCOUNTING 2. EVERYONE	Accou Syste	nting D m Defa	epartment ult Departmer	nt		
		3. MARKETING 4. PRODUCTION	Marke	eting De action D	epartment			
Access Log Attendance	End o	f List	11000				Total 5 R	ecord(s)
Employee List Internal Memory Smart Card Add Employee	Delet	Delete Selected Departn	nent					
Add Department Access Control				(Last Update D2000 Lucky Te	d: Sun, schnoloj	10 Jun 200 gy. All right	1 22:25:35 5 reserved.
Done					J.) Internet	1.

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.

iGuard Fingerprint Sec File Edit <u>V</u> iew F <u>a</u> v	curity System - Microsoft Into orites <u>T</u> ools <u>H</u> elp	ernet Explorer				
🗢 Back 🔹 🔿 🔹 🙆	🗿 🚰 😡 Search 🛛 🙀 Favor	ites 🤎 🛛 Address 🚺 http://203.80.2	36.61/Admins/index.ht	nl	• 🖓 Go	
-	iGuard [™] Security	System				
iGuard Security System	Department Record	First	Previous Next	Last Acc. Log	Help	
Terminal: Main						
Search Employee	Department R	ecord				
	Donartmont Data					
• By ID	Department ID -		/11	Char Maul		
🔘 By Last Name	Department ID .		(10	- (16 Char, Max)		
Go	Description :	Marketing Department	(30) Char. Max)		
Reports Access Log Attendance Employee List Internal Memory Smart Card Add Employee Department List Add Department Access Control Quick Access Other Branch Administration	Time Restrictions : ((00 0 Sunday Tuesday Wenesday Thursday Friday Saturday Remarks Terminals	Jick Monday - Sunday to edit the 1 02 03 04 05 06 07 08 09 10	a time restriction.) 111 12 13 14 15 	16 17 18 19 20 21 2 Y YY W YY YY YY YY AMAGAMAGANA	2 23	
Terminal Status	C All Terminals					
Terminal Setup	🔽 Main)ffice			
In/Out Trigger Holiday Setup Terminal List	1	Save Dee Save or Delete th	is record			
Done				🔹 🚺 🔮 Internet		

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.

01 (YY) YY) YY) YY) YY) YY)	ault De 02 0: YY Y YY Y YY Y YY Y YY Y	partm 3 04 7 YY 7 YY 7 YY 7 YY 7 YY	05 YY YY YY YY YY	06 YY YY YY YY	07 YY YY YY	08 YY YY YY YY	09 YY YY YY	10 YY YY YY	11 YY YY YY	12 YY YY YY	13 YY YY	14 YY YY	15 YY YY	16 YY YY	17 YY YY	18 YY YY	19 YY YY	20 YY YY	21 YY YY	22 YY YY	23 YY YY
01 (YY) YY) YY) YY) YY)		3 04 7 YY 7 YY 7 YY 7 YY 7 YY	05 YY YY YY YY	06 \\ \\ \\ \\ \\ \\	07 YY YY YY	08 YY YY YY YY	09 YY YY YY	10 YY YY YY	11 YY YY YY	12 YY YY	13 YY YY	14 YY YY	15 YY YY	16 YY YY	17 YY YY	18 YY YY	19 YY YY	20 YY YY	21 YY YY	22 YY YY	23 YY YY
	YY YY YY YY YY YY YY YY YY YY	 YY YY YY YY YY YY YY YY 		* * * * *	YY YY YY YY	YY YY YY YY	YY YY YY ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	YY YY YY	YY YY YY	YY YY YY	YY YY	YY YY	YY YY	YY YY	YY YY	YY YY	YY YY	YY YY	YY YY	YY YY	
	YY YY YY YY YY YY YY YY	 YY YY YY YY YY YY YY 	YY YY YY YY	YY YY YY	YY YY YY	YY YY YY	YY YY ~~	YY YY	YY YY	YY YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
YY Y YY Y YY Y	YY Y YY Y YY Y YY Y	YYYYYYYYYY	YY YY YY	YY YY YY	YY YY	YY YY	W w	YY	YY	YY											
YY 1 YY 1 YY 1	177 Y 177 Y 177 Y	YYYYYY	YY YY	YY W	YY	YY	w			S. S. S. S. S.	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
YY 1 YY 1	YY Y YY Y	<pre>Y YY</pre>	YY	W				YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
YY N	YY Y			100 C 100 C 100	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
101 1		YY YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
YY Y	YY Y	YY YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
	<u></u>						-	<u></u> 0		<u></u> 2	2 <u>-</u> 2				<u></u> -	<u></u>	<u></u>		2 <u>-</u> -	<u> </u>	
	-		~																		
		ACCESS	06	User	r Det	ine no	10	- - -	- 	2 1	3 1	4	15	16	17	18	10	20	21	22	23
	V V	- 	- -	- -	- -	- -	-10 			- -	v	v			<u>v</u>	10	V.	120			
	<u>v</u> v	7	V	V	V	7	1		· .	7 1	7 1	7	7		V	7	V	V	V	V	V
		All C No A 22 03 04 V V V V V V	All C No Access 22 03 04 05 7 7 7 7 7 7 7 7 7 7	All C No Access © 12 03 04 05 06 17 17 17 17 17 17 17 17 17 17 18 10 10 10 10 10 10 10 10 10 10 10 10 10	All C No Access C User 22 03 04 05 06 07 V V V V V V V V V V V V All Days C Sup V h	All C No Access C User Def 22 03 04 05 06 07 08 27 17 17 17 17 17 17 17 28 17 17 17 17 17 17 29 17 17 17 17 17 17 20 17 17 17 17 17 17	All C No Access C User Define 12 03 04 05 06 07 08 09 V V V V V V V V V V V V V V V All Days S Sup V Mon Tu	All C No Access C User Define 22 03 04 05 06 07 08 09 10 V V V V V V V V V V V V V V V Apply Set All Days Sun V Mon Tue	All C No Access C User Define 22 03 04 05 06 07 08 09 10 1: V V V V V V V V V V V V V V V V Apply Setting All Days Sup V Mon Tue Wei	All C No Access C User Define 12 03 04 05 06 07 08 09 10 11 1 17 18 19 19 19 19 19 19 19 19 19 19 19 19 19	All C No Access C User Define 12 03 04 05 06 07 08 09 10 11 12 1 V V V V V V V V V 1 V V V V V V V V 1 Apply Setting to : All Days Sup V Mon The Wed Thu	All C No Access C User Define 12 03 04 05 06 07 08 09 10 11 12 13 1 V V V V V V V V V V V V V V V V V V V	All C No Access C User Define 12 03 04 05 06 07 08 09 10 11 12 13 14 1 V V V V V V V V V V V V V V V V V V V	All C No Access C User Define 12 03 04 05 06 07 08 09 10 11 12 13 14 15 V V V V V V V V V V V V V V V V V V V	All C No Access C User Define 12 03 04 05 06 07 08 09 10 11 12 13 14 15 16 V V V V V V V V V V V V V V V V V V V	All C No Access C User Define 22 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 V	All C No Access C User Define 22 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 V V V V V V V V V V V V V V V V V V V	All C No Access C User Define 22 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 V	All C No Access C User Define 22 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 V V V V V V V V V V V V V V V V V V V	All © No Access © User Define 12 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 17 17 17 17 17 17 17 17 17 17 17 17 17 1	All C No Access C User Define 22 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 V V V V V V V V V V V V V V V V V V V

