

BioAdmin 사용 설명서

Version 4.3

(주)슈프리마의 BioAdmin, BioEntry, BioStation, BEACon은 (주)슈프리마의 상표로 등록되어 있으며 모든 권리는 (주)슈프리마에 있습니다. 이에 관하여 저작권이 미치는 제품의 모든 부분은 (주)슈프리마의 서면 승인 없이는 어떠한 형태나 수단(그래픽이나 사진복사, 녹음, 비디오녹화 또는 정보 검색 방식을 포함하는 전자적, 기계적인 수단)에 의해 재생산 또는 복제될 수 없습니다. 라이선스를 획득하여 제공되는 소프트웨어는 이러한 라이선스에 의거한 범위에서만 사용되거나 복제될 수 있습니다.

(주)슈프리마는 공지 없이 이 문서의 부분 또는 전부를 수정하거나 개정할 수 있는 권리를 보유하고 있으며, 이들 자료에 의거하여 발생된 간접 손실을 포함한 손실, 비용 또는 손상에 대하여 책임지지 않습니다.



슈프리마의 보증정책

슈프리마는 구매자에게, 아래 설명된 범위에서 제품이 배송된 날짜로부터 1년 간의 “보증기간” 동안, 이 제품이 공시된 설명서에 따라 제품의 성능을 보증합니다. 만약 구매자가 보증서에 의해 보장된 결함을 보증 기간 안에 서면으로 슈프리마에 통지할 경우, 슈프리마는 임의로 구매자가 미리 지불한 보증기간, 운송료와 보험 한도에서 반송된 불량품을 수리하거나 교환해 줄 것입니다. 이러한 수리나 교환은 제품과 관련한 보증 위반에 대한 슈프리마의 구제책입니다. 이 제한된 보증은 다음과 같은 경우의 제품에 대해서는 보장되지 않습니다:(i) 이례적인 물리적 또는 전기적 압력, 잘못된 사용, 부주의, 사고 또는 다른 외부적 요인들에 의해 손상된 경우;(ii) 공급자에 의해 서면으로 승인되지 않은 부적절한 수리, 개조 또는 변경된 경우;(iii) 슈프리마가 제공한 안내서 내용을 위반하여 부적절하게 설치하거나 사용한 경우

슈프리마는 결함들이 나타난 후 30일까지 그리고 제품들이 배송된 날로부터 최근 1년까지 슈프리마가 제공하는 RMA(Return Material Authorization 반품 자료 인증) 보고서에 이러한 결함들을 서면으로 공지할 것입니다. 이 보고서에는 각 불량 제품, 모델 번호, 송장 번호와 일련 번호에 대한 상세한 설명이 있어야 합니다. 슈프리마에 의해 발행된 RMA 번호가 없는 어떠한 제품도 인정되지 않으며 모든 결함은 보증 서비스를 위해 재현되어야 합니다.

여기에 명백히 규정된 것을 제외하고는 특정 목적을 위한 보증성, 상업성 또는 적합성 등에 관련해서는, 명시적 묵시적이든 어떤 종류의 보증 없이 제품은 있는 그대로 제공됩니다.

경고문

이 문서에 있는 정보는 슈프리마 제품과 관련하여 제공됩니다. 지적재산권에 대한 어떠한 라이선스도 이 문서에 의해 부여되지 않습니다. 제품 판매에 관하여 슈프리마와의 교섭과 조건에 따라 제공되는 경우는 예외로 합니다.

슈프리마는, 특정 목적을 위한 적합성, 상업성 또는 특허, 저작권, 다른 지적재산권의 어떠한 침해와 관련하여, 보증책임을 포함한 슈프리마 제품의 판매 또는 사용에 관하여, 여하간의 책임을 지지 않으며 보증을 하지 않습니다.

