Access Controller NAC-3000

Terminal User Manual

NITGEN
biometric solutions

니트젠 고객지원센터

Tel. 080-060-1600
(수신자 부담)
Fax. 02-3415-1601
E-mail : customer@nitgen.com
URL : http://www.nitgen.com

목 차

제1장
시작하기 전에

1.1 제품 소개

■ 개 요

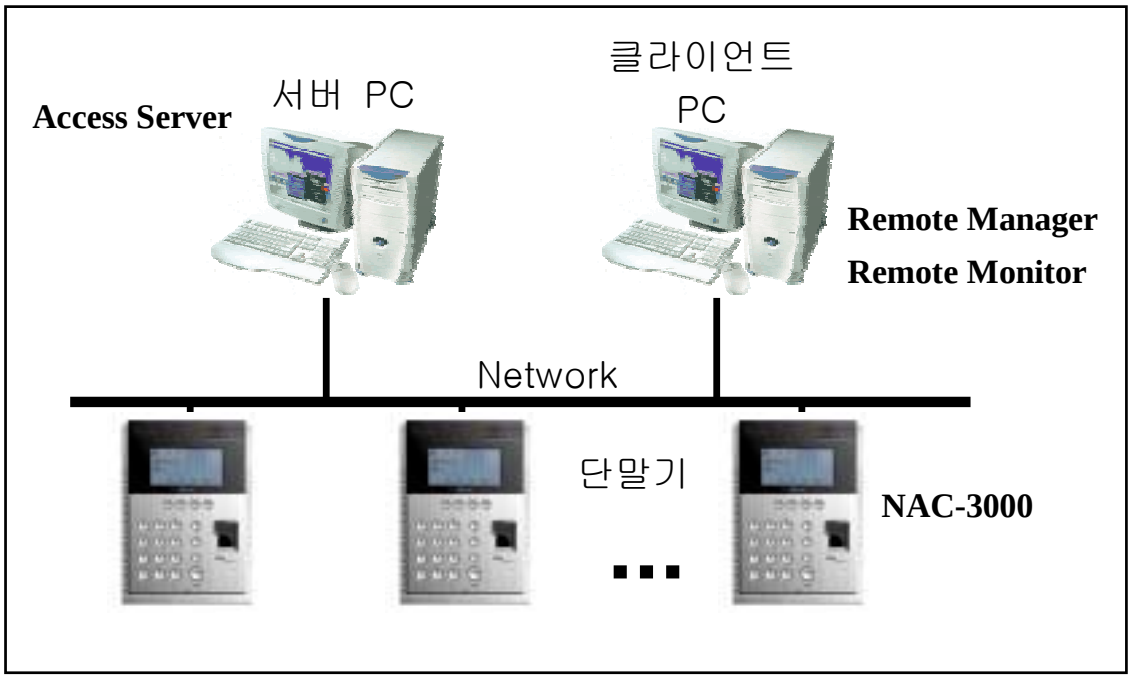
최근 각종 인증시스템에 활용되고 있는 생체인식 시스템은 고도의 보안을 필요로 하는 곳뿐만 아니라, 사용상의 편리함과 경제성으로 그 이용이 점차 증가 하고 있습니다. 여러 생체인식 시스템 중에서도 지문인식 시스템은 이용이 편리할 뿐만 아니라 경제적인 제품구현, 다양한 형태의 응용 개발이 가능하여 생체인식 시장의 대부분을 차지하고 있습니다. 지문인식 업계의 선도 업체로 성장해온 ㈜니트젠은 지문인증을 이용한 PC보안, 지식관리, 금고, 출입통제, 전자결재, 금융결제 등 다양한 솔루션을 제공하고 있으며 지속적인 연구개발과 품질관리를 통해 고객요구에 능동적으로 대응하고 있습니다.

니트젠 출입통제 시스템은 지문인식 알고리즘, 광학식 센서, 임베디드 설계 기술, 소프트웨어 응용기술 등 세계적으로 인정 받아온 니트젠의 핵심 기술들이 유기적으로 결합되어 최적화된 우수한 제품입니다. 또한, 비밀번호 또는 ID카드만을 사용하는 지금까지의 출입통제 시스템과 달리 비밀번호 망각, 카드 도용 또는 복제의 위험 없이 편리성과 보안성을 동시에 만족시키고 있으며, 독립적으로 운용되어 왔던 단말기들을 네트워크로 원격지에서 통합적으로 모니터링하고 체계적으로 관리할 수 있도록 운영의 효율성을 최대한 고려하여 설계되었습니다.

니트젠 출입통제 시스템은 RF카드, 비밀번호, 지문인증을 다양하게 조합하여 사용할 수 있으며, 그룹ID, 단축ID, 1:N 매칭 기능 등 편리한 기능과 인터폰 및 음성안내 기능이 내장되어 있어 기업체 및 관공서 등의 다양한 고객환경에 이용될 수 있도록 범용성과 특수성을 함께 고려하여 설계된 제품입니다.

본 매뉴얼은 니트젠 출입통제 단말기(NAC-3000)의 사용방법에 대하여 설명합니다.

■ 시스템 구성



구 성	주요 기능
서버 PC	1. 서버S/W : Access Sever 2. 단말기 통신, 로그 데이터 수집 3. 사용자 정보 및 로그 데이터 DB 4. 인증 수행
클라이언트 PC	1. 클라이언트S/W : Remote Manager/Monitor 2. 사용자 등록 등 관리 기능 3. 단말기 상태 및 이벤트 모니터링
단말기 (NAC-3000)	1. 사용자 확인 및 인증 수행 2. 출입문 제어

니트젠 출입통제 단말기(NAC-3000)는 단독으로도 모든 기능을 사용할 수 있으며, 네트워크에 연결하여 관리용 프로그램(Access Server, Remote Manager, Remote Monitor)과 함께 사용할 경우 많은 수의 단말기를 좀 더 편리하고 효율적으로 관리할 수 있습니다. 서버S/W와 클라이언트S/W는 한 PC내에서도 사용 가능합니다.

1.2 제품 특징 및 사양

■ 제품 특징

니트젠 출입통제 시스템(NAC-3000)은 다음과 같은 특징들을 가지고 있습니다.

① 대규모 출입인원의 통제 및 관리

② 다양한 인증 방식의 조합 (지문, 암호, RF카드)

③ 다수의 출입 통제 단말기를 네트워크를 통하여 통제

④ 시스템의 원격 관리 용이(서버/클라이언트PC 분리 가능)

⑤ 사용자 출입 이력 조회, 인터폰 등 다양한 부가 기능

⑥ 실시간 출입 상황 모니터링

⑦ 기간 및 시간대별 출입 통제 기능

⑧ 근태 관리 등의 다양한 응용 프로그램 개발을 위한 SDK (S/W Developer's Kit) 제공 (별도)

⑨ 고속 1:N 인증 가능

⑩ 사용자 편리성 강화(단축ID/그룹ID인증, Auto-on)

■ 시스템 사양 (서버 연동 시)

구 분	내 용
접속 단말기	최대 255대 까지 연결 가능
원격 관리	최대 8개까지 서버에 동시 접속 가능
등록 인원	5,000 명 (1인당 2지문 등록) 10,000 명 (1인당 1지문 등록)
네트워크	TCP/IP, 10M bps
인증방식	지문, 패스워드, RF 카드(옵션)
인증속도	1:1모드 : 1초 이내

	1:N모드 · 평균 2.5초(1,000FP, 서버) · 평균 2초 (500FP, 단말기) · 평균 1초 (300FP, 단말기) ※PentiumIV 1GHz, 512MB RAM

■ 단말기 세부 사양

구 분		Spec.
Display	방식	128 * 64 Dots LCD
	언어	한글, 영문
센서	Model	OPP01
	방식	광학식
	해상도	500 DPI
	부가기능	Auto on / Latent Image Check
인증	속도	1:1모드 : 1초 이내 1:N모드 · 평균 2.5초(1,000FP, 서버) · 평균 2초 (500FP, 단말기) · 평균 1초 (300FP, 단말기) ※PentiumIV 1GHz, 512MB RAM
	알고리즘	FRR:0.1%이내, FAR:0.001%이내
등록인원	단말기	2,000 명 (1인당 2지문 등록) 4,000 명 (1 인당 1지문 등록)
통신	TCP/IP	10base-T Ethernet
	RS-232C	최대 115200bps(옵션)
	Wiegand	26bit, 34bit 모드(Output Only) ※ID길이는 4자리만 가능

크기	케이스	135(W)*45(L)*202.5(H) mm
	고정 브라켓	102.4(W)*26.6(L)*157.5(H) mm
도어지원	Dead Bolt / Strike / EM Lock / 자동문	
전원	어댑터	입력: AC 100V ~ 240V, 50/60 Hz 출력: DC 12V, 3A
부가기능	인터폰	MIC, Speaker 포함
	음성안내	
	로고/펌웨어 다운로드	
	ID 길이 설정 (4 ~ 15 자리)	
옵션	정전 시 비상전원장치 (12V / 2.9Ah)	
	RF Module (HID)	
온도	보관	-25℃ ~ 65℃
	동작	-20℃ ~ 60℃ (결로현상 없을 시)
습도	보관	15% ~ 90% RH
	동작	25% ~ 85% RH

1.3 제품 세부 명칭

① LED 램프 : 단말기의 동작 상태를 나타냅니다. 각 램프가 의미하는 바는 좌측부터 아래 표와 같습니다.

구분	동작상태	Color
Power	전원의 상태를 표시하며, Power On 시에 LED가 점등 됩니다.	적색
Network	네트워크의 연결상태를 표시하며, Network 연결 시 LED가 점등 됩니다.	녹색
Door	출입문의 개폐상태를 표시하며, 출입문 개방 시 LED가 점등 됩니다.	녹색

② LCD화면 : 모든 동작상태를 문자 메시지로 표시합니다.

③ 키 패드 : ID입력 또는 환경설정 시에 사용하며, 각 키별 사용 용도는 아래 표와 같습니다.

구분	설 명
0 ~ 9	숫자를 입력할 때 사용합니다.
*, #	방향버튼, 메뉴를 선택할 때 커서를 위 아래로 이동시킬 수 있습니다. *(Backward), #(Forward)
Enter	ID입력 또는 환경설정을 한 후에 이 버튼을 사용하여 입력을 마무리합니다.
Cancel	입력한 숫자를 하나씩 지우거나 메뉴에서 상위 메뉴로 올라갈 때 사용합니다.
Call	방문자가 인터폰으로 내부와 연결/통화해야 할 경우에 사용합니다.
Menu	환경을 설정하거나 변경을 위해 사용합니다.
F1 ~ F4	사용자가 기능을 직접 정의하여 사용할 수 있는 버튼이며, 출근/퇴근/외출/귀사 등의 근태 관리 용으로도 사용할 수 있는 버튼입니다. 기능키는 연동하는 S/W의 요구사항에 따라 자유롭게 설정하여 사용할 수 있습니다.

④ 스피커: 음성안내 및 인터폰통화, 경고음 발생시 사용됩니다.

⑤ 지문 입력 센서 : 지문 입력을 받는 장치입니다.

⑥ Auto-On 스위치 : 별도의 키 패드 조작 없이 지문 입력 센서에 손가락을 접촉하기만 하면 자동으로 지문입력이 되도록 하는 것입니다.

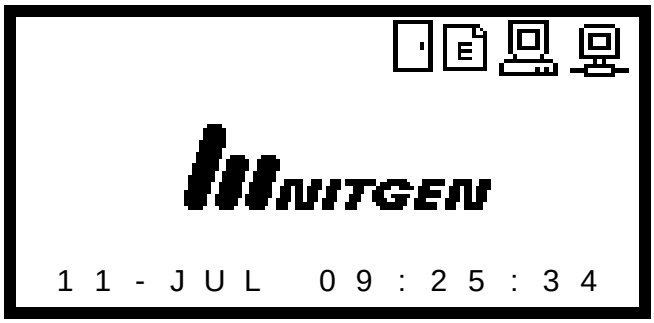
⑦ 마이크 : 단말기와 연결된 인터폰과 통신 시 음성을 송신하는 역할을 합니다.

⑧ Reset 스위치 : 단말기가 예기치 않은 상황으로 인하여 정상 동작하지 못할 경우, 단말기를 Reset 시키는 스위치 입니다.

1.4 ＬＣＤ화면구성

■ 단말기 초기 화면

단말기 초기 화면은 다음의 그림과 같습니다. LCD창의 상단부에 단말기의 상태를 표시해 주는 아이콘이 표시되어 있으며,중앙부에는 관리자가 지정해 준 로고 그림이 있고 하단부에는 현재 날짜와 시각이 표시됩니다.



■ 단말기 초기 화면

LCD화면에 표시되는 각종 아이콘의 의미는 다음 표와 같습니다.