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.

iGuard Fingerprint Security 5	ystem - Microsoft Internet Expl	orer	_ 🗆 🗵
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	Tools Help		
] ⇔Back • → • 🙆 🗗 🖓	🔇 Search 🙀 Favorites	>> Address 🙋 http://192.168.0.250/Admins/index.html	▼ 🖓 Go
📕 📥 iGu	ard [™] Security Syster	n	
iGuard™ security System			Help
Terminal: iGuard	iG	uard Security Access Control System	
Search Employee			
	Terminal Information :		
By ID	Terminal ID	iGuard (MASTER)	
🔘 By Last Name	Descriptions	iGuard FingerPrints Security Terminal	
Go	Firmware Version	3.1.0702A	
	Model	100 -Employees Version (Fingerprints)	
Reports	Registered Employee	46	
Attendance:	Mode	Time Attendance	
Employee List	IP Address	192.168.0.250	
Add Employee	Your IP Address	192.168.0.17	
Department	Start Time	Wed, 27 Jun 2001 06:59:54	
List Add Department	Up Time	000 days 04 hours 35 mins 04 secs	
Access Control	Hit Count	200	
Quick Access Other Branch	Serial No.	VK-9940-019C-1009	
Administration			
Terminal Status Password Setup Terminal Setup Clock Setup In/Out Tringer		Last Updated: Wed, 27 J ©2000 Lucky Technology. A	un 2001 11:34:58 II rights reserved.
🖉 Done		In	ternet //

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.

🚈 iGuard Fingerprint Sec	curity System - Microsoft Internet Explorer	
j <u>F</u> ile <u>E</u> dit ⊻iew F <u>a</u> vo	orites Iools Help	1
] 🗧 Back 👻 🌩 👻 🧕	2 🚰 🔯 Search 😹 Favorites 🎽 Address 🚺 http://203.80.236.61/Admins/index.html 💽	∂G0
-	iGuard [™] Security System	-
iGuard Security System	System Configuration He	lp
Terminal: Main	System Passwords Setting:	
Search Employee	System Administration User Name : admin	
 By ID By Last Name 	System Administration Password :	
Go	User Administration User Name :	
Access Log Attendance	User Administration Password : 🚧	
Employee List Internal Memory Smart Card	Door Access Password : 🔤	
Add Employee Department List	Serial No : VK-9940-0132-F121	
Add Department Access Control Quick Access Other Branch	Save	
Administration Terminal Status	Remarks: 1. For security reason, System Administartion User Name and Pass word cannot leave blank.	
Password Setup Terminal Setup Clock Setup In/Out Trigger Holiday Setup	Account. 3.Leave blank in Door Access Password will disable Door Access Password.	
Terminal List Add Access Log Tools	Last Updated: Mon, 2 Jul 2001 18:4 ©2000 Lucky Technology. All rights rese	17:18 rved. 🚽
Done	👘 🚺 👘 Internet	1.