슈프리마 제품이, 의학적 상황, 인명 구조, 생명 유지 등의 목적 또는 슈프리마 제품의 오류로 인해 인명 상해나 사망을 야기할 수 있는 상황에 적용되어 사용되는 것은 고려되지 않았습니다. 구매자가 슈프리마 제품을 무단으로 이러한 경우에 적용하여 사용한다면, 구매자는 이러한 의도적이지 않은 사용 또는 무단 사용과 관련하여 인명 상해 또는 사망과 관련한 어떠한 클레임으로 인해 직,간접적으로 야기되는 모든 청구, 비용, 손해, 지출과 적절한 변호사 비용에 대해서, 슈프리마, 슈프리마 임원, 고용인, 자회사, 계열회사와 판매자들에게, 설령 슈프리마가 그 부분의 설계나 생산을 간과했다고 클레임에서 주장되더라도, 해가 없도록 보상하고 보호해야 할 것입니다.

슈프리마는 제품의 신뢰성, 기능 또는 설계 사항을 향상시키기 위해, 공지 없이 어느 때라도 규정과 제품내용을 변경할 수 있는 권리를 보유합니다. 설계자는 "유보된" 또는 "불확정적인" 이라고 표시된 어떠한 특징이나 사용설명의 특성이나 부재를 신뢰해서는 안됩니다. 슈프리마는 장래 규정에 대해 이러한 권리를 보유하고 있으며 이에 대한 장래 변경사항으로부터 야기되는 비호환성에 대하여 여하간의 책임도 지지 않을 것입니다.

가장 최근의 제품 사양이 필요 할 경우에는 제품주문 전에 슈프리마, 지역 슈프리마 판매 대리점에 연락하여 주시기 바랍니다.

Note : 제3자의 상표와 명칭은 해당 권리자의 소유입니다.

BioEntry 시리즈와 BioStation 에 대해

BioEntry 와 BioStation은 지문 인증 컨테스트(FVC2004, FVC2006)에서 2회 연속 세계 1위를 수상한 알고리즘과 표준 Wiegand 인터페이스를 가진 바이오 인식 출입통제 장치입니다. BioEntry 와 BioStation은 기존 시스템을 손쉽게 대체하거나, 기존 시스템에 기존 출입통제시스템에 쉽게 추가

할 수 있습니다.

BioEntry Smart는 지문 인식과 스마트 카드 장치의 최적화된 통합 제품으로 지문인식정보는 비접촉식 스마트 카드에 저장되어 스마트 카드 소지인의 지문 인증 시 사용되게 됩니다. 지문인식정보를 스마트 카드에 저장함으로써, 지문 등록 및 관리의 필요성이 없으며, 추가적인 배선이 필요 없이 간편하게 기존의 Proximity, Wiegand 또는 Magstrip 장치를 대체할 수 있습니다.

BioEntry Pass는 FVC 2004와 FVC2006에서 2회 연속 세계 1위를 차지한 슈프리마 자체 알고리즘이 내장된 탁월한 성능의 출입 통제용 지문 인식 장치입니다. 업계 최고의 빠른 지문 인증 속도를 자랑하는 **BioEntry Pass**는 수 천명의 사용자들이 **Keys, Cards** 또는 **PINs code** 없이도 지문인증만으로 출입할 수 있는 편리하고 안전한 출입통제시스템을 실현시킵니다.

BioStation은 FVC 2004와 FVC2006에서 2회 연속 세계 1위를 차지한 슈프리마 자체 알고리즘이 내장된 탁월한 성능의 출입 통제용 지문 인식 장치입니다. 출입통제와 근태관리를 위한 다기능 지문인식 종합단말기 **BioStation**은 대형 컬러LCD와 고품질 사운드를 채용해 각종 멀티미디어 정보를 실시간으로 제공합니다. 또한 무선랜이나 USB메모리를 이용해 복잡한 배선 없이 네트워크 구성과 자료전송이 가능합니다.

BioEntry 와 **BioStation**은 사용자가 응용시스템에 맞는 최적의 지문센서를 활용할 수 있도록, 광학식, 반도체식 (촉전식), 또는 스캔식 (열감지식) 등의 다양한 지문 센서를 지원합니다.