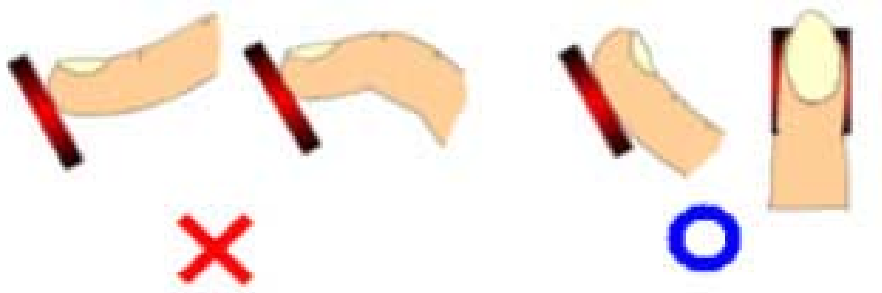
아이콘	표시 내용
	도어락 장치와 연결되어 문의 상태를 표시합니다.
	사용자의 신분이 인증되어 문이 열릴 때 표시됩니다.
	LCD 창의 상태가 영어로 표시될 때 나타납니다.
	LCD 창의 상태가 한글로 표시될 때 나타납니다.
	단말기 모드 표시 SO (Stand Alone) : 모든 동작이 단말기에서만 이루어집니다.
	NS (Network Server) : 서버에서 인증하는 모드입니다.

	NL (Network Local) : 단말기 내에서 인증하며 서버에 로그가 저장됩니다.
	단말기가 서버와 연결될 때 표시됩니다.
	단말기가 서버에 연결되지 않을 때 표시됩니다.

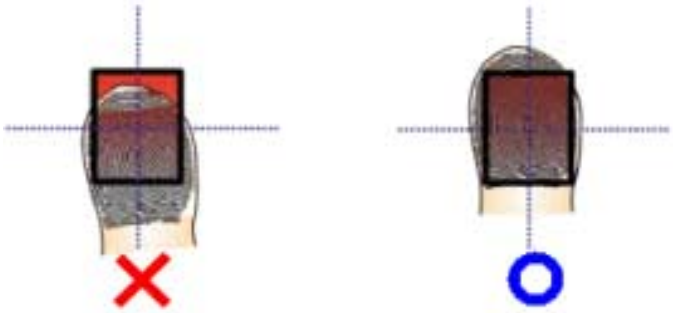
1.5 지문입력안내

사용자 지문 등록 및 인증 시 아래와 같은 방법으로 지문을 입력하면 인증오류를 방지할 수 있습니다.

① 입력 면적을 최대화하며, 누르는 힘을 고르게 합니다. 가장 약하게 눌렀을 때를 0%, 가장 강하게 눌렀을 때를 100%라고 가정하면 약 50~70%의 힘으로 지긋이 눌러주십시오.



② 지문 형상의 중심점 (Core)을 중앙에 오도록 합니다. 일반적으로 지문의 중심점은 손톱의 반달모양과 동일선상에 위치하므로 지문입력 시 손톱의 반달모양이 지문입력창의 중앙에 위치하도록 입력하십시오.



1.6 인증방법

니트젠 출입통제 시스템은 지문과 비밀번호, RF카드(옵션)를 인증 수단으로 사용할 수 있으며, 고객환경에 따라 개인별로 아래와 같은 인증방법을 편리하게 설정할 수 있습니다.

■ 지문 인증

지문을 이용하여 출입 권한을 확인하는 방식으로 아래와 같이 다양한 방법으로 사용할 수 있습니다.

- 1:1 인증
  미리 등록한 ID를 입력 후 지문을 입력하는 방식으로, ID에 해당하는 등록된 지문과 입력된 지문을 1:1로 비교하는 방식입니다. 1:1인증방식은 사용자수와 관계없이 인증시간이 매우 짧습니다. 특별히 시스템에서 설정할 필요는 없으며 ID를 입력한 후 지문을 입력하시면 인증 절차를 수행합니다.

- 1:N 인증
  등록된 지문만으로 인증하는 방식으로 인증 절차가 간편하지만 사용자가 많을 경우 인증시간이 1:1인증 방식에 비해 다소 길어질 수 있습니다. 특별히 시스템에서 설정할 필요는 없으며 지문만 입력하면 인증 절차를 수행합니다. 만약 사용자가 많아 1:N 인증시간이 너무 오래 걸린다면 ‘ 1:N 시간설정’을 사용하십시오. 설정된 시간 내에 인증을 하지 못한 사용자의 경우 실패로 처리됩니다. ‘ 1:N 인증시간’에 관한 사항은 해당 항목을 참고하십시오.

- 단축ID (SID) 인증
  사용자 ID는 초기 설정에 따라 4자리 ~ 15자리까지 지정할 수 있습니다. 단축 인증은 ID입력절차를 간소화하기 위한 것으로, 설정된 ID를 모두 입력하지 않고 앞자리의 일부만 입력하여 인증 절차를 수행하는 방식입니다. 예를 들어 ID가 1234567인 사용자가 앞자리 12만 입력한 후 지문을 입력하면 시

스템은 12xxxxx로 시작하는 ID에 한해 1:N인증을 시도하게 됩니다. 특별히 시스템에서 설정할 필요는 없습니다.

- 그룹 인증
  그룹 인증은 사용자 그룹별로 1~4자리의 그룹ID를 지정한 다음, 인증 시 그룹 ID와 지문을 입력하여 인증 절차를 수행하는 방식입니다. 예를 들어 아파트 같은 공동 주택의 경우 호수를 그룹ID로 사용할 수 있습니다. 사용자 등록 시 그룹ID를 설정할 수 있으며, 다른 방식과 달리 **그룹ID 입력 후엔 반드시 F1 키를 누른 후 지문을 입력해야** 그룹인증 절차를 수행합니다.

- 근태 모드 인증
  근태 모드 인증은 기능키 (F1~F4)를 이용한 인증 방법입니다. 인증을 시도하기 전에 원하는 기능키를 누르고 인증을 시도하면, 로그에 그 기능키의 결과가 이력으로 남습니다. 그 이력을 근태의 데이터로 이용할 수 있습니다. 예를 들어 F1을 누르고 ID를 입력한 후 인증을 하면 그 ID+F1이 기록으로 남습니다. 또, F1만 누르고 1:N인증을 행하면 알맞은 ID를 찾아서 ID+F1을 기록으로 남기게 됩니다.

■ 비밀번호 인증

4~8 자리의 비밀번호를 통해서 출입 권한을 확인하는 방식이며 지문 훼손 등 특수한 경우에 사용됩니다.

■ RF카드 인증 (옵션)

사용자가 소지하고 있는 RF카드를 통해서 사용자의 신분을 확인하는 방식입니다. 시스템에 RF카드 번호를 미리 등록하여 분실 또는 도난에 대비할 수 있습니다.

■ 자동 근태모드 인증

일반 1:N 인증만으로 원하는 근태 결과를 자동으로 로그에 남길 수 있는 기능입니다. 예를 들어 집중적으로 특정 근태가 연속적으로 발생하는 경우에, 사용자가 기능키(F1~F4)를 매번 눌러주어야 하는 불편함을 없애기 위한 것입니다.
자동 근태모드로 들어가면 초기화면이 아래와 같이 바뀌게 되며, 이 경우 1:N 인증을 하면 인증 결과가 자동으로 해당 근태기능이 첨부되어 일일이 기능키를 누를 필요가 없게 됩니다.

자동 근태 모드를 설정하는 방법 및 해제방법은 다음과 같습니다.

1) 자동 근태 모드 설정하기 : 메뉴에서 그룹/근태 중에서 근태를 선택합니다. 이어서 초기화면으로 나온 후 원하는 기능의 키 패드의 기능키(F1~F4)를 4초 이상 누르고 있으면 각 기능키에 해당하는 자동 근태 모드로 들어갑니다.

2) 자동 근태 모드 해제하기 : CANCEL키를 1초 이상 누르면 자동 근태 모드가 해제됩니다.

참고)
근태 모드로 설정이 되어있으면, 사용자 등록 시, 그룹 ID를 입력할 필요가 없습니다.

제2장
환경 설정

2.1 메뉴 구성

■ 특 징

단말기의 전체 메뉴 구성은 아래와 같습니다. 메뉴를 이용하여 초기 환경 설정과 사용자 등록, 지문인식 장치 설정, 네트웍 설정 등을 할 수 있습니다. 메뉴를 사용하기 위해서는 단말기 키패드의 메뉴 버튼을 이용합니다.

사용자 등록, 정보변경 및 삭제방법과 등록인원, 버전 등의 정보를 얻는 방법은 다음 3장에서 다루겠습니다.

메 뉴	상세 메뉴
사용자 관리	1. 사용자 등록 2. 사용자 정보변경 3. 사용자 삭제 4. 모든 사용자 삭제
지문 센서 설정	1. 센서 옵션 2. 보안 등급 3. 캡쳐 모드 4. 지문입력시간설정 5. Auto-On 설정 6. 1:N 시간설정
UI 설정	1. 언어선택 2. 음성안내 3. 버튼음
출입문 설정	1. 열림 시간 설정 2. 경고 시간 설정
시스템 설정	1. 암호화통신 2. 로그저장 3. RF 카드 4. WIEGAND 5. 기능키 설정 6. 단말기모드 7. 시간설정

	8. 출입시간모드
출입시간 설정	1. 출입가능 요일 2. 출입가능 시작시각 3. 출입가능 종료시각
네트워크	1. 단말기ID 2. TCP/IP 3. 통신시간 제한 4. 포트설정
정보	1. 사용자 수 2. 펌웨어 버전
공장초기화	1. DB 포맷 2. 등록지문 수 3. ID 자리수 4. 리셋터미널

■ 마스터 인증

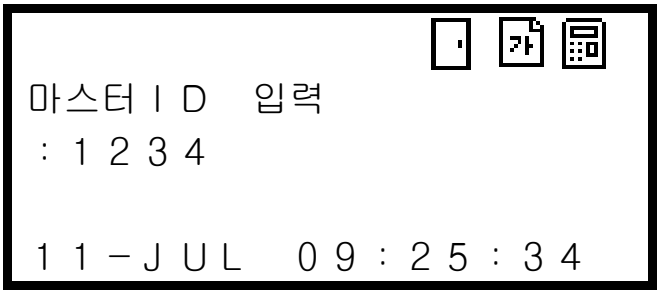
단말기 최초 설치 시에는 마스터의 인증 없이 환경설정이 가능하나, 마스터 등록 이후에 단말기의 환경설정을 변경하기 위해 메뉴를 사용하려면 마스터의 인증이 반드시 필요합니다.

⚠ 네트워크를 사용하지 않고 독립적으로 설치된 단말기의 경우에는 최초등록자가 자동으로 마스터로 등록됩니다. 등록방법은 제3장의 사용자 등록을 참조하세요. 최초 사용자 등록과정 중 권한설정부분의 기본값이 마스터로 설정됩니다.

⚠ 네트워크를 사용하는 경우에 최초 등록자는 마스터 또는 일반사용자중 선택적으로 등록할 수 있습니다. 즉, 일반적인 사용자 등록 과정과 동일합니다.

메뉴를 보기 위해 메뉴버튼을 누르면 마스터 인증을 위해 다음과 같은 화면이 표시됩니다. 마스터의 ID를 입력하고 미리 지정

한 인증 방법(지문, 비밀번호, RF등)으로 인증한 후 메뉴를 볼 수 있습니다.



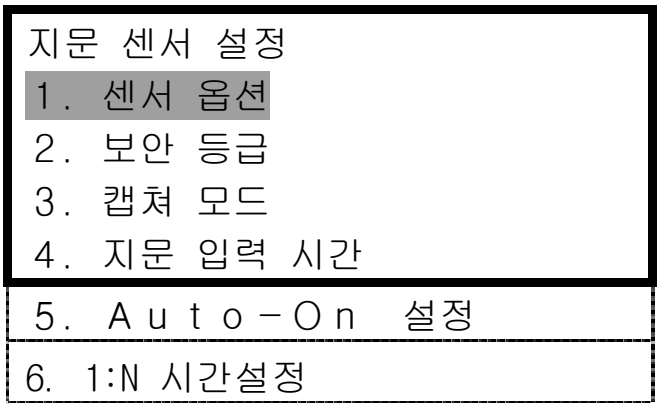
■ **결과 화면**

메뉴의 환경 설정이 성공적으로 끝나면 다음과 같은 화면이 표시되고 메뉴화면이 나타납니다.

만일 설정이 실패한 경우에는 다음과 같은 화면이 표시되고 초기화면으로 돌아갑니다. 아래 화면이 표시된 경우에는 현재 변경한 사항이 적용되지 않았음을 의미합니다.

2.2 지문 센서 설정

지문 입력 센서의 동작환경을 설정하는 메뉴입니다. 다음의 다섯 가지 하위메뉴가 있습니다. 방향 버튼(*,#)을 이용하여 이동한 다음 Enter버튼으로 선택합니다.