4.9. Administration – Terminal Setup

Wybierz Terminal Setup:

🚰 iGuard Fingerprint Sec	urity System - Microsoft Internet Explorer	
j <u>F</u> ile <u>E</u> dit <u>V</u> iew F <u>a</u> vo	rites <u>T</u> ools <u>H</u> elp	1
] 💠 Back 🔹 🤿 👻 🙆	🖞 🚰 😡 Search 💿 Favorites 🔷 🛛 Address 🚺 http://203.80.236.61/Admins/index.html	▼ ∂°60
<u> </u>	iGuard™ Security System	
iGuard™	Terminal Configuration	Help
Terminal: Main		Statistics and the
	Terminal Setting:	
Search Employee	Network Setting :	and a start of the
• By ID	Terminal ID : Main	Construction of the
O By Last Name	Domain Name : inuardsystem.com	-
Go	Description LiGuard Security System	
Reports	Master / Slave Unit : China and Security System	
Access Log	G Clause Unit /Master Unit ID 192168.0.200	
Employee List	IP Address : C use puce	
Internal Memory Smart Card	G Statio ID - 192 168 0 252	
Add Employee Department	Cubact Mack / 200 200 200	-
List Add Department	Subhet Mask : [255.255.0	
Access Control	DNS Server IP : [192.168.0.200	
Quick Access Other Branch	WINS Server IP : 192.168.0.200	
Administration Terminal Status	Default Gateway IP : 192.168.0.254	
Password Setup	Operation Setting :	
Clock Setup	Operation Mode : • Access Control	
Holiday Setup	Time Attendance Management	
Add Access Log	Default In/Out : Follow In/Out Trigger	
Tools	About Abierre an	
🛃 Done	Ini	ernet //

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.

iGuard Fingerprint Security S	ystem - Microsoft Internet Explorer			_ 🗆 ×
<u>File Edit View Favorites</u>	<u>T</u> ools <u>H</u> elp			19
] ← Back • → • 🕥 🗗 🖓	Search » Address () http://203.80.2	236.61/Admins/index.ht	ml	• 🗟 😡
iG ı™ <mark>≜</mark> iGu	ard™ Security System			_
Security System	Dut Time Trigger			Help
Terminal: Main Search Employee	Out Time Trigger:			
	Trigger at (HH:MM):	C Out Add		
• By ID	Time	In	Out	
By Last Name	08:00	1 () () () () () () () () () (Q	
Go	12:30	0		
	13:30		Contra la	
Reports	16:00	0		
Access Log	Click time to r	emove / edit.		
Attendance				
Employee List				
Internal Memory		Tool The Lat	A. Mar. 2 5.4.20	07 22.57.40
Add Employee		©2000 Lucky To	almology All rig	101 22.31.48
Department 🗾		ez ooo Lacky Te	chilology. All rig	Tus reserved.
Done			🚺 谢 Internet	

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	Wy ś wietlacz LCD
Domyślnie IN (standardowe przy rejestracji czasu pracy na	Monady 30 13:49
wejście)	ID#_ IN
Domyślnie OUT (standardowe przy rejestracji czasu pracy na	Monady 30 13:49
wyjście)	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.

iGuard Fingerprint Securit File Edit View Favorite	<mark>y Syste</mark> s Tool	sm - Mie s Helc	crosofi	Intern	et Exp	lorer		
$ \exists \varphi = Back \bullet \Rightarrow \bullet \textcircled{3} \textcircled{3} $	 ⊿∣ ©) Search	»	Addres:	s 🚺 H	ittp://	203.80.	236.61/Admins/index.html
Employee List Internal Memory Smart Card	Guaro ompar	I™ Se iy Holi	ecur iday L	ity Sy .ist	/ster	n		▲ Help
Add Employee Department List Add Department Access Control		Dat	e of H	loliday	(mm	/dd/	' YYYY): 09/10/2001 Add
Other Branch Administration Terminal Status Password Setup Terminal Setup Clock Setup	Sel	ect Mo	nth:	Sep, 20	01 💌	Go	,	Company Holiday (mm/dd/yyyy)
	Sep, 2001 Sun Mon Tue Wed Thu Fri Sat							09/10/2001 10/30/2001 12/25/2001
Clock Setup In/Out Trigger Holiday Setup Terminal List Add Access Log Tools	2 9 16 23 30	3 10 17 24	4 11 18 25	5 12 19 26	6 13 20 27	7 14 21 28	8 15 22 29	
Exports (XLS) Exports (TXT) Export Employee Backup Restore	C	lick to	add d	late to	holida	ay lis	t	Click to remove date from holiday list.
Web Camera								Last Updated: Mon, 2 Jul 2001 22:59:14

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

Des Feet Terre (Free	ites Loois Heip	and the second	
🕁 Back 🔹 🤿 🔸 🎯 [] 🖄 📿 Search 👋 🛛 Addre	ss 🚺 http://203.80.236.61/Admins/index.html	• @Go
·	Wenesday		
iGuard™	Thursday		
Security System	Friday		
Terminal: Main	Saturday		
	Holiday		
Search Employee -	Remarks : Apply onl	y in Access Control Mode. N/A in Time Attendar	nce Mode
C Internet in the second	Terminals		
• By ID			Charles and
By Last Name	🔽 Main	Grice	
Go			
Go		Save Delete	

- 23 -

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.