(주)슈프리마에 대해

슈프리마는 지문인식 핵심기술과 각종 응용제품을 공급하는 세계 일류의 바이오 인식 보안업체입니다. 슈프리마의 지문인식 기술은 편의성과 보안성을 겸비한 최고의 본인 인증수단으로서 출입보안, 정보보안, 금융보안 등 다양한 분야에 적용되고 있습니다. 슈프리마의 지문인식 기술은 지문인증 컨테스트(FVC2004, FVC2006)에서 가장 낮은 에러율을 기록함으로써, 세계적으로 가장 신뢰성 있는 솔루션으로 인정 받았습니다. 슈프리마의 지문관련 제품은 세계 80 여 개국에 판매되고 있으며 다양한 응용제품에 쓰이고 있습니다.

슈프리마의 기술과 제품에 대한 더 많은 정보를 원하시면, 슈프리마 웹사이트(<http://www.supremainc.com>)를 방문하시거나 전자 우편(sales@suprema.co.kr)으로 문의해 주시기 바랍니다.

이 사용 설명서에 대해

이 사용 설명서는 **BioEntry Plus, Smart**와 **Pass** 그리고 **BioStation**의 사용법을 안내하며, 사용시 발생할 수 있는 문제점들을 해결하는 것을 목적으로

로 하고 있습니다. 장치의 지문인식정보를 등록, 삭제하는 등의 운영 방법
과 각종 설정 값을 조정하는 방법에 대하여 기술하고 있습니다.

목차

BioEntry 시리즈와 BioStation 에 대해	3
(주)슈프리마에 대해.....	4
이 사용 설명서에 대해.....	4
1. 시작하기.....	15
1.1. 개요	15
1.2. 기초 지식	15
1.2.1. 지문인식 장치	15
1.2.2. 지문인식 스마트카드 장치.....	15
1.2.3. 지문정보.....	15
1.2.4. 등록.....	16
1.2.5. 인증.....	16
1.2.6. 인식.....	16
1.2.7. 사용자 데이터베이스.....	16
1.2.8. 전송.....	16
1.2.9. 스마트카드에 대한 사이트 키	17
1.3. 올바른 지문 입력 방법	17
1.3.1. 지문입력을 위한 손가락 선택	17
1.3.2. 지문을 센서에 바르게 입력하는 방법	17
1.3.3. 손가락 상태에 따른 대처방안	17
1.3.4. 지문입력 시 권고사항.....	18
1.4. 소프트웨어 설치.....	18
1.4.1. 1단계: BioAdmin 서버 설치하기	18
1.4.2. 클라이언트 설치 하기.....	24
1.4.3. 별도 DB의 설정	26
1.4.4. 소프트웨어 설치 확인.....	30
1.5. BioAdmin 에 로그인 하기	33
1.5.1. 서버에 접속	33
1.5.2. 초기 시스템 관리자 등록	33
1.5.3. BioAdmin 소프트웨어에 로그인	33
1.6. BioAdmin 사용자 별 권한	34

1.7.	BioAdmin 구성	34
1.7.1.	메뉴 바	35
1.7.2.	주 메뉴	35
1.7.3.	작업 목록과 도구 목록	36
1.7.4.	주 윈도우.....	36
1.8.	사용자 데이터베이스.....	36
2.	시작하기 전에 결정할 사항	36
2.1.	바이오 정보 보호 가이드 라인	36
2.2.	지문 옵션	37
2.3.	출입 그룹 설정	37
2.4.	Mifare 카드 사용.....	37
3.	빠른 시작.....	37
3.1.	BioStation 과 함께 빠른 시작	37
3.1.1.	1단계 : 하드웨어 설치.....	38
3.1.2.	2단계 : 새 장치 검색	38
3.1.3.	3단계 : 장치 연결.....	41
3.1.4.	4단계 : 사용자 관리	45
3.1.5.	5단계 : 사용자의 Mifare 카드 발급하기	52
3.1.6.	6단계 : 사용자 근태관리 규칙	54
3.1.7.	7단계 : 체크된 사용자를 장치에 전송 메뉴로 사용자 등록.....	55
3.1.8.	8단계 : 실시간 감시	56
3.1.9.	9단계 : 로그 확인.....	57
3.1.10.	10단계 : 보고서 리포트	57
3.2.	BioEntry Plus와 함께 빠른 시작.....	58
3.2.1.	1단계 : 하드웨어 설치.....	58
3.2.2.	2단계 : 새 장치 검색	58
3.2.3.	3단계 : 새 장치에 연결.....	58
3.2.4.	4단계 : 사용자 관리	61
3.2.5.	5단계 : 사용자의 Mifare 카드 발급하기	67
3.2.6.	6단계 : 사용자 근태관리 규칙	69
3.2.7.	7단계 : 체크된 사용자를 장치에 전송 메뉴로 사용자 등록.....	70
3.2.8.	8단계 : 실시간 감시	71