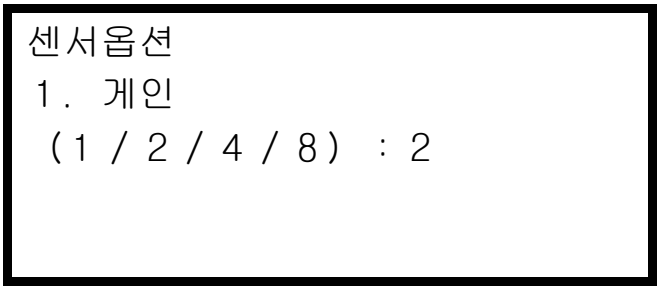


■ 센서 옵션

선명한 지문이미지를 얻기 위하여 센서의 옵션을 설정하는 메뉴입니다. 센서 옵션값은 CMOS이미지센서의 내부 설정값으로 게인, 밝기, 명암 3가지가 있습니다. 기본 설정값은 게인(2), 밝기(40), 명암(20)입니다.

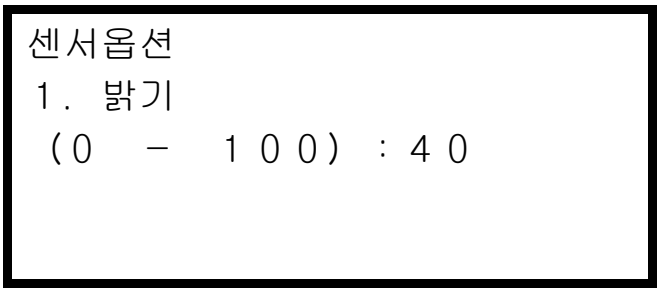
> ⚠ 이 설정값들은 센서성능에 매우 민감한 부분으로 지문인식 성능에 크게 영향을 미칠 수 있기 때문에 되도록 변경하지 않고 기본 설정값 사용을 권장합니다.

- 게인 (1 / 2 / 4 / 8)



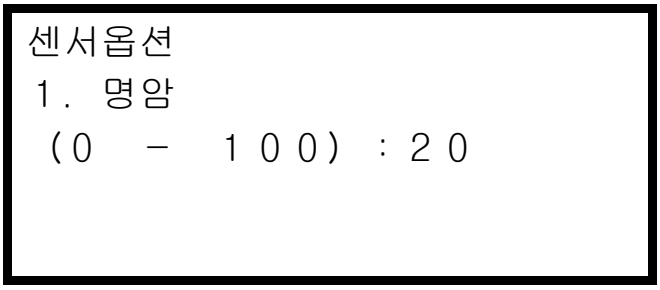
게인값 입력 후 Enter버튼을 누르면 밝기 값을 설정하는 화면이 나타납니다.

- 밝기 (0~100)



밝기값 입력 후 Enter버튼을 누르면 명암을 설정하는 화면이 표시됩니다

- 명암 (0~100)



⚠ 겨울철 등 사용환경이 매우 건조하여 건조지문에 대한 인식성능이 저하된 경우에는 밝기 값만을 20 ~ 30사이로 (권장값 : 20) 조정하여 주십시오.

⚠ 여름철 등 사용환경이 매우 습하여 습한 지문에 대한 인식성능이 저하된 경우에는 밝기 값만을 50 ~ 80사이로 (권장값 : 60) 조정하여 주십시오.

■ 보안 등급

지문인증을 하는 경우에 있어 보안 등급을 설정합니다. 1부터 9까지 중에서 선택하며 숫자가 클수록 보안성이 높음을 의미합니다. 『1:1모드』와 『1:N모드』로 구분하여 각각의 보안등급을 설정하며, 이는 시스템의 사용 효율성을 높이기 위한 것입니다. 일반적으로 『1:N모드』의 보안등급을 『1:1모드』의 보안등급보다 높게 설정합니다. 숫자키를 이용하여 원하는 보안등급값을 입력하고 Enter버튼을 눌러 설정을 종료합니다.

> ⚠ 고도의 보안성이 요구될 경우에 보안등급을 높게 설정하여야 하나, 이 경우 지문의 상태에 따라 본인거부율(본인임에도 불구하고 인증에 실패할 확률)이 증가할 수 있습니다. 반대로 보안등급을 낮게 설정하게 되면 타인수락율(정당한 권리가 없는 사람에 대해 인증을 허가할 확률)이 증가할 수 있으니 유의하십시오.

- 1:1모드

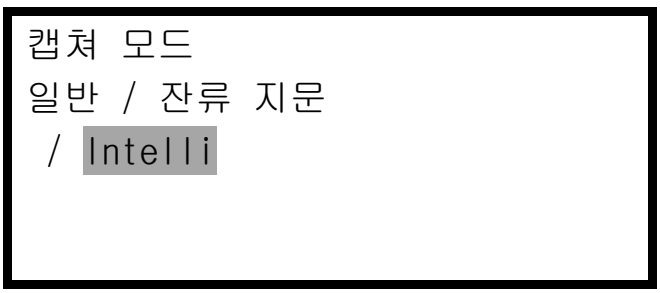
  사용자ID를 입력한 후 지문을 입력하여 인증하는 경우로서, 기본 설정값은 5입니다. 1:1모드의 경우 입력된 ID에 해당하는 등록지문과 입력된 지문을 1:1 비교하는 것이므로 1:N모드의 경우보다 보안등급을 다소 낮추어도 보안성의 저하는 없습니다.

- 1:N모드
  사용자ID를 입력하지 않고 지문만 입력하여 인증하는 경우로서, 1:1모드의 경우보다 보안등급을 다소 높게 설정하는 것이 바람직합니다. 기본 설정 값은 8입니다.

⚠ 1:N모드의 경우 유사지문이 나올 가능성이 존재하므로 보안등급을 너무 낮게 설정하면 타인수락율이 증가하여 보안성이 저하될 수 있는 반면에 너무 높게 설정하면 본인거부율이 증가하여 이용상 불편을 초래할 수 있으니 주의하십시오.

■ 캡쳐 모드

땀이나 피지 등에 의해 지문 입력 창에 남아 있는 잔류지문에 의한 오인식의 가능성을 방지하기 위한 기능 또는 건조한 지문에 대하여 인식성능을 높이기 위한 기능입니다. 초기 설정은 **『잔류 지문』**입니다. 방향 버튼을 이용하여 커서를 이동한 다음 Enter버튼으로 선택합니다.



⚠ 잔류지문 또는 Intelli 설정 기능을 사용할 경우 보안성은 향상되나 인증시간은 다소 길어질 수 있습니다. 높은 보안성이 요구되는 출입통제기로 사용할 경우에는 잔류지문 체크기능을 사용하는 것이 바람직하며, 보안성 보다는 편리성이 요구되는 근태관리 등으로 사용할 경우와 같이 필요에 따라 신속한 인증을 위해서는 사용하지 않는 것이 유리합니다.

■ 지문입력 시간설정 (1 ~ 30초)

단말기에 지문이 입력되어야 하는 시간을 설정합니다. 단말기에 설정된 시간 동안 LED가 점멸하면서 사용자의 지문입력을 기다리고, 설정된 시간이 경과하면 LED는 소등됩니다. 기본 값은 『5초』 입니다. 숫자키를 이용하여 원하는 시간을 입력하고 Enter 버튼을 눌러 설정을 종료합니다.

```
지문입력시간설정
 (1  -  30)  :  5
```

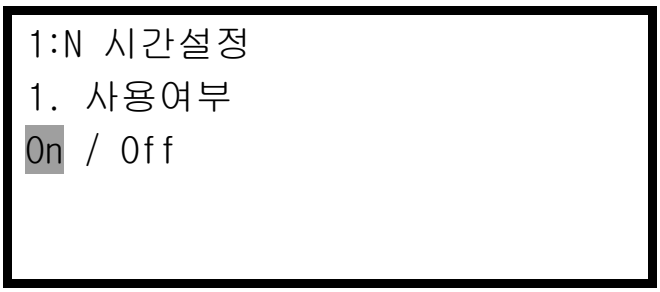
■ Auto-On 설정

이 기능은 지문입력 시에 Enter키를 누르지 않고 지문센서에 손가락을 데면 자동적으로 지문이 입력될 수 있도록 하는 기능입니다. 기본값은 『ON』 입니다.

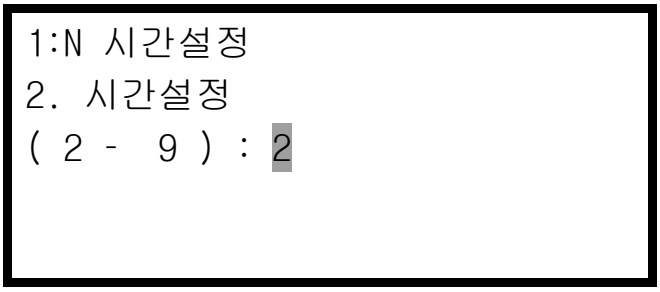
■ 1:N 시간설정

이 기능은 1:N 인증 시에 Timeout이 발생하는 시간을 설정하는 기능입니다. 1:N 인증의 경우, 설정 된 시간 이내에 결과가 나오지 않으면 실패 메시지가 표시됩니다.

만약 이 기능을 사용하지 않기를 원한다면 사용여부 창에서 Off를 선택하면 됩니다.



On을 사용하여 이 기능을 사용하면 원하는 Timeout 시간을 설정하여야 합니다. 기본값은 **『2초』**입니다.

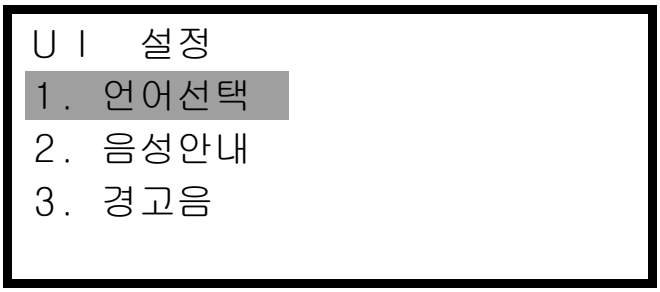


⚠ 사용자 수가 적을 경우에는 최소의 시간으로 설정하여도, 시간 내에 모든 인증이 끝날 수도 있습니다.

⚠ 사용여부에서 Off를 선택하면 시간설정 창이 나타나지 않습니다.

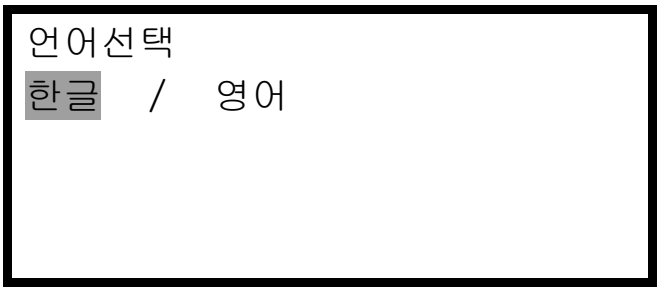
2.3 UI(User Interface) 설정

LCD화면과 음성안내, 경고음 등의 사용자 환경을 설정하는 메뉴입니다. 다음의 세가지 하위메뉴가 있습니다. 방향 버튼을 이용하여 이동한 다음 Enter버튼으로 선택합니다.



■ 언어선택

LCD창에 표시되는 언어를 한글과 영어 중에서 선택합니다. 방향 버튼을 이용하여 이동한 다음 Enter버튼으로 선택합니다.

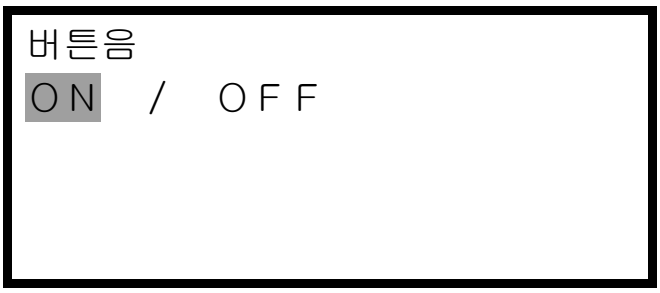


■ 음성안내

단말기에서 지문인증 시 음성으로 사용방법을 안내하는 기능입니다. 방향 버튼을 이용하여 이동한 다음 Enter버튼으로 선택합니다.

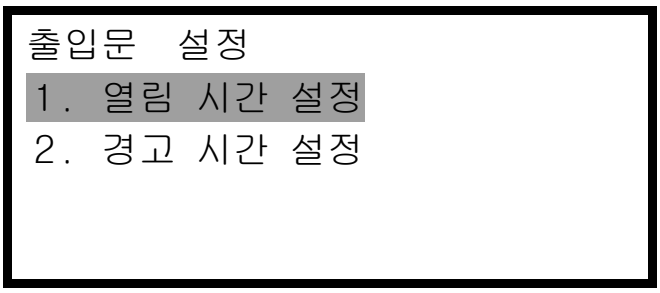
■ 버튼음

키패드의 버튼을 누를 때 소리가 나도록 하는 기능입니다. 방향 버튼을 이용하여 이동한 다음 Enter버튼으로 선택합니다.