🖉 iGuard Fingerprint Se	curity System - Microsoft Internet Explorer	
Eile Edit View Fav	rorites <u>I</u> ools <u>H</u> elp	
] 🕁 Back 🔹 🤿 👻 🎱	2 🖓 🔞 Search 🛛 🖹 Address 🚺 http://203.80.236.61/Admins/index	u.html ▼ 🖓 Go
Employee List Internal Memory	iGuard [™] Security System	
Smart Card Add Employee	Add Access Record	Employee Help
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	New Access Record: ID: Date: 07/02/2001 (MM/C Time: (HH:M In/Out: © In © Out Save	DD/YYYY) 4M:SS)
Tools Exports (XLS)	Last Up ©2000 Luck	pdated: Mon, 2 Jul 2001 23:06:58 kv Technology. All rights reserved. 🔻
Done		Internet

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

🗿 iGuard Fingerprint Se	curity System	n - Micro	soft Internet Explorer					_ 8 >
<u>File E</u> dit <u>V</u> iew F <u>a</u> r	vorites <u>T</u> ools	Help						1
+ - → - 🙆 🗗 🖉	3 0 0 0	3 3.	🔄 🛛 👌 🖉 ht	tp://192.16	8.0.252/Admins/	index.html		▼ 🖓 Go
Links 🙋 Yahoo! 🙋 iG	uard WebPage	@] 140	@141 @142 @Flat	C 🙋 Fla	B EFP_C	€ FP_B €I	P_A	د
Search chiployee	iGuard	™ Sec	urity System		-			
● By ID	Access	nn		First	Previous	Next L	ast Emplo	vee Help
C Bu Last Name	Incourse L	Rabely av	COLORAN AL COLORAN COLORA	Becky State	STREET, STOLEN STOLEN			Part Charles and
Go		ID:	Department:	Period	: From	n / To (mm/c	d/vvvv)	
do			All Departments	All	-		G	
Reports	122		Contraction of the second					
Access Log	No.	ID	Name		Date	Time	Terminal	In / Out
Attendance		1.20		+ 48 -		-	The second second	
List	631.	B1009	Chu, Kin Man	木健氏	10/09/1999	18:02:49	FLATE	Out
Add New	633	A1015	Tsui, Ping Fuk	徐平福	10/09/1999	18:01:57	FLATE	Out
Department	E 634	B1011	Leuna, Wei Kun	梁維根	10/09/1999	18:00:00	*Manual*	Out
List	635	A1176	Chow Sin Yee	周倩儀	10/09/1999	17:01:15	FLATC	Out
Administration	636.	A1045	Mo, Hang Hing	巫恒興	10/09/1999	16:11:28	FLATC	Out
Terminal Status	637.	B1077	Yu, Andre	余妙爱	10/09/1999	15:14:57	FLATB	In
Password Setup	638 .	B1166	Chan, Chuen	陳泉	10/09/1999	15:00:00	*Manual*	Out
Terminal Setup	639.	B1138	Chan, Jessie	陳詩慧	10/09/1999	14:22:13	FLATB	Out
Password Access	640.	B1109	Yu, Venus	余惠芳	10/09/1999	14:22:02	FLATB	Out
In/Out Trigger	641.	B1106	Cheung, Sherry	最思读 進制の	10/09/1999	14:21:50	FLATB	In
Holiday Setup	642	B1082	Cheung, Moni	市設係	10/09/1999	14:21:41	FLATE	In
Terminal List	644.	C001	Leung, Brian	梁瑞基	10/09/1999	13:47:29	FLATB	In
Add Access Log	645.	C001	Leung, Brian	梁瑞基	10/09/1999	13:46:10	FLATB	In
Exports (XLS)	646.	A1045	Mo, Hang Hing	巫恒興	10/09/1999	13:39:50	FLATB	In
Exports (TXT)	647.	B1017	Liu, Joseph	廖傳偉	10/09/1999	13:12:36	FLATB	Out
Backup	648.	A1045	Mo, Hang Hing	业恒興	10/09/1999	13:01:47	FLATB	Out
Restore	649.	811/5	Lee, Dick	学山康	10/09/1999	13:00:18	FLATE	Out
	650.	B1014	Tso, Chung Ling	EITT	10/03/1333	12:20:59	FLAIB	Out .