3.2.9. 9단계 : 로그 확인.....	72
3.2.10. 10단계 : 보고서 리포트.....	72
3.3. BioLite Net 과 함께 빠른 시작.....	73
3.3.1. 1단계 : 하드웨어 설치.....	73
3.3.2. 2단계 : 새 장치 검색.....	73
3.3.3. 3단계 : 새 장치에 연결.....	73
3.3.4. 4단계 : 사용자 관리.....	75
3.3.5. 5단계 : 사용자의 Mifare 카드 발급하기.....	81
3.3.6. 6단계 : 사용자 근태관리 규칙.....	83
3.3.7. 7단계 : 체크된 사용자를 장치에 전송 메뉴로 사용자 등록.....	84
3.3.8. 8단계 : 실시간 감시.....	85
3.3.9. 9단계 : 로그 확인.....	86
3.3.10. 10단계 : 보고서 리포트.....	86
3.4. BioEntry Smart와 함께 빠른 시작.....	87
3.4.1. 1단계 : 하드웨어 설치.....	87
3.4.2. 2단계 : 사용자 등록.....	87
3.4.3. 3단계 : 사용자의 스마트카드 발급하기.....	93
3.4.4. 4단계 : 외부 컨트롤러에 사용자 ID 등록.....	95
3.4.5. 5단계 : 인증 테스트.....	95
3.5. BioEntry Pass와 함께 빠른 시작.....	95
3.5.1. 1단계 : 하드웨어 설치.....	96
3.5.2. 2단계 : 새 장치 검색.....	96
3.5.3. 3단계 : 사용자 등록.....	99
3.5.4. 4단계 : 체크된 사용자를 장치에 전송 메뉴로 사용자 등록.....	105
3.5.5. 5단계 : 외부 컨트롤러에 사용자 ID 등록.....	107
3.5.6. 6단계 : 인식 테스트.....	107
3.5.7. 7단계 : 실시간 감시.....	107
3.5.8. 8단계 : 로그 확인.....	108
4. 사용자 관리.....	108
4.1. 사용자 관리 페이지의 구성.....	109
4.2. 사용자 리스트 윈도우.....	110
4.3. 사용자 리스트 표시 설정.....	110
4.4. 사용자 검색.....	112

4.5.	사용자 선택.....	113
4.6.	새 사용자를 추가.....	113
4.6.1.	사용자 정보.....	114
4.6.2.	사용자 정의 항목.....	115
4.6.3.	지문.....	117
4.6.4.	사용자 스마트카드 발급하기.....	120
4.6.5.	PC USB 스마트카드 장치로 발급.....	120
4.6.6.	단말기로 발급.....	121
4.6.7.	사용자 보안 등급과 항상 통과카드 설정.....	121
4.6.8.	ID 카드 이용하여 Wiegand 스트링 설정.....	121
4.6.9.	발급된 스마트카드 정보 읽기.....	122
4.6.10.	카드 포맷.....	122
4.6.11.	카드 발급 시 중요한 주의사항.....	122
4.6.12.	사용자 근태관리 규칙.....	122
4.7.	체크된 사용자를 삭제.....	122
4.7.1.	BioAdmin 소프트웨어에서 체크된 사용자 삭제.....	123
4.7.2.	삭제된 사용자 정보를 장치와 동기화.....	123
4.8.	체크된 사용자를 장치에 전송.....	123
4.9.	체크된 사용자를 장치에서 삭제.....	124
4.10.	체크된 사용자의 출입그룹 설정.....	124
4.11.	체크된 사용자의 근태 규칙 그룹 설정.....	124
4.12.	장치 별 사용자 관리.....	124
4.13.	모든 사용자를 장치와 동기화.....	126
4.14.	파일로 내보내기.....	127
4.15.	파일에서 가져오기.....	128
5.	장치 관리.....	129
5.1.	새 장치 추가.....	131
5.1.1.	직렬 포트.....	131
5.1.2.	이더넷.....	132
5.1.3.	USB 장치.....	133
5.1.4.	USB 가상 BioStation.....	134
5.1.5.	UDP (BioEntry Plus / BioLite Net).....	136