2.4 출입문 설정

단말기에 의해 개폐되는 출입문의 동작을 설정하는 메뉴입니다. 방향 버튼을 이용하여 이동한 다음 Enter버튼으로 선택합니다.



■ 열림 시간 설정

사용자가 인증을 하고 출입문이 개방된 후 출입문이 열려 있는 시간을 지정합니다. 시간은 1초에서 20초 사이로 지정할 수 있습니다. 숫자키를 이용하여 원하는 시간을 입력하고 Enter 버튼을 눌러 설정을 종료합니다.

■ 경고 시간 설정

출입문이 설정한 시간을 초과하여 열려 있음을 경고음을 통해 알려주는 기능입니다. 경고음이 울리면 문이 닫히지 않는 원인을 확인하여 정상적으로 문이 닫힐 수 있도록 조치를 취하십시오. 1~20초 사이로 설정하되, **반드시 출입문 열림 시간 이상으로 설정되어야 합니다.** 숫자키를 이용하여 원하는 시간을 입력하고 Enter 버튼을 눌러 설정을 종료합니다.

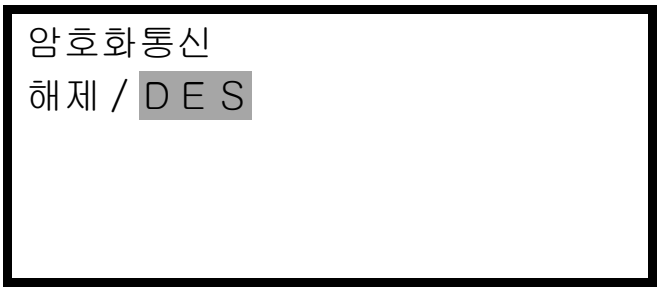
⚠ 이 기능은 출입문의 종류에 따라 지원되지 않을 수 있습니다.

2.5 시스템 설정

단말기의 시스템을 설정하는 메뉴입니다. 다음의 일곱 개의 하위메뉴를 가지고 있습니다. 다음의 메뉴를 보기 원할 때에는 방향버튼을 이용하여 화면을 아래로 이동시킨 후 Enter버튼을 눌러 선택합니다.

■ 암호화 통신

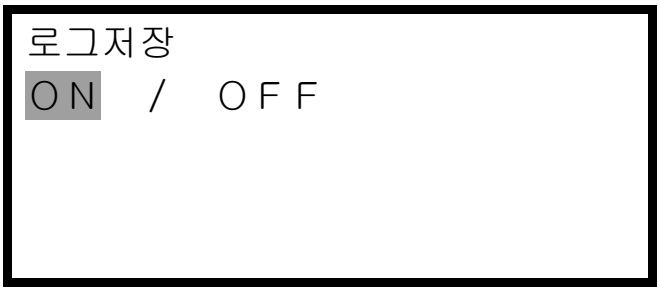
단말기의 네트워크 통신에 있어 송수신 되는 내용을 암호화 할 것인지에 대해 설정합니다. 방향 버튼을 이용하여 이동한 다음 Enter버튼으로 선택합니다.



⚠ 암호화를 사용할 경우 통신내용의 보안성이 강화되고 시스템의 안전성이 향상되는 반면에, 통신 데이터의 암호화 및 복호화에 따른 약간의 시간 지연이 있습니다.

■ 로그저장

사용자가 출입한 정보를 저장할 것인지에 대해 설정합니다. 네트워크에 연결되어 사용되는 경우에는 이벤트정보를 실시간으로 서버에 전송하며, 네트워크에 연결되지 않고 단말기 독립적으로 사용되는 경우에는 단말기 내에 저장됩니다. 방향 버튼을 이용하여 이동한 다음 Enter버튼으로 선택합니다.



⚠ 단말기에는 가장 최근 이벤트부터 최대 3,000개까지의 로그가 저장됩니다.

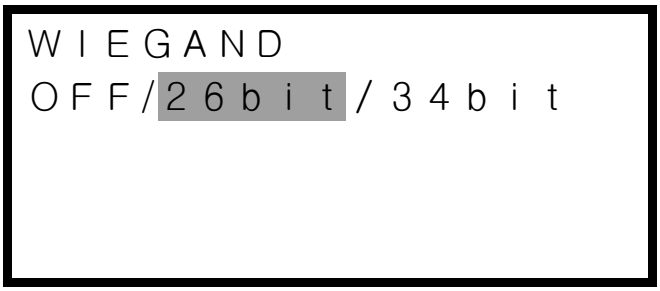
■ RF카드

사용자의 인증방법으로 RF카드를 사용할 것인지에 대해 설정합니다. 방향 버튼을 이용하여 이동한 다음 Enter버튼으로 선택합니다.

⚠ RF는 단말기 선택사양입니다. RF모듈이 포함되지 않은 단말기에서는 사용할 수 없습니다.

■ Wiegand

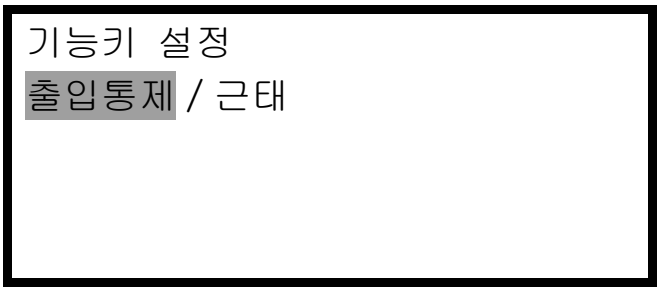
인증결과를 사용자 ID와 함께 서버로 전송하기 위한 Wiegand 통신 프로토콜 사용여부를 설정합니다.



⚠ Wiegand 통신은 사용자 ID가 4자리일 경우에만 지원이 가능합니다.

■ 기능키 설정

키 패드의 기능키(F1 ~ F4)의 기능을 출입통제기능과 근태관리 기능 중에 선택합니다. **『출입통제』**를 선택하면 기능키 중 F1은 그룹인증 시에 사용되며, **『근태』**를 선택하여 근태관리 기능으로 사용할 경우 F1~F4키를 출근, 퇴근, 외출 등 원하는 기능을 선택적으로 사용할 수 있습니다(반드시 근태관리 S/W 연동). 방향 버튼을 이용하여 이동한 다음 Enter버튼으로 선택합니다.



■ 단말기 모드

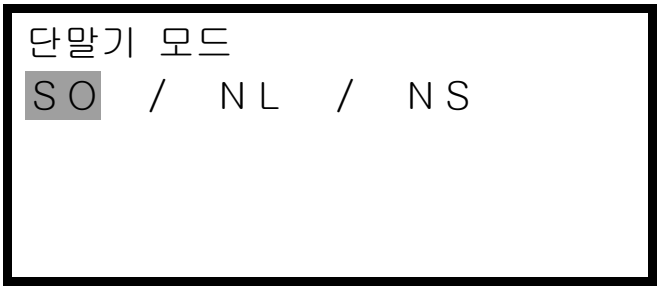
단말기는 다음의 세가지 모드로 사용할 수 있습니다. 방향 버튼

을 이용하여 이동한 다음 Enter버튼으로 선택합니다.

- SO (Stand Alone Only) :
  하나의 단말기를 독립적으로 사용하는 경우입니다. 사용자의 등록/삭제, 출입관리 등 모든 동작이 단말기에서만 이루어 집니다. 이벤트 로그에 대한 정보는 단말기 내에 저장됩니다.
- NL (단말기 인증) :
  사용자가 출입문에 인증 할 때 단말기 내에서 사용자 인증을 시도하고, 각종 로그 이벤트들은 단말기에 저장하지 않고 서버로 실시간 전송됩니다.

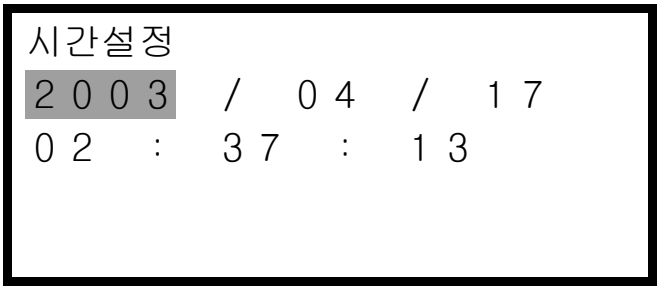
- NS (서버 인증) :
  사용자 인증 과정이 서버에서 이루어지는 모드입니다

위에서 설명한 인증모드를 참조하시어 원하는 모드를 선택하십시오



■ 시간설정

LCD창에 표시되는 현재 날짜와 시각을 설정해 줍니다. 숫자키를 이용하여 원하는 날짜와 시각을 입력합니다. 연도입력 후 Enter를 누르면 커서가 “월”로 이동하는 방식으로 순차적으로 (연→월→일→시→분→초) 입력할 수 있습니다. 단, 시간은 24시간을 기준으로 하여 입력합니다.



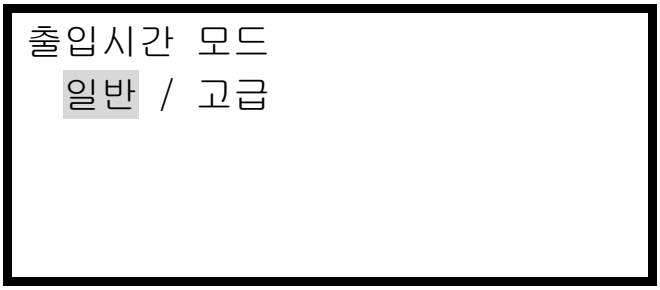
■출입시간 모드

출입시간을 제한하기위한 방법은 일반모드와 고급모드, 두 가지가 있습니다. 사용자는 두 가지 모드 중 하나를 선택해야 하며 본 메뉴에서 선택할 수 있습니다.

일반모드는 2.6 에 나와있는 것과 같이 출입통제기의 사용 시간대를 설정 함으로서 사용할 수 있습니다.

고급모드는 출입통제기 뿐 아니라 각 사용자별로 출입시간과 날짜를 제한할 수 있는 모드입니다.

일반모드의 세팅은 출입통제기에서 만 가능하며 고급메뉴의 세팅은 본 메뉴에서 고급으로 선택한 후, Access manager 소프트웨어를 통해서만 세부 세팅을 할 수 있습니다. 자세한 세팅 방법은 소프트웨어 매뉴얼을 참조하시기 바랍니다.



2.6 출입시간 설정

출입통제기의 사용 시간대를 설정해 주는 메뉴입니다. 여기서 설정한 출입시간을 이용하여 단말기를 제어하기 위해서는 2.5 출입시간 모드가 일반으로 선택되어 있어야 합니다.
출입시간 설정에는 다음의 세가지 하위메뉴가 있습니다.

```
출입시간 설정
1. 출입가능 요일
2. 출입가능 시작시각
3. 출입가능 종료시각
```

■ 출입가능 요일

일주일 가운데 단말기를 이용할 요일(들)을 지정합니다.
기본 설정은 모든 요일이 사용가능요일로 되어 있으며, 사용가능으로 설정된 요일 옆에는 『*』가 표시됩니다. 방향키를 이용하여 원하는 요일로 이동한 다음 Enter버튼을 눌러 설정합니다. 설정된 상태에서 Enter버튼을 누르면 설정이 해제됩니다. 설정이 해제된 요일에는 출입이 불가능하므로 유의하십시오.

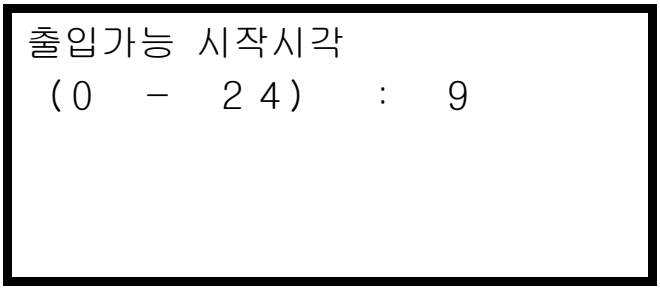
```
출입가능요일
월요일  *
화요일  *
수요일  *
목요일  *
```

```
출입가능요일
금요일  *
토요일  *
일요일  *
저장 후 나가기
```

출입가능요일을 선택 한 후 『**저장 후 나가기**』를 선택하여 설정을 종료합니다.