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

🚰 iGuard Fingerprint Sec	urity	Syster	n - Microsol	ft Internet Explorer				
File Edit View Favo	orites	Tools	Help					-
] 🕁 Back 👻 🤿 – 🙆 [2 6	8 Q	Search »	Address 🚯 http://203	.80.236.61/A	dmins/index.html		• 🖓 60
Smart Card		E2	•	= 6/30/2001				
Add Employee	1	A	В	C	E	F	G	Н
Department	1	No.	Employee	Name	Date	Time	Terminal	In/Out
LIST Add Department	2	1	A1155	Shek, Ying Kuen	6/30/2001	21:46:39	Main	OUT
Access Control	3	2	BB02	Hui, Jacky	6/30/2001	19:44:12	Main	OUT
Quick Access	4	3	A1188	Lam, Kan On	6/30/2001	19:30:57	Main	OUT
Other Branch	5	4	B1186	Yeung, Yan Wah	6/30/2001	18:13:21	Main	OUT
Administration	6	5	A1154	Chow, Man Keung	6/30/2001	18:12:52	Main	OUT
Terminal Status Recoverd Setup	7	6	A1050	Chan, KC	6/30/2001	18:10:08	Main	OUT
Terminal Setup	8	7	B1011	Leung, Wei Kun	6/30/2001	18:08:03	Main	OUT
Clock Setup	9	8	A1019	Chan, Chuen Heung	6/30/2001	18:04:31	Main	OUT
In/Out Trigger	10	9	A1176	Chow, Sin Yee	6/30/2001	18:03:03	Main	OUT
Terminal List	11	10	B1004	Mo. Lee Fong	6/30/2001	18:02:55	Main	OUT
Add Access Log	12	11	A1010	Liu, May Wan	6/30/2001	18:02:39	Main	OUT
Tools	13	12	A1041	Chan, Kin Wai	6/30/2001	18:02:22	Main	OUT
Exports (XLS)	14	13	B1006	Tam, Hon Kee	6/30/2001	18:02:05	Main	OUT
Exports (1A1)	15	14	A1007	Tsui, Ping Fuk	6/30/2001	18:01:54	Main	OUT
Backup	16	15	A1015	Chu, Chuk Ching	6/30/2001	18:01:46	Main	OUT
Restore	17	16	A1002	Wong, Kit Ching	6/30/2001	18:01:36	Main	OUT -
Web Camera			\ex010702					
E Done							🤡 Inter	rnet

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

5.3. Reports – Access Log

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

		123324 70	7					
🗘 Back 🔹 🤿 👻 🔰) 4	QSearc	th 🙀 Favorites 😕	Address	Http://192.168.0.	250/Admins/ind	ex.html	
	iGua	ard™ S	Security System			and the second		Sheet and
iGuard ^M	Acce	ss Log		1	First Previous	Next	Last Emp	loyee Help
oursinal iGuard	THE OWNER	- Milles		1. 10 to 10 to 10	MA SAME		STRANGESOL:	Supression and
entima: reliaria	ID:		Department:	Period:	Fr	om / To (mn	n/dd/vvvv)	
earch Employee	10		All Denartments	- Al	-	· · · · · · · · · · · · · · · · · · ·		Go
	and the second		Trin beparantino 1			TAR AND		
• 8v 1D	No.	ID	Name		Date	Time	Terminal	In / Out
By Last Name	1	B1106		西田住	100/27/2001	10.57.22	Office	In
Co	5	41155	Shek Ying Kuen	石茎梗	06/27/2001	09:56:21	Main	In
Go	3	BBD1	Leung, Brian	初時世世	06/27/2001	09:50:35	Main	In
and a state of the	4.	B1077	Yu. Andre	会创爱	06/27/2001	09:41:08	Office	In
eports	5.	A1019	Chan, Chuen Heung	陣息香	06/27/2001	09:32:57	Main	In
ccess Log	6.	BB13	Chuna, Andy	iComm	06/27/2001	09:29:49	Main	In
cendance.	7.	B1014	Tsp. Chung Ling	曹仲玲	06/27/2001	09:25:53	Office	In
npioyee List	В.	B1109	Yu, Venus	余惠芳	06/27/2001	09:23:33	Office	In
dd Employee	9.	A1007	Tsui, Ping Fuk	徐平福	06/27/2001	09:19:05	Office	In
enartment	10.	A1154	Chow, Man Keung	周交强	06/27/2001	09:15:27	Main	In
st	11.	B1138	Chan, Jessie	陳詩慧	06/27/2001	09:14:27	Office	In
dd Department	12.	B1196	Fung, Emily	调查药	06/27/2001	09:11:24	Office	In
cess Control	13.	A1041	Chan, Kin Wai	陳建威	06/27/2001	09:10:50	Main	In
uick Access	14.	A1002		100 <u></u>	06/27/2001	09:06:34	Main	In
ther Branch	15.	81172	Chan, Natalie	陳敬儀	06/27/2001	09:02:38	Office	In
Iministration	16.	B1004	Ma, Lee Fong	巫莉芳	06/27/2001	09:01:38	Office	In
erminal Status	1 17.	B1006	Tam, Hon Kee	譚漢祺	06/27/2001	09:00:41	Main	In
rasswora Setub	L	DA DA A	1 and a Atlantice	<76440	00.007/0001	00.57.44	1.8 mile	F-

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:

🗿 iGuard Fingerprint See	curity Sy	stem - Mio	rosoft Internet	Explorer					_ _ >
Ele Edit Yiew Fav	orites]	jools <u>H</u> elp	ia						100
4=Back 🔹 🔿 - 🙆	1	QSearch	🙀 Favorites	10	Address 🖉 Http:	//192.168.0.250/Adh	iins/index.html		• 🗟
-	iGua	ard™ Se	curity Sys	stem	-		123		-
iGuard Mark	Acce	ss Log			First	Previous Nex	t Last	Employee	Help
Terminal: iGuard	ID:		Denarti	nent	Period:	From / 1	n (mm/driAv	(9.9)	
Search Employee	A10	50	All Depa	artments 🚽	Last Month 💌	05/01/2001	05/31/2	001	Go
• By 1D	No.	ID	Name		Date	Time	Terminal	In / O	ut
By Last Name	1.	01050	Chan KC	油面样	05/31/2001	18:43:12	Main	Out	
Go	2.	A1050	Chan, KC	陳國柱	05/31/2001	08:54:42	Office	ln	
	3.	A1050	Chan, KC	陳國柱	05/30/2001	18:41:04	Main	Out	E CALLER -
	4.	A1050	Chan, KC	陳國柱	05/30/2001	09:01:24	Main	ln	
Reports	5.	A1050	Chan, KC	演回柱	05/29/2001	19:15:08	Main	Out	
Attendance	6.	A1050	Chan, KC	陳國柱	05/29/2001	08:54:05	Office	ln	
Employee List	7.	A1050	Chan, KC	直 國柱	05/28/2001	18:55:47	Main	Out	
List	В.	A1050	Chan, KC	陳國柱	05/28/2001	08:55:14	Office	ln	
Add Employee	9.	A1050	Chan, KC	 」 」 」 」	05/26/2001	18:09;23	Main	Out	
Department	10.	A1050	Chan, KC	陳國柱	05/26/2001	08:47:14	Main	ln	
List	11.	A1050	Chan, KC	陳國柱	05/25/2001	18:44:09	Office	Out	
Add Department	12.	A1050	Chan, KC	陳國柱	05/25/2001	08:50:07	Main	In	
Access Control	13,	A1050	Chan, KC	陳國柱	05/24/2001	18:30:21	Main	Out	
Quick Access	14.	A1050	Chan, KC	陳國性	05/24/2001	09:06:13	Main	In	
Other Branch	15.	A1050	Chan, KC	陳國柱	05/23/2001	19:03:24	Office	Out	
Administration	16.	A1050	Chan, KC	旗國柱	05/23/2001	08:50:12	Office	In	
Possword Setup	17.	A1050	Chan, KC	陳國柱	05/22/2001	18:44:05	Main	Out	
Done								🗿 Internet	

5.4. Reports Attendance

🗿 iGuard Fingerprint Se	curity S	stem - N	licrosoft	Internet Explore	r						1	-101
<u>File E</u> dit <u>V</u> iew F <u>a</u> v	rorites	<u>T</u> ools <u>H</u>	elp									193
4=Back 🔹 🔿 👻 🎱	9 6	Q Sear	°n <u>k</u> a⊨	avorites ¹	2 Address 🖉 Http:	//192.168.	0.250/Ad	mins/inde	ex.html		•	(PGG
-	iGu	ard™	Securi	ty System	Carlos Contraction		ANE:	100				
iGuard "	Atte	ndance	Report		First	Previou	s Ne	kt	Last	Empl	oyee He	lp
Terminal: IGuard						新聞の						
	ID:		C	Department:	Period:	-	rom /	To (mr	n/dd/y	<u> </u>	112 200	111
Search Employee		- Alterna		All Departments	Last Week	- 05/17/	2001	(C	16/23/2	001	Go	
• By 1D	No.	ID	Name		Date	In	Out	ťn	Out	1n (Out More	
O By Last Name	1.	A1002	Wong, I	Kit Ching	06/18/2001 Man	09:24	18:06	;	;	;	;	and the second
Go	2.				06/19/2001 Tue	09:12	18:06	:		!	!	
	3,				06/20/2001 Wed	09:00	18:03	·····	:	:	!	
Pennets	4.				06/22/2001 Thu	09:34	10.04					
Access Log	6.				06/23/2001 Sat	09:06	18:03		!			
Attendance	7.	A1007	Tsui, Pir	na Fuk	06/18/2001 Man	08:57	18:02					
Employee List	8.	High A			06/19/2001 Tue	09:09	18:03	:	;	;	;	
List	_ 9.				06/20/2001 Wed	08:48	18:02	:	:	:	;	
Add Employee	10.				06/21/2001 Thu	08:55	18:02		्रोक्त्रांत्त्व	; :		
Department	11.				06/22/2001 Fri	08:56	18:35	;	·	;		
USE Odd Department	12.	A1010		. 161-0	06/23/2001 Sat	08:55	18:04	14.00	10.01	:		
Add Department	13.	ALUIU	Liu, May	y wan	06/18/2001 Man	00.55	13:02	14:08	19:04			
Quick Access	15				06/20/2001 Tue	00.00	13.00	13.53	18:00			
Other Branch	16.				06/21/2001 Thu	D8:4E	13:01	13:51	18:01			
Administration	17.				06/22/2001 Fri	08:45	13:02	13:36	18:02			
Terminal Status	1 18.				06/23/2001 Sat	08:58	13:04	13:46	18:04	+ ;		
Possword Setup	1 10	A1015	Chu Ch	nuk China	06/18/2001 Man	08.52	18 02	1000000				115-2
Done										💋 Inter	net	

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.

iGuard iServer				_02
Eile View Server Ierminal	s Tools Help ? Boout Exit			
Unlock iGuard02 iG	uard01 🚺 iGua	rd		
Server Server Access Log Reports Event Log Guard Terminals Guard132 Guard01 Guard01 Guard02	Name Guard132 Guard01 Guard02	192.168.0.132 192.168.0.101 192.168.0.102	Description iGuard FingerPrints iGuard FingerPrints iGuard FingerPrints	Senal No. VK-9940-0147-F113 VK-9940-01F4-F13E VK-9940-01C7-F13B
ERM: 3	Server	🖳 iGuards 🔀	Access Log 🛃 Rep	oorts 🖳 Event Log