5.2. BEACon 컨트롤러 추가.....	139
5.3. 장치제거	140
5.4. 목록창.....	141
5.4.1. 장치목록.....	141
5.4.2. 구역목록.....	142
5.5. BioStation 장치 관리.....	143
5.5.1. 장치정보.....	144
5.5.2. 동작모드.....	144
5.5.3. 네트워크.....	147
5.5.4. 근태 기능 키	151
5.5.5. 단말기 설정	152
5.5.6. 화면 / 음성.....	155
5.5.7. 공지사항.....	157
5.5.8. Wiegand 설정.....	158
5.5.9. 출입문 설정	162
5.5.10. 입/출력 설정	163
5.5.11.출입 통제 설정.....	165
5.5.12. 인증 거부 리스트.....	166
5.6. USB 가상 BioStation 장치 관리	167
5.7. BioEntry Plus 장치 관리	168
5.7.1. 장치 정보.....	168
5.7.2. UDP로 환경 설정하기	168
5.7.3. 동작 모드.....	170
5.7.4. 네트워크.....	173
5.7.5. 출입 통제 설정.....	174
5.7.6. 출입문 설정	176
5.7.7. 입/출력 설정	177
5.7.8. 커맨드카드.....	178
5.7.9. Wiegand.....	179
5.7.10. 인증 거부 리스트.....	181
5.8. BioLite Net 장치 관리	182
5.8.1. 장치 정보.....	182
5.8.2. UDP로 환경 설정하기	183

5.8.3. 동작 모드.....	185
5.8.4. 지문 설정.....	187
5.8.5. 네트워크.....	189
5.8.6. 근태 이벤트.....	191
5.8.7. 출입 통제 설정.....	192
5.8.8. 출입문 설정.....	194
5.8.9. 입/출력 설정.....	195
5.8.10. Wiegand.....	196
5.8.11.인증 거부 리스트.....	198
5.9. BioEntry 장치 관리.....	199
5.9.1. 장치정보.....	200
5.9.2. 시스템 설정.....	200
5.9.3. 입출력 설정.....	203
5.9.4. LED / 비프 음 설정.....	206
5.9.5. Wiegand 설정.....	208
5.9.6. 스마트 카드 설정.....	211
5.10. BEACon 환경설정.....	213
5.10.1. 동작 모드.....	214
5.10.2. 통신속도.....	215
5.10.3. BEACon 릴레이 설정.....	215
5.10.4. 스위치 설정.....	216
5.10.5. 다시 가져오기 / 적용 / 다른 장치에 적용.....	218
6. 스마트 카드 / Mifare 카드.....	218
6.1. 스마트카드 페이지의 구성.....	219
6.2. 스마트카드 리스트.....	219
6.3. 카드 발급.....	220
6.4. 스마트카드 관리.....	220
6.4.1. 발급된 스마트카드 읽기.....	221
6.4.2. 스마트카드 포맷.....	221
6.5. 카드 레이아웃 편집.....	221
6.5.1. Mifare 설정.....	221
6.5.2. 스마트카드 레이아웃 편집.....	222
6.5.3. 지문데이터 크기.....	223