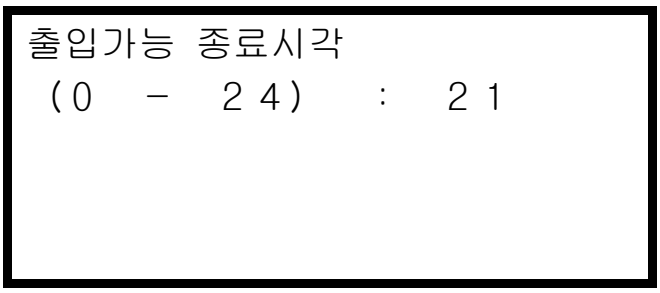
■ 출입가능 시작시각

하루 중에 단말기 이용 시간대의 시작 시각을 지정합니다.
예를 들어 오전 9시부터 오후 9시까지 사용하고자 한다면 아래와 같이 출입가능 시작시각과 출입가능 종료시각을 각각 설정합니다. 숫자키를 이용하여 원하는 시각을 입력하고 Enter 버튼을 눌러 설정을 종료합니다.



■ 출입가능 종료시각

하루 중에 단말기 이용 시간대의 종료 시각을 지정합니다. 숫자키를 이용하여 원하는 시각을 입력하고 Enter버튼을 눌러 설정을 종료합니다.



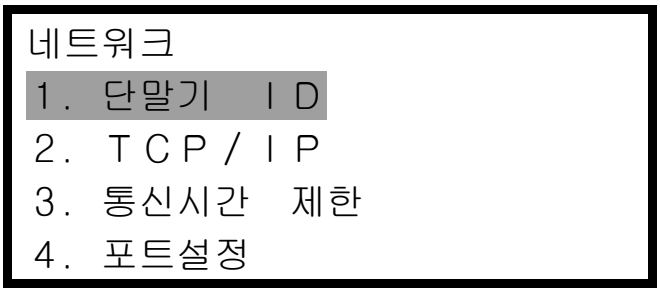
⚠ 출입가능 시간을 설정하여 출입을 제한하면 지정한 시간대 이외에는 출입이 불가능하므로 주의하십시오. 단, 단말기 마스터는 메뉴에서 설정값을 변경할 수 있는 권한이 있으므로 출입제한 시간을 변경하면 인증이 가능합니다.

⚠ 만일 이틀에 걸쳐 출입가능 시간을 설정하고자 할 경우, 예를 들어 당일 오후 1시부터 익일 오전 2시까지 사용하고자 한다면, 시작시각을 13, 종료시각을 2로 입력하시면 됩니다.

⚠ 단말기 설정을 통하여 출입시간 설정을 하고자 할 때에는 출입시간 모드가 일반으로 설정되어 있어야 한다.

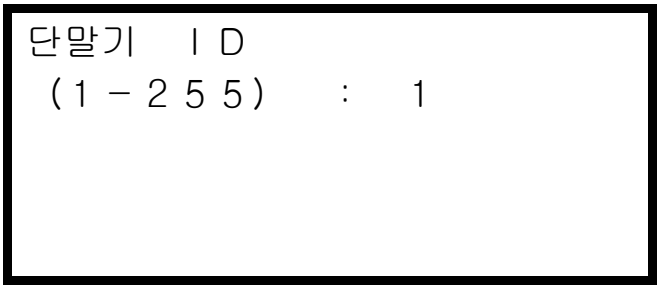
2.7 네트워크 설정

단말기의 네트워크 연결에 필요한 환경을 설정해 주는 메뉴입니다. 다음의 네 가지 하위 메뉴가 있습니다. 방향 버튼을 이용하여 이동한 다음 Enter버튼으로 선택합니다.



■ 단말기 ID

단말기의 고유한ID를 지정해 줍니다. 여러 개의 단말기가 네트워크를 통해 서버와 연결되는 경우를 고려해 관리자 프로그램에 설정된 단말기 ID와 일치하도록 설정되어야 합니다.



■ TCP/IP

단말기의 TCP/IP 네트워크를 설정합니다.

① DHCP

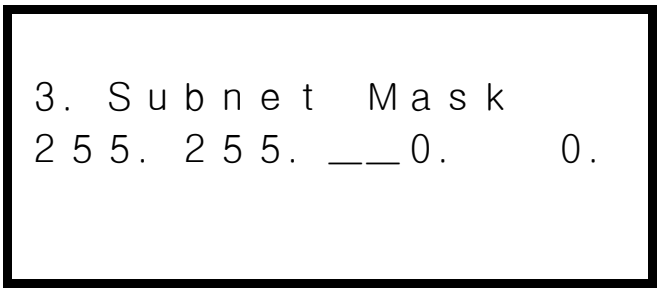
네트워크 설정에 있어 자동으로 주소를 할당하는 DHCP의 사용 여부를 선택합니다. 『ON』으로 DHCP 사용을 선택하면 ②, ③ 의 단계가 생략됩니다.

② 단말기의 IP

IP는 3자리 수 4개로 구성되는데, 숫자 3자리를 모두 입력하면 자동으로 다음 숫자를 차례로 입력할 수 있습니다. 2자리 숫자의 경우에는 Enter를 이용해 다음 숫자로 이동합니다.

③ Subnet Mask

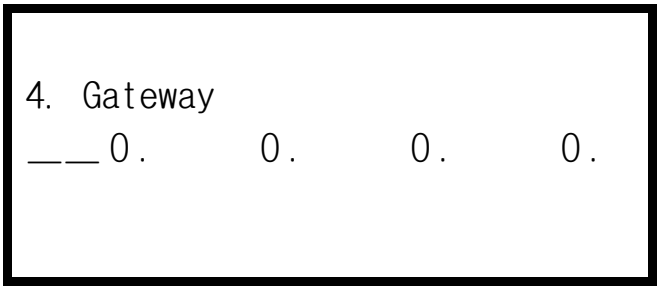
Subnet Mask 앞의 두 숫자는 255.255로 고정되어 있습니다. 숫자 입력방법은 위에서 설명한 단말기 IP입력방법과 동일합니다.



④ Gateway

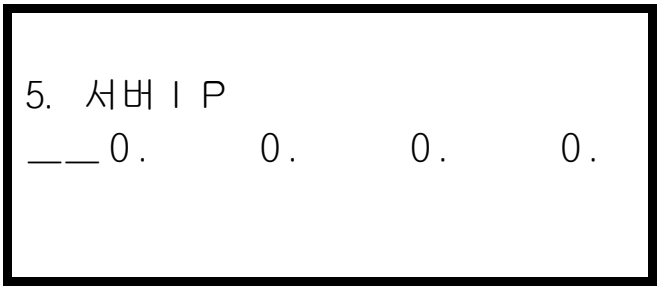
Gateway는 IP와 마찬가지로 3자리 수 4개로 구성되는데, 숫자 3자리를 모두 입력하면 자동으로 다음 숫자를 차례로 입력할

수 있습니다. 2자리 숫자의 경우에는 Enter를 이용해 다음 숫자로 이동합니다.



⑤ 서버의 IP

서버 IP를 입력합니다. 입력방법은 단말기 IP 입력 방법과 동일합니다.



⚠ Gateway 주소가 변경될 경우에는 단말기를 리셋합니다. 이는 단말기의 오류가 아니라, 네트워크의 원활한 재접속을 위한 것입니다.

■ 통신시간 제한

네트워크를 통해 서버와 단말기간 통신을 하는 경우에 설정된 제한시간 내에 응답이 없으면 네트워크가 연결되지 않은 것으로 처리합니다. 2 ~ 20초 범위에서 설정할 수 있으며, 네트워크 환

경이 좋지 않다면 기본값 10초에서 설정 값을 증가시키십시오.

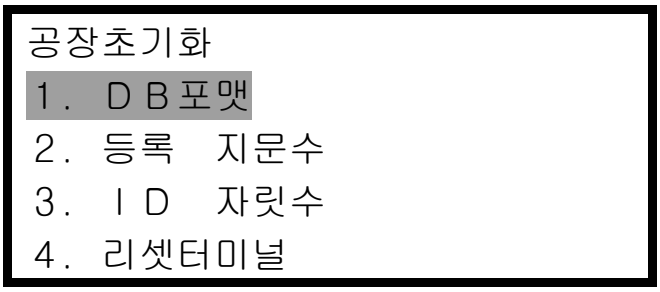
⚠ 통신시간 제한을 너무 짧게 설정하면 네트워킹에 너무 과도한 통신부하가 초래될 수 있으며, 너무 길게 설정하면 실시간 감시체계에 허점이 발생할 수 있으므로 설치상황을 고려하여 적절한 값으로 설정하여 주십시오.

■ 포트설정

네트워크를 통해 서버와 단말기와 통신을 하기 위한 통신포트번호를 설정합니다. 1~65535 사이에서 설정합니다.

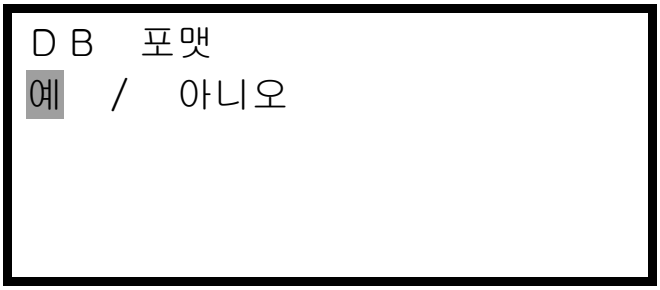
2.8 공장 초기화

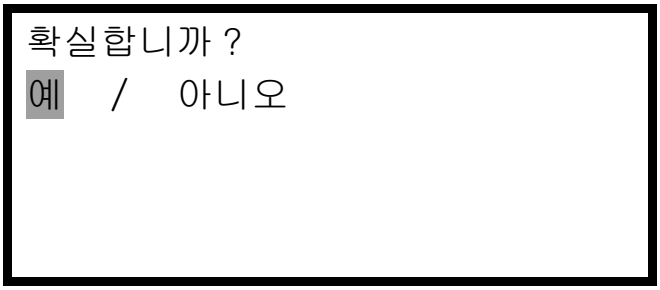
공장초기화 메뉴는 현재 사용중인 시스템의 환경을 초기화 하기 위한 것입니다. 하위 세가지 메뉴 중 **『등록 지문수』**와 **『ID 자릿수』**는 사용자가 1명이라도 등록되어 있는 경우에는 사용할 수 없으며, 사용 전에 반드시 모든 사용자를 삭제하시기 바랍니다.



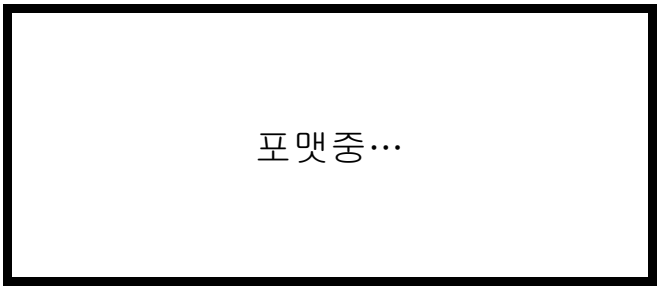
■ DB 포맷

단말기의 플래쉬메모리에 저장되어 있는 사용자정보와 로그정보가 기록되어 있는 메모리부분에 대한 포맷을 수행합니다. DB 포맷을 선택하면 다시 한번 포맷수행여부를 확인합니다.

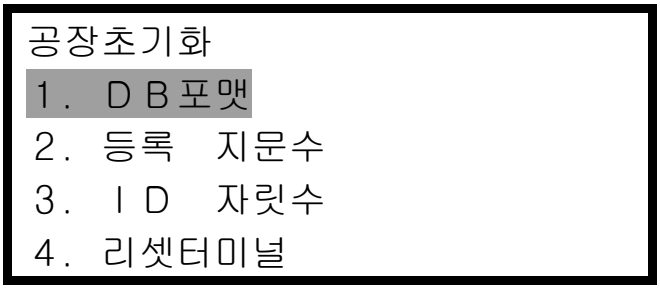




"예"를 선택하면 포맷을 수행하게 되며 아래와 같은 화면이 표시되며 포맷이 진행됩니다.

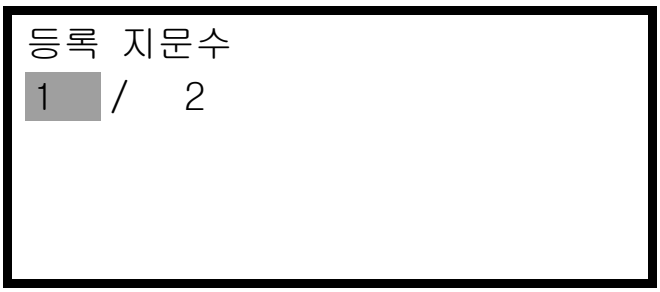


포맷이 완료되면 초기화면으로 돌아갑니다.