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, TerminaIID)

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), TerminaIID char(20), InOut Int, Primary Key(RCDID, EmployeeID, LogDate, LogTime, TerminaIID)

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 \rightarrow Narzędzia Administracyjne \rightarrow ODBC \rightarrow System DSN \rightarrow 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	Przeka ź nik drzwi normalnie otwarte	
СОМ	Przeka ź nik drzwi masa	
NC	Przeka ź nik drzwi normalnie zamkni ę te	
DOOR SW	Prze łą cznik drzwi	
DOOR SW	Prze łą cznik drzwi	
A-RS485	Pod łą czenie do iGuard	
B-RS485	Pod łą czenie 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	0	2. Westing the figure and Terminaly included and the second states of the strength of the stre
4	ŏ	2. W oknie koninguracji reminalu iGuaru malezy zaznaczyć checkbox output w Remote Door Relay Setup
5	16	
U	10	
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

-	Prese Mudel:
Access Log	AXIS 2100 V2.0X
Attendance Daily In / Out	Cam 4's Descriptions :
mployee List Internal Memory	Wiegand Setup:
Smart Card Add Employee	Output : 🥅 Enable
epartment	Site Code : 0
Add Department	Note : Only last 4 digit of Employee ID will be used as the card no. (Wiegand 26bit format)
Quick Access Other Branch	Remote Door Relay Setup: Output : F Enable
Terminal Status Password Setup	Remote Relay ID : 0 (0 - 255)
Diock Setup In/Out Trigger Holiday Setup	Serial No : VK-2003-01AF-105A
Ferminal List Add Access Log D ols Exports (XLS)	Terminal may need to restart after configuration saved.
Exports (TXT) Export Employee Backup Restore Web Camera	Last Updated: Sat, 19 Jun 1982 12:25:0 ©2001 Lucky Technology. All rights reserve
	🔰 👘 Internet

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 (domvślny)	Jeśli wybrna jest wartość domyślna tego parametru ustawienia przełacznika IN/OUT sa ustawiane w In/Out Trigger Setup (patrz sekcia
	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 recznie wybierać za pomoca przycisku return (\leftarrow) z klawiatury
Status	terminalu. Odpowiednie zapisy zostaną również umieszczone w systemie
	logów. Stosownie do wymagan oznaczenia F1 – F4 mogą być przypisane okroślonym 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.

Reports	AXIS 2100 V2.0X Cam 3's Descriptions :
Daily In / Out Employee List Internal Memory	Cam 4's IP : 0.0.0.0 Model:
Add Employee Department	Cam 4's Descriptions :
Add Department Access Control Quick Access	Output: IF Enable
Other Branch Administration Terminal Status Password Seture	Site Code : 0 Note : Only last 4 digit of Employee ID will be used as the card no. (Wiegand 26bit format)
Terminal Setup Clock Setup In/Out Trigger	Remote Door Relay Setup: Output : T Enable
Holiday Setup Terminal List Add Access Log	Remote Relay ID : 0 (0 - 255)
Exports (XLS) Exports (TXT) Export Employee	Serial No : VK-2003-01AF-105A
Backup Restore Web Camera	Terminal may need to restart after configuration saved. Save

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

Reports Access Log Attendance Daily In / Out	Time Server: F Enable (All other iGua with this iGuard) Web Cam Setting (IP = 0 to disable):	ords in the network will synchronize
Employee List Internal Memory Smart Card Add Employee	Cam 1's IP : 0.0.0.0	Model:
Department	Cam 1's Descriptions :	
Add Department Access Control Quick Access	Cam 2's IP : 0.0.0.0	Model:
Other Branch Administration Terminal Status	Cam 2's Descriptions :	
Password Setup Terminal Setup Clock Setup In/Out Trigger	Cam 3's IP : 0.0.0.0 AXIS 2100 V2.0X	Model:
Holiday Setup Terminal List	Cam 3's Descriptions :	
Add Access Log Tools Exports (XLS) Exports (TXT)	Cam 4's IP : 0.0.0.0	Model:
Export Employee Backup Pestore	Cam 4's Descriptions :	
Web Camera	Output : T Enchip	<u>.</u>

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.

Reports	authorized)
Access Log Attendance	Log Unauthorized Access : Enable (if enabled, unauthorized smartcard access record will be added to log)
Employee List	Web Server Options :
Smart Card	Access Restrictions : • No IP Address Restrictions
Add Employee	C Specified IP Address Range
List	(Example: 192.168.0.0-192.168.0.100)
Add Department	Rejected address can access after Authenticate
Quick Access	(System Administration / User Administration Password.)
Other Branch	Must Authenticate before Access
Terminal Status	Web Page Language : English
Password Setup Terminal Setup	Note: Your browser may need to restart if Language of Web
Clock Setup	Fingerprints Matcher Setting :
Holiday Setup Terminal List	Security Level : High 💽 (Default: Standard)
Add Access Log Tools	Automatch Security Level : Maximum 🗾 (Default: Maximum)
Exports (XLS)	Door Relay and Beep Setting :
Exports (1X1) Export Employee	Door Switch : 🗖 Disable
Backup Restore	Door Relay Control for 'In' : 🙃 Enable
Web Camera	C Disable

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.