6.5.4. 블록.....	223
6.5.5. 편집과정.....	223
6.5.6. 초기 설정 레이아웃	224
6.5.7. Mifare 카드 레이아웃 설정 (BioStation / BioEntry Plus)	224
6.5.8. 편집 과정.....	225
7. 출입 통제.....	226
7.1. 시간대 설정	227
7.2. 휴일 군 설정	228
7.3. 출입시간 설정	229
7.4. 출입구역 설정	230
7.5. 출입 그룹 설정	231
7.6. 출입 그룹 장치에 적용.....	233
8. 실시간 감시	233
8.1. 실시간 감시 설정	234
8.2. 실시간 감시 시작.....	235
8.3. 실시간 감시 멈춤.....	235
8.4. 출입문 실시간 감시	235
8.4.1. 문열기/문닫기	236
8.4.2. 경보 해제.....	236
9. 로그 확인.....	236
9.1. 로그 확인 페이지의 구성	237
9.2. 로그 데이터베이스 관리	237
9.2.1. 최근 로그 가져오기	237
9.2.2. 예약 전송 설정.....	238
9.2.3. 예약 전송 설정을 해제	239
9.2.4. 모든 로그를 다시 가져오기.....	240
9.2.5. 파일로 내보내기	241
9.2.6. 로그 정보 삭제.....	242
10. 보고서	242
10.1. 보고서 목록 페이지의 구성.....	243
10.2. 근태관리 규칙 설정	243
10.2.1. 장치 설정.....	244

10.2.2.	시간 설정.....	246
10.2.3.	바이오 스테이션 기능 키 설정.....	247
10.3.	월간 규칙 설정.....	248
10.4.	근태 관리 그룹 설정.....	249
10.5.	보고서 작성 방법.....	250
10.6.	보고서 자료 수정.....	252
11.	메뉴 바의 기능들.....	254
11.1.	시스템.....	254
11.1.1.	관리자 계정 관리.....	254
11.1.2.	자료 백업.....	254
11.1.3.	자료 복구.....	254
11.1.4.	모든 장치 잠금.....	255
11.1.5.	모든 장치 잠금 해제.....	255
11.1.6.	BioAdmin 1.X 자료 가져오기.....	255
11.1.7.	옵션.....	255
11.1.8.	BioAdmin 정보.....	262
11.1.9.	서버 재 접속.....	262
11.2.	사용자 관리.....	263
11.3.	장치 관리.....	263
11.3.1.	시간 설정.....	264
11.3.2.	펌웨어 업그레이드.....	264
11.3.3.	사이트 키 설정(BioEntry Smart).....	265
11.3.4.	사이트 키 설정(Mifare).....	267
11.4.	출입 통제.....	268
기술 문의.....		269

개정 연혁

버 전	날 짜	설 명
V1.0	2005.9.27	생성됨.
V1.1	2005.12.2	BioAdmin V1.1의 변경사항을 추가함. 제12장 사이트 키 부분이 추가됨.
V2.0	2006.4.17	BioAdmin V2.0의 변경사항을 추가함. 제8장 출입 통제 부분이 추가됨. 제9장 모니터링 부분이 추가됨.
V3.0	2006.7.20	BioAdmin V3.0의 변경사항을 추가함. BioStation 장치 추가됨.
V4.0	2007.3.5	BioAdmin V4.0의 변경사항을 추가함.
V4.1	2007.5.30	BioAdmin V4.1의 변경사항을 추가함.
V4.2	2007.10.19	BioAdmin V4.2의 변경사항을 추가함. BioEntry Plus 장치 추가됨.
V4.2.2	2008.4.28	BioAdmin V4.2.2의 변경사항을 추가함.
V4.3	2008.12.10	BioAdmin V4.3의 변경사항을 추가함. BioLite Net 장치 추가됨.

1. 시작하기

1.1. 개요

이 사용 설명서는 PC 윈도우 기반 환경에서 작동하는 슈프리마의 BioAdmin 프로그램의 사용법에 대해 소개합니다. BioAdmin 프로그램은 슈프리마의 BioEntry, BioStation, BEACon 등의 장치와 연결하여 출입통제 및 근태관리 응용을 위한 관리시스템으로 사용되는 소프트웨어입니다.

BioAdmin 프로그램 사용에 앞서 올바른 하드웨어 연결을 위해 BioEntry 와 BioStation, BioLite Net 설치 안내서를 참조하시기 바랍니다.

BioEntry 와 BioStation, BioLite Net장치를 운영하는 방법에는 두 가지가 있습니다.

- 슈프리마 BioAdmin 소프트웨어 사용

윈도우 기반 PC 환경에서 작동하는 슈프리마의 관리소프트웨어인 BioAdmin 프로그램 사용할 수 있습니다. 이 사용설명서는 BioAdmin 프로그램을 이용하여 BioEntry 와 BioStation 장치를 사용하는 사용자들을 주로 고려하였습니다.