■ 등록 지문수

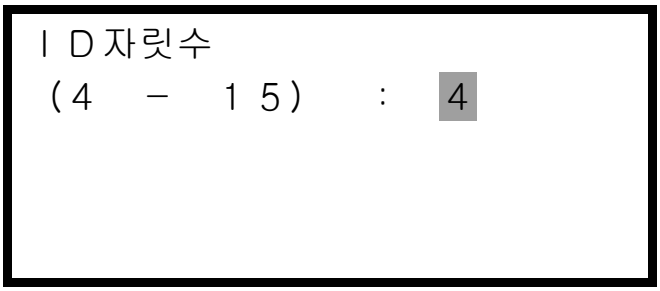
사용자 ID당 등록 가능한 지문 수를 변경합니다. 방향버튼을 이용하여 이동하고 Enter버튼을 이용하여 선택합니다.



⚠ 등록지문 수를 1로 하면 최대 4,000명까지 등록가능하며, 등록지문 수를 2로 설정하면 최대 2,000명까지 등록하여 사용할 수 있습니다.

■ ID 자리수

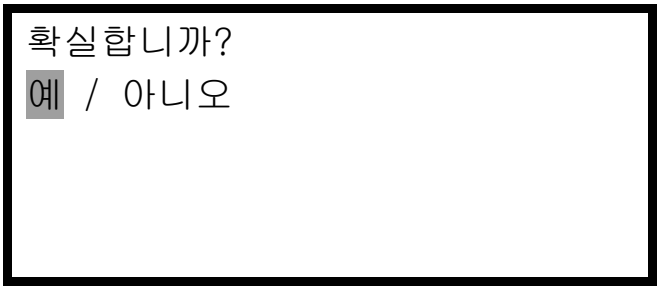
사용자 ID의 자리수를 설정할 수 있으며, 최소 4자리부터 최대 15자리까지 설정할 수 있습니다.



⚠ 사용자가 1명이라도 등록되어 있는 경우에는 ID 자릿수의 변경이 불가합니다.

■ 리셋 터미널

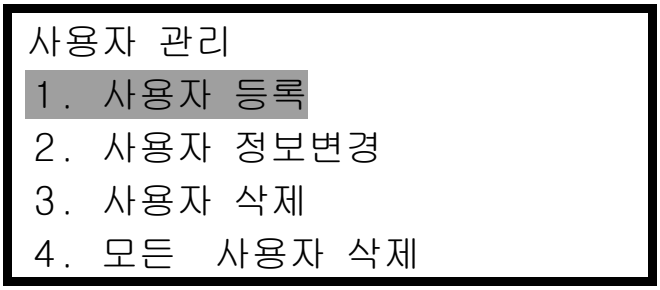
단말기를 해체하지 않고도 단말기를 리셋 시킬 수 있습니다.확인 창이 나타났을 때 **『예』**를 선택하면 단말기가 리셋 됩니다.



제3장
단말기 사용방법

3.1 사용자 관리

사용자의 정보가 저장되어 있는 DB를 관리하는 메뉴로서 마스터의 인증을 통해서만 접근할 수 있습니다. (제2장의 마스터 인증 참조) 사용자의 등록, 변경, 삭제 등의 네 가지 하위메뉴가 제공됩니다. 방향버튼으로 이동하고 Enter버튼을 선택합니다



⚠ 단말기 모드가 NL 또는 NS로 설정되어 있을 경우에는 사용자 관리 메뉴 중에 **『사용자 등록』**이외의 메뉴는 화면에 표시되지 않습니다. 사용자 등록 이외의 기능은 서버에서만 수행 가능합니다.

■ 사용자 등록

출입 통제기를 사용하고자 하는 사용자의 정보를 DB에 저장하기 위한 것으로 마스터 인증 후에 아래와 같은 절차에 의해 사용자를 등록합니다.

⚠ 사용자 등록은 단말기 모드가 SO일 경우에는 단말기에서 수행하며, NL 또는 NS모드로 설정되어 있을 경우에는 서버 또는 단말기에서 수행할 수 있습니다. 단, NL/NS모드에서 네트워크가 정상일 때에는 단말기 등록이 가능하나, 단선 되었을 시에는 단말기 등록이 불가능합니다.

⚠ SO모드로 사용중인 단말기를 NL 또는 NS로 변경하여 사용하고자 하는 경우에는 단말기의 사용자 DB를 모두 삭제하고 재등록하여 사용하셔야 합니다.

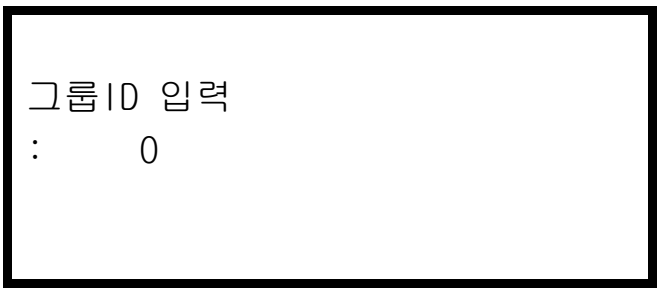
① 사용자ID 입력

사용자 등록메뉴를 선택하면 등록하고자 하는 사용자의 ID를 입력하는 화면이 나타납니다. 원하는 ID를 입력한 후 Enter버튼을 누릅니다. 동일한 ID가 이미 존재한다면 실패 메시지를 표시하고 이전 메뉴로 돌아갑니다.

⚠ 입력도중 ID를 수정하려면 cancel 버튼을 이용하십시오. 입력된 내용이 있으면 한자리씩 지워지며 입력된 내용이 없으면 상위메뉴로 돌아갑니다.

② 그룹ID 입력

ID입력이 완료되면 사용자가 소속되어 있는 그룹ID를 입력하기 위한 화면이 표시됩니다. 그룹ID 사용을 원하지 않을 경우에는 Enter버튼을 눌러 다음단계로 이동합니다. 그룹 ID는 4자리 이하로 입력하고, Enter버튼을 누릅니다.



⚠ 초기 환경설정에서 그룹ID를 선택하지 않은 경우에 그룹 ID입력단계는 생략됩니다.

⚠ 네트워크 모드에서 사용자를 등록할 때, 서버에 등록되지 않은 그룹으로 등록하면 등록 실패가 발생하니, 반드시 서버에 등록된 그룹ID만 사용하셔야 합니다.

③ 권한설정

다음은 사용자의 권한을 설정해줍니다. 사용자의 권한은 일반 사용자와 마스터 둘 중의 하나를 선택합니다. 방향 버튼을 이용하여 선택하고 Enter버튼을 눌러 설정합니다.

- 일반 사용자 : 단말기 관리 권한이 없으며 신분확인을 통한 출입 권한만 갖습니다.

- 마스터 : 단말기의 관리자로서 출입권한은 물론 사용자 DB관리와 환경 설정 등의 메뉴를 사용할 수 있는 권한을 가집니다.

④ 인증방법 선택

다음은 사용자의 인증방법을 선택하십시오. 지문, 비밀번호, RF카드, 다양한 혼합인증 방법 중에 선택합니다. 방향버튼을 이용하고 이동하고 Enter버튼을 눌러 선택합니다.

⚠ 만일 시스템설정에서 RF를 선택하지 않았다면 인증방법 중 RF가 포함된 인증방법은 화면에 표시되지 않습니다.

- **인증방법에 따른 사용법**

※범례 : FP(지문), PW(비밀번호), RF(RF카드), Enter(↵)
"/" (OR 조합), "&" (AND 조합)

구분	설 명
지문	지문만으로 인증을 수행합니다. ① ID + 지문 (1:1인증) ② 지문입력 (1:N인증)
비밀번호	비밀번호만으로 인증을 수행합니다. ① ID + ↵+ PW + ↵
RF	RF카드만으로 인증을 수행합니다.

	① RF
지문/비밀번호	지문 또는 비밀번호로 인증을 수행하며, 지문 인증을 우선적으로 수행합니다. 단, ID를 먼저 입력하고 지문인증에 실패하면 비밀번호인증을 시도하나, ID입력 없이 지문인증에 실패하면 비밀번호 인증 없이 인증실패 처리됩니다. ① ID + FP (FP 실패 시 PW +↵) ② FP (FP 실패 시 인증실패)
지문/RF	지문 또는 RF카드로 인증을 수행하며, 지문 인증을 우선적으로 수행합니다. 단, ID를 먼저 입력하고 지문인증에 실패하면 RF카드인증을 시도하나, ID입력 없이 지문인증에 실패하면 RF카드 인증 없이 인증실패 처리됩니다. ① ID + FP (FP 실패 시 RF) ② FP (FP 실패 시 인증실패) ③ RF
비밀번호/RF	비밀번호 또는 RF카드로 인증을 수행합니다. ① RF ② ID + ↵+ PW + ↵(PW 인증실패 시 RF)
지문&비밀번호	지문과 비밀번호로 모두 인증 시도하며, 두 가지 모두 인증에 성공해야 합니다. 단, 반드시 ID를 먼저 입력하고 지문을 입력해야 합니다. ① FP + PW + ↵ ② ID + FP + PW + ↵

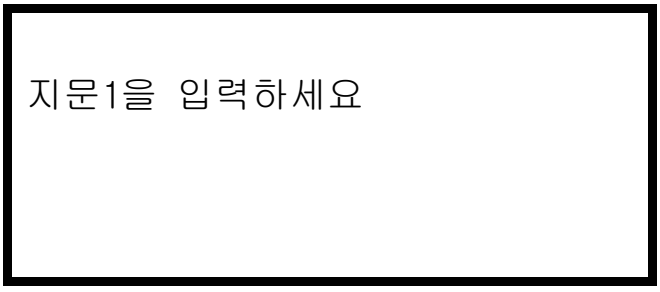
지문&RF	지문과 RF카드로 모두 인증에 성공해야 최종 인증에 성공하는 방법입니다. 아래와 같이 세 가지 방법이 있습니다. ① RF + FP ② FP(1:N인증) + RF ③ ID + FP + RF
비밀번호&RF	비밀번호와 RF카드 모두 인증에 성공해야 최종 인증에 성공하는 방법입니다. ① RF + PW + ↵ ② ID + ↵+ PW + ↵+ RF
지문&비밀번호 &RF	지문, 비밀번호, RF카드 모두 인증에 성공해야 최종 인증에 성공하는 방법입니다. ① FP + PW + ↵+ RF ② ID + FP + PW + ↵+ RF ③ RF + ↵+ FP + PW + ↵

위 표의 인증방법 중에서 지문인증을 시도하는 경우에 단축ID 인증 및 그룹ID인증(제1장 1.6 인증방법 참조)도 가능합니다.

⑤ 지문입력

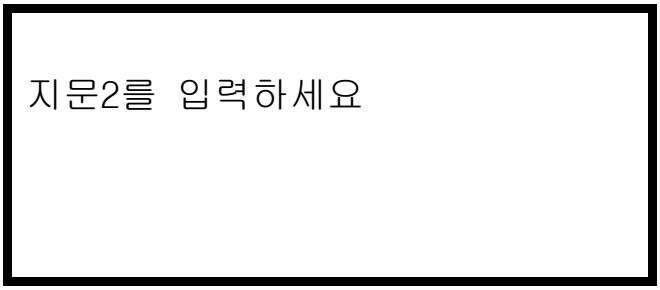
인증방법에서 지문이나 지문이 포함된 인증방법을 선택한 경우에 사용자의 지문을 입력합니다. 지문입력은 총 2회에 걸쳐서 이루어지며 한번 입력 후 손가락을 떼었다가 재차 입력합니다.

지문을 입력합니다.



지문을 입력한 후 아래 화면이 표시되면 지문입력창에서 손가락을 떼십시오

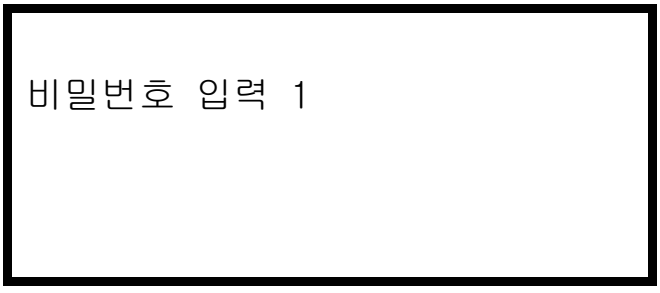
입력했던 지문을 다시 입력합니다.



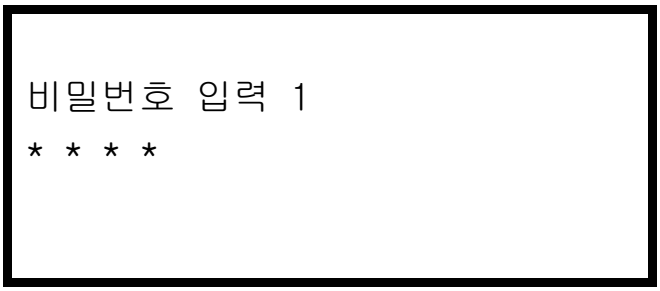
지문입력이 성공적으로 끝나면 성공 메시지가 나타나고 실패했을 경우엔 실패 메시지가 나타나며 최초 등록화면으로 돌아갑니다.