Poporte	 Static IP ; 192.168.0.132
Access Log	Subnet Mask : 255.255.0
Daily In / Out	DNS Server IP : 192.168.0.200
Internal Memory Smart Card	Default Gateway IP : 192.168.0.200
Add Employee Denartment	Internet SNTP Time Server time synchronization
List	SNTP Time Server URL : stdtime.gov.hk
Add Department Access Control Quick Access Other Branch	Status : F Enabled To use SNTP Time synchronization, DNS Server IP and Time Zone (Clock setup) must be valid.
Administration Terminal Status Password Setup Terminal Setup Clock Setup	Operation Setting : Weekday Start : 0 (0 = Sunday, 1 = Monday 6 = Saturday)
In/Out Trigger Holiday Setup Terminal List	Others Options : Default In/Out : Follow In/Out Trigger 💌
Add Access Log	Disable 'Key-In' ID: 🔽 Yes
Exports (XLS) Exports (TXT)	Quick Access By Key-In ID: 🏳 Yes (cannot use with "Disable 'Key-In' ID")
Export Employee	Anti-Pass-back: 🗖 Yes (Not applicable if 'Auto In/Out Trigger' is selected)
Restore	Disable Enrollment Overwrite : 🔽 Yes
web camera	Extended In/Out Status : 🗆 🕫 🗖 🕫 🗖 🕫 🗖 🕫 🖊 💆

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.

ittendance Jaily In / Out	System Clock Setup		Helt
nployee List nternal Memory	Clock Adjustment:		
mart Card dd Employee partment st	New Date : 6/19/2003	(mm/dd/yyyy)	
ld Department cess Control uick Access her Branch ministration erminal Status	Auto Date/Time Value : © ON © OFF (Values shows the Click 'OFF' to stop o	(nn:mm:ss) time on your PC, lock and enter value manually)	
ssword Setup rminal Setup ack Setup /Out Trigger bliday Setup	Serial No : VK-2003-01AF-105A	<u></u>	
rminal List d Access Log ils ports (XLS) ports (TXT)		Save	
ports (171) port Employee ckup		Last Updated: Sat, 19 Jun	1982 12:17

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.

	AND 1935 BOOK 1 YES (NOT APPLICABLE IF AUTO IN/OUT INIGGER IS SElected)		
Access Log	Disable Enrollment Overwrite : TYes		
Attendance Daily In / Out	Extended In/Out Status : 🔽 F1 🔽 F2 🖵 F3 🖵 F4		
Employee List	Show Chinese on Terminal : 🥅 Enable		
Smart Card Add Employee	Show only ID when Authorized : Enable (if enabled, only Employee ID will be shown when authorized)		
List Add Department	Log Unauthorized Access : F Enable (if enabled, unauthorized smartcard access record will be added to log)		
Access Control Quick Access Other Branch	Web Server Options : Access Restrictions : No IP Address Restrictions		
Administration Terminal Status Password Setup	C Specified IP Address Range (Example: 192,168.0.0-192,168.0.100)		
Terminal Setup Clock Setup In/Out Trigger Holiday Setup Terminal List	Rejected address can access after Authenticate (System Administration / User Administration Password.)		
Tools	Web Page Language : English		
Exports (XLS) Exports (TXT) Export Exployee	Note: Your browser may need to restart if Language of Web page changed.		
Backup	Fingerprints Matcher Setting :		
Restore Web Camera	Security Level : High 🔄 (Default: Standard)		
	🗶 Automatch Security Level : Maximum 🚽 👝 🧭 🧰 🧰 🔨		

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	Wy ś wietlacz LCD
W czasie gdy urządzenie jest w trybie oczekiwania wciśnij FUNC i	Enter Password: _
wpisz hasło administratora.	
Wciśnij FUNC aby potwierdzić a następnie wybierz opcję 7	Press 7: System
"System Shutdown/Reset	Shutdown/Reset
Teraz system poprosi Cię o podanie czy chcesz usunąć bazę	Reset User Dbase
danych użytkowników. Wybierz 1 aby to zrobić lub 2 aby ominąć	Yes/No (1/2)? _
Teraz system poprosi Cię o podanie czy chcesz usunąć bazę	Reset User Access Log
zapisanych logów przejść. Wybierz 1 aby to zrobić lub 2 aby	Yes/No (1/2)? _
ominąć	
Teraz system poprosi Cię o podanie czy chcesz przywrócić	Factory Default
domyślne ustawienia urządzenia. Wybierz 1 aby to zrobić lub 2	Yes/No (1/2)? _
aby ominąć.	
System wykonuje procedurę resetu a następnie powraca do trybu	Mon Aug 30 13:46
oczekiwania.	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	Wy ś wietlacz LCD
W czasie gdy urządzenie jest w trybie oczekiwania wciśnij FUNC i	Enter Password: _
wpisz hasło administratora.	
Ponownie wciśnij FUNC aby potwierdzić a następnie naciśnij	== Test Mode! ==
klawisz "A". Na wyświetlaczu pojawi się napis "Test Mode". Tera	ID #:_
możesz testować wzorce i szkolić pracowników.	
Według tej same powyższej procedury ponowne wciśnięcie	Mon 30 Dec 13:49
klawisza "A" spowoduje opuszczenie trybu testowego.	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