- 고객의 응용 소프트웨어 사용

장치 제어를 위한 다양한 API를 포함하는 슈프리마의 SDK를 사용하여 고객이 응용 소프트웨어를 직접 개발할 수 있습니다. 상세한 정보를 위해서는 BioEntry의 경우 SFM SDK, 사용 설명서, BioStation의 경우 BioStation 사용 설명서를 참조하시기 바랍니다.

1.2. 기초 지식

이 장에서는 BioEntry 와 BioStation 장치 및 BioAdmin 소프트웨어에 대하여 기본 개념, 작동 절차 및 소프트웨어의 개요를 포함한 개괄적인 정보를 제공하고 있습니다.

1.2.1. 지문인식 장치

지문인식 장치는 지문을 이용하여 각 개인의 신원을 인증하는 장치입니다. 이 장치는, Wiegand 인터페이스와 같은 표준 인터페이스를 통해 출입 통제 컨트롤러에 연결되므로 출입 통제 시스템에 쉽게 통합될 수 있습니다. 지문은 각 개인이 고유하게 가지는 생체 인식 특징이므로, 지문인식 장치는 기존의 출입 장치, 즉 바코드, 자기 카드, 키 패드 또는 RF 카드 장치 등에 비해 보다 강력한 보안성과 효율성을 갖춘 시스템을 제공합니다.

1.2.2. 지문인식 스마트카드 장치

지문인식 스마트카드 장치는 기존 지문인식 장치에 스마트카드 기술을 통합함으로써 시스템의 보안성을 향상시킨 지문인식 장치의 진보된 모델입니다. 사용자의 지문정보는 사용자의 스마트카드에 저장되고 장치는 스마트카드에 저장된 지문과 입력 지문을 비교하여 사용자를 인증합니다.

1.2.3. 지문정보

지문정보는 각 지문의 특징을 나타내는 데이터입니다. 지문 센서에 입력된 지문 영상은 지문정보로 변형되는데, 이 정보가 지문인식 장치나 사용자의 스마트카드에 저장됩니다. 사용자를 인증할 때 새로운 지문정보가 생성되어 저장된 지문정보와 비교됩니다.

1.2.4. 등록

등록은 지문정보를 사용자의 정보와 함께 저장하는 과정입니다. 등록 과정을 통해 새로운 사용자들이 출입통제 시스템에 들어올 수 있습니다.

1.2.5. 인증

인증이란 하나의 특정 지문과 입력지문의 동일여부를 확인하는 과정입니다. **BioEntry Smart**의 경우 사용자의 지문정보와 ID 정보를 스마트카드에 저장합니다. 그리고 장치는 입력 지문을 스캐닝하여 스마트카드에 저장된 지문과 비교하는 인증 과정을 수행합니다. **BioEntry Pass**에서 인증과정은 외부 **Wiegand** 리더, 즉 현재 사용자 ID 정보를 제공하는 RF 카드 장치등과 연결하여 구현될 수 있습니다.

1.2.6. 인식

인식은 장치에 등록된 여러 개의 지문들 중에서 입력 지문과 일치하는 지문을 찾아내는 과정입니다. **BioEntry Pass** 와 **BioStation** 은 기본적으로 인식모드에서 작동되며 이 때 지문을 입력 하면 됩니다.

1.2.7. 사용자 데이터베이스

사용자 데이터베이스는 사용자 ID, 사용자 이름, 지문정보 등을 포함하는 사용자 정보 일체를 말합니다. **BioAdmin** 소프트웨어는 사용자 데이터베이스를 중점적으로 관리하는 것에 기반을 두고 있습니다. 즉, 사용자 데이터베이스가 생성되고, 갱신되고 호스트 PC에 저장됩니다. 호스트 PC에 저장된 정보는 전송을 이용하여 네트워크에 연결된 장치들에게 선택적으로 분배됩니다.

1.2.8. 전송

장치로 내보내기는 호스트 PC의 사용자 데이터베이스를 **BioEntry** 와 **BioStation** 장치들에게 보내기 위해 사용됩니다. 사용자 ID, 지문정보, 출입 그룹