⑥ 비밀번호 입력

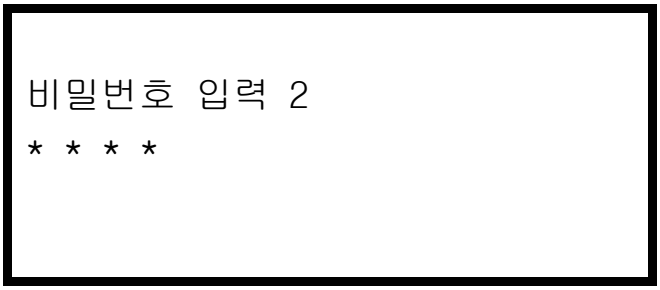
인증방법 중에서 비밀번호 인증이나 비밀번호 인증이 포함된 인증방법을 선택한 경우에 사용자의 비밀번호를 입력합니다. 비밀번호는 4 ~ 8 자리를 사용할 수 있습니다.



비밀번호는 입력 받을 때 보안을 위하여 다음과 같이 『*』표시로 보여집니다.



입력된 비밀번호가 맞는지 다시 한번 확인합니다.



비밀번호 입력이 성공적으로 끝나면 성공 메시지가 나타나고 실패했을 경우엔 실패 메시지가 나타나며 최초 등록화면으로 돌아갑니다

⑦ RF카드 입력

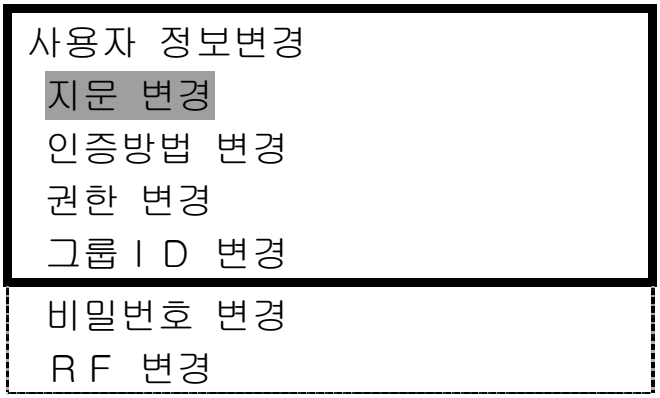
시스템 설정에서 RF카드를 설정했다면, RF카드를 이용하여 사용자를 등록합니다. 지문입력 센서 근처에 사용자의 RF카드를 접근시키십시오. 만일 단말기 환경설정에서 RF옵션을 설정 하지 않았다면 Enter버튼을 눌러 다음 단계로 넘어갑니다.

RF카드입력이 성공적으로 끝나면 성공 메시지가 나타나고 실패했을 경우엔 실패 메시지가 나타나며 최초 등록화면으로 돌아갑니다

■ 사용자 정보변경

등록된 사용자의 정보를 변경하기 위한 것으로, 지문, 비밀번호, 그룹ID, RF카드, 인증방법, 권한을 변경할 수 있습니다. **『사용자 정보변경』**을 선택하면 변경하고자 하는 사용자의 ID를 입력하는 화면이 표시됩니다.

ID를 입력하고 Enter를 누르면 아래와 같이 변경 가능한 항목들이 표시됩니다. 방향 버튼을 이용하여 이동한 다음 Enter버튼으로 선택합니다.

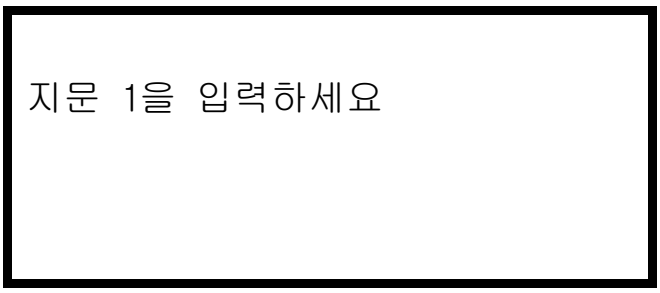


- **지문 변경**

  등록된 개별 사용자의 등록 지문을 변경하기 위한 메뉴입니다.

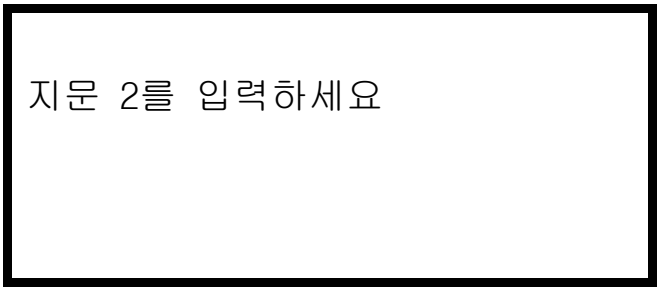
지문을 등록할 때와 마찬가지로 지문을 2회 입력하며 두 번째 입력은 반드시 손가락을 떼었다가 다시 입력하십시오.

지문을 입력합니다.



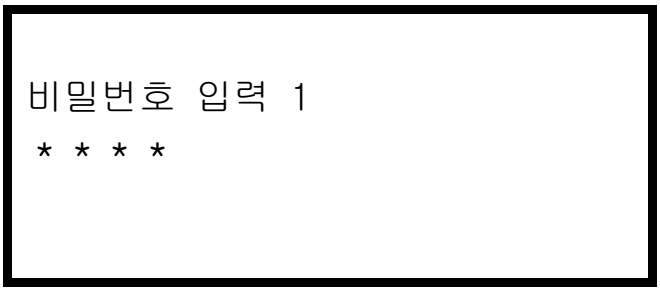
지문을 입력한 후 아래 화면이 표시되면 지문 입력창에서 손가락을 떼십시오

입력했던 지문을 다시 입력합니다.

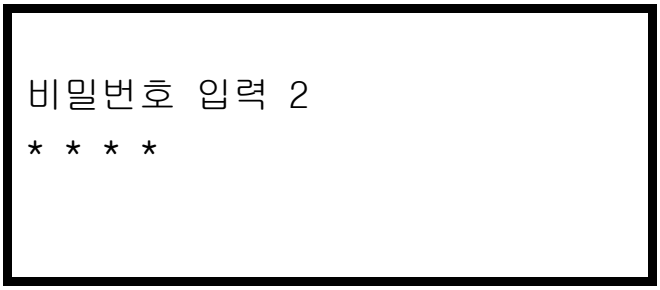


- **비밀번호 변경**
  등록된 개별 사용자의 비밀번호를 변경합니다.

새로운 비밀번호를 입력합니다.

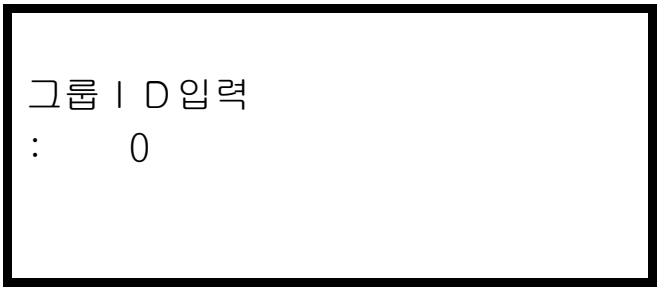


입력된 비밀번호가 맞는지 다시 한번 확인합니다.



- **그룹ID 변경**
  사용자가 소속된 그룹의 ID를 변경합니다.

  새로운 그룹 ID를 입력합니다. 만일 그룹ID 사용을 해제하고자 하는 경우에는 Enter버튼을 누르십시오



- **RF카드변경**
  등록된 개별 사용자의 RF카드를 변경합니다.

- **인증 방법 변경**
  등록된 개별 사용자의 인증 방법을 변경합니다.

  변경하고자 하는 인증 방법을 선택합니다.

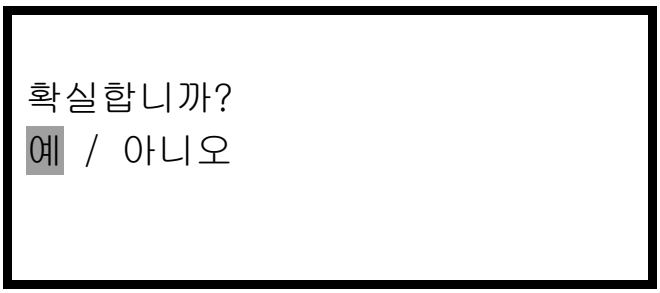
- **권한 변경**
  등록된 개별 사용자의 권한을 변경합니다.

  일반사용자와 마스터 중에서 선택합니다.

■ **사용자 삭제**

삭제 하고자 하는 사용자의 ID를 입력합니다.

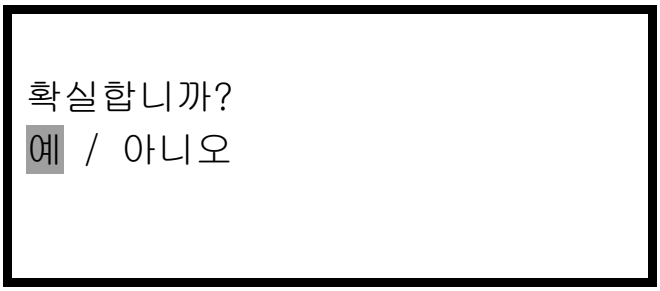
사용자 삭제를 한 번 더 확인 합니다. 예/아니오 중 선택하신 후 Enter버튼을 누르십시오.



■ **모든 사용자 삭제**

단말기에 등록되어 있는 모든 사용자를 삭제합니다.

『예/아니오』 중 선택한 후 Enter버튼을 누르십시오.

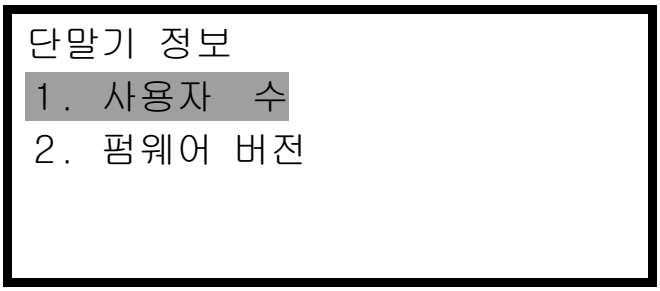


⚠ 단말기에 등록되어 있는 모든 사용자가 삭제되므로 주의하십시오.

모든 사용자를 삭제하기 위해 『예』를 선택하면 삭제가 진행됩니다.

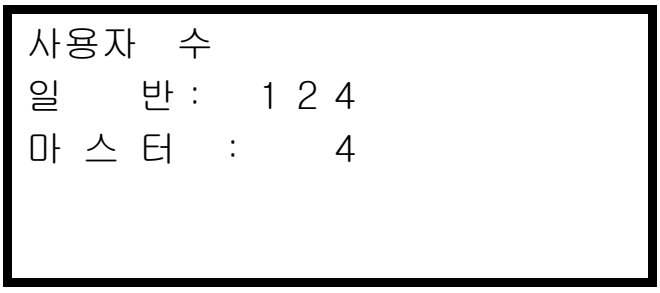
3.2 단말기 정보 확인

단말기의 정보를 확인할 수 있습니다.



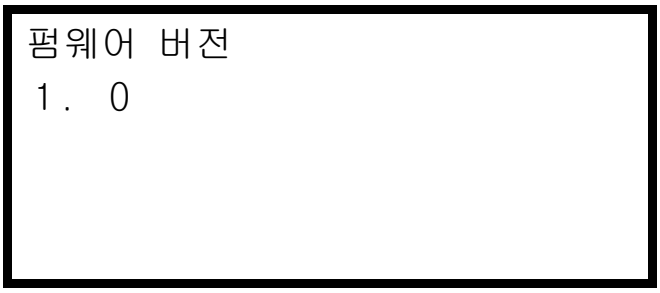
■ 사용자 수

현재 단말기에 등록되어 있는 사용자의 수를 알려줍니다. 일반 사용자와 마스터를 구분해서 나타냅니다.



■ 버전 확인

단말기의 펌웨어 버전을 알려줍니다.



Appendix

Appendix I
네트워크 연결 오류 및 대응방법

단말기가 네트워크에 연결되지 않을 경우 아래 내용을 참조하십시오.

서버에 단말기가 등록되어 있지 않은 경우
서버에서 단말기를 등록합니다.

```
0 0 1
관리자에 문의
미등록 단말기
```

단말기 ID가 유효하지 않은 경우
단말기 ID를 확인한 후 유효한 ID (1~255)로 재설정 하십시오.

```
0 0 2
관리자에 문의
단말기 ID 오류
```

서버와 단말기에 설정된 사용자ID의 자릿수가 다른 경우
서버와 단말기의 사용자 ID 자릿수를 동일하게 설정하십시오.

```
0 0 3
관리자에 문의
ID 자릿수 오류
```

서버와 단말기에 설정된 사용자 등록 지문수가 다른 경우
서버와 단말기의 등록 지문수를 동일하게 설정하십시오.

```
００４
관리자에 문의
등록 지문수 오류
```

단말기 ID가 충돌하는 경우
단말기 ID를 등록되어 있지 않은 ID로 변경하십시오.

```
００５
관리자에 문의
단말기 ID 충돌
```

MAC Address가 일치하지 않는 경우
고객지원센터로 연락하여 주십시오.(☎ 080-060-1600)

```
００６
관리자에 문의
ＭＡＣ  Ａｄｄｒ  오류
```

Firmware Version이 현재 사용중인 Access manager 소프트웨어와 맞지 않는 경우, 현재 사용중인 소프트웨어 버전에 맞는 적당한 Firmware로 Upgrade해 주십시오.
Access manager 1.1* 버전과 Firmware applrom_1.1** 의 기준으로, Access manager와 Firmware의 소수점 이하 첫번째 자리까지 버전이 서로 다른 경우에는 단말기가 정상적으로 동작되지 않는

상황이 발생될 수 있으므로 ㈜니트젠의 고객지원센터(☏ 3415-1600)로 문의하여 주시기 바랍니다.

```
0 07
관리자에 문의
F W  V e r  오류
```

Appendix II
단말기 초기화 오류 및 대응방법

단말기에 전원이 인가된 후 초기화 과정에서 발생할 수 있는 오류와 그에 따른 대처방법 입니다.

Err. Code	내용	대응방법
001	미확인 오류	재부팅 또는 A/S
002	FPGA 초기화 실패	재부팅 또는 A/S
003	LCD 초기화 실패	LCD module 연결확인 또는 A/S
004	RTC 초기화 실패	A/S
005	Optic module 오류	Optic module 연결확인 또는 A/S
010	시스템 소프트웨어 오류	A/S
011		A/S
012		A/S
013		A/S
014		A/S
015		재부팅
016		A/S

※ Error code 001부터 003까지는 LCD가 초기화 되기 이전이므로 LCD 화면에 표시되지 않으며, 부저음으로 Error code를 확인할 수 있습니다. 001은 부저음이 5초간격으로 1회 울리고, 002는 2회, 003은 3회의 부저음이 울립니다.

Appendix III
음성안내 볼륨 조절 및 외부스피커 연결

기본적으로 현재 출력되는 단말기의 볼륨은 가장 적절한 값으로 조절되어 있습니다. 그러나, 주변 환경이 시끄러워 잘 들리지 않는 곳에서는 단말기에 점퍼를 연결하면 볼륨을 일부 키울 수 있습니다.

또한 현재 단말기에 내장되어 있는 스피커의 용량을 넘어서는 아주 큰 소리를 원하는 경우라면, 외부스피커 단자에 앰프가 내장된 스피커를 연결하면 큰 소리로 출력할 수 있습니다.

A. 볼륨 업 기능

단말기 뒤편에 존재하는 JP6에 점퍼를 연결하면 단말기 음성안내의 볼륨을 키울 수 있다.

※ 이것은 특별히 큰 소리를 요하는 상황을 위한 것으로, 볼륨을 키우면 스피커 크기의 한계로 인하여 약간의 음질 저하가 발생할 수 있습니다.

B. 외부스피커 연결

단말기 뒤편에 존재하는 J4 커넥터에 모노 스피커를 연결하여 음성안내를 스피커를 이용하여 들을 수 있습니다. 큰 소리를 출력하기 위해서는 앰프가 내장된 스피커가 좋습니다.

J4 커넥터의 핀에 대한 정의는 다음과 같습니다.

1번 Pin : GND
2번 Pin : OUTPUT

Appendix IV
직사광선에 의한 인식율 저하 개선방법

1) 지문 인증 시 직사광선을 차단해야 하는 이유

지문인식기는 사진기와 마찬가지로 Image를 Capture 하는데, 많은 양의 빛이 들어올 경우 Image가 어둡게 되어 정도에 따라 Image를 인지할 수 없게 된다.

사진기와는 달리 센서에는 셔터나 조리개가 없으므로 따라서 인위적으로라도 직사광선을 차단해야 한다.

2) 설치장소의 선택

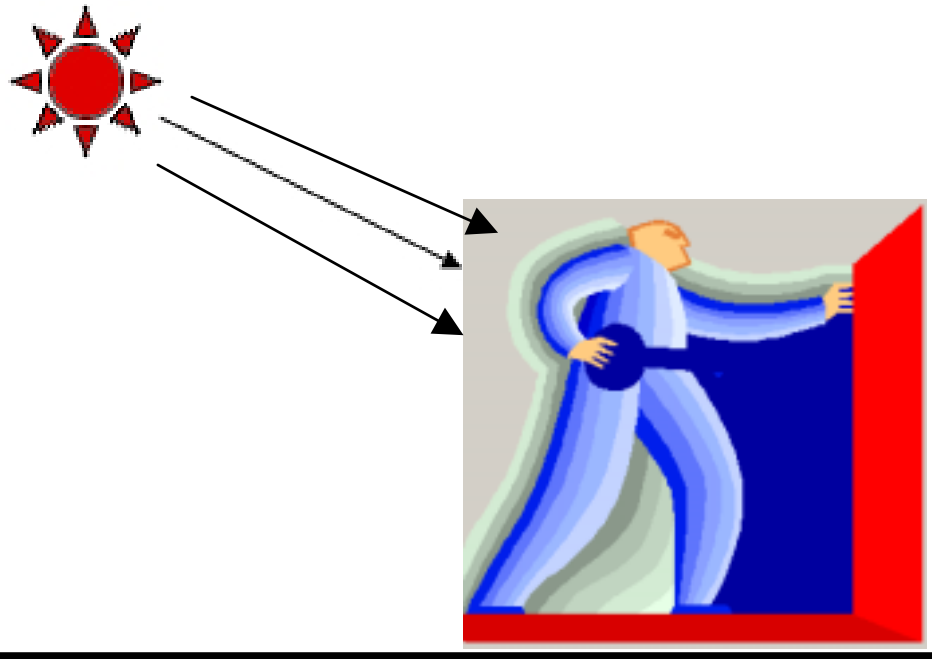
당사의 제품은 모두 직사광선에 영향을 받을 수 있는 광학식 제품이므로 다음과 같은 위치는 피하여 설치할 것.

① 직사광선이 들어올 수 있는 창문가
② 차양막 등이 없는 옥외 장소
③ 지면으로부터 수직으로 1700㎜ 이상의 높이 위치

3) 직사광선을 피할 수 없는 곳에 설치된 경우 인증율을 높이는 방법

① 태양을 등지고 선다

(그림과 같이 몸을 이용하여 직사광선을 가림)



② 인증을 시도하지 않는 손으로 센서 부위를 감싸듯 가린다.
③ 설치 높이를 우리나라 성인 남자의 평균키 높이인 1700㎜ 보다 낮게 한다.
④ 인증 시 양산 등 햇빛을 차단할 수 있는 보조 도구를 이용한다.

Appendix Ⅴ
FAQ (Frequently Asked Question)

지문으로 인증이 되지 않는데, 어떻게 해야 합니까?

1. 날씨가 추워지거나 손을 씻고 난 직후에는 지문상태가 건조되기 쉽습니다. 또한 흙먼지 등으로 손이 오염된 경우에도 건조한 지문이 됩니다. 이러한 경우에는 보습제 등을 이용하여 지문을 Normal 한 상태로 만들어 주신 후 지문 인증을 시도해 주십시오.

2. 손에 땀이 많거나 물이 묻은 경우 또는 겨울철 주머니에 손을 넣고 보행한 직후에는 지문이 습할 수 있습니다. 이 경우 지문 인증이 잘 되지 않으면 손의 습기를 제거 후 인증 시도 바랍니다.

3. 지문 인증이 잘 되지않는 경우에는 ID를 입력하지 않고 인증을 시도하는 Identification 보다는 ID를 입력하여 본인의 원본 지문과 1:1로 비교하는 Verification 인증 방법을 시도하는 것이 바람직합니다. 또한 NAC-3000 은 SID 기능을 지원하여 ID의 앞자리 숫자만 누르고 인증을 시도하는 방법도 있는데, 이것도 Identification 인증 방법보다는 지문 인증율을 높일 수 있습니다.

4. 지문의 상태가 상처 등으로 인하여 저장된 원본과 다르게 변형될 경우를 대비하여 비밀번호나 RF 카드를 보조 인증 도구로 활용하시는 방법도 있습니다.

5. 네트워크 인증모드 중에서 서버 인증 모드(NS모드)로 사용하는 경우에 서버를 개인용 PC 또는 업무용 PC로 이용하시면 인증 작업이외에 다른 작업으로 인하여 서버PC에 부하량이 증가할 경우 인증율이 떨어질 수 있습니다. NAC-3000 전용 서버를 구축하여

이용하시지 않는 경우에는 가급적 단말기 인증 모드(NL모드)로 사용하시기 바랍니다.

Auto-on 기능이 되지 않거나 오동작 합니다.

1. 지문 입력창에 손을 대어도 동작되지 않는 경우
   우선 Auto-on 기능이 'OFF' 되어있는지 확인하시고, 설정된 값을 'ON' 상태로 맞춰주십시오. 설정값을 변경한 후에도 동작되지 않을 경우는 ㈜니트젠 고객지원센터로 연락하여 주시기 바랍니다.
   ㈜니트젠 고객지원센터(080-060-1600, customer@nitgen.com)

2. 손을 대지않아도 연속적으로 동작되는 경우
   사용 중 지문인식기의 LED가 반복해서 깜박거리거나 단말기 전원을 리셋하면 지문인식기의 LED가 일정시간 깜박거리다가 Auto-on 기능이 되지않는 현상이 발생되면 ㈜니트젠 고객지원센터로 연락하여 주시기 바랍니다.

3. RF 카드를 갖다 대면 오동작하는 경우
   NAC-3000R 제품의 경우 RF 카드로 인증하기 위하여 단말기에 RF 카드를 갖다 대면 Auto-on Sensor가 동작할 수 있는데, 주로 구형 버전의 제품에서 발생됩니다. 이 같은 경우에도 ㈜니트젠 고객지원센터로 연락하여 주시기 바랍니다.

RF 카드로 인증할 수 없습니다.

우선 RF 카드 기능이 'OFF' 되어있는지 확인하시고, 설정된 값을 'ON' 상태로 맞춰주십시오. 설정값을 변경한 후에도 동작되지 않을 경우는 ㈜니트젠 고객지원센터로 연락하여 주시기 바랍니다.

Firmware를 업그레이드 하려면 ?

Access Manager 프로그램을 이용하여 ㈜니트젠에서 제공하는

Firmware(binary file)를 서버에서 단말기로 다운로드 하면 됩니다.
(TCP/IP 통신 이용)

단말기에서 “웅 ~” 하는 소음이 납니다.

NAC-3000과 연결될 수 있는 인터폰의 종류에 따라서 하울링(Howling)이 심하게 발생되는 경우가 있습니다. 이 경우에는 NAC-3000과 호환성이 검증된 코콤(Kocom)제 인터폰(DP-202H)을 적용하시면 하울링을 없앨 수 있습니다.

정전기 방지 대책이 있는지요 ?

NAC-3000 제품은 ESD(Electro Static Discharge)와 관련하여 CE 인증을 획득하였고, 회사 내부 QA인증시험을 통하여 IEC 61000-4-2 규격의 Level 3 (Contact : 6㎸, Air : 8㎸)에 만족함을 보증하고 있습니다.
다만, 겨울철이나 습도가 낮은 지역이면서 카페트 등이 깔려져 있는 사용 환경에 설치될 경우 사람에게 대전될 수 있는 정전기가 35㎸ 정도이므로 이런 환경에 설치 시에는 별도의 사용자 주의를 요망합니다.

외부 침입자에 의한 강제 파손이 되면 어찌하나요 ?

NAC-3000 제품은 설치 방법에 따라 일반형과 매립형으로 나눌 수 있는데 매립형의 경우 벽 속에 함몰되어 있어 우발적인 제품 파손은 피할 수 있고 일반형의 경우에도 특수 금속 브라켓으로 제품을 보호하여 쉽게 파손할 수 없는 구조입니다. 다만, 어떠한 방법을 동원해서라도 강제로 제품을 부수거나 해체할 경우에는 이를 대비하여 Tamper Switch가 동작하여 경보장치가 울리도록 되어 있습니다.

기종별	사용자 안내문
B급 기기 (가정용 통신기기)	이 기기는 가정용으로 전자파적합등록을 한 기기로서 주거지역에서는 물론 모든 지역에서 사용할 수 있습니다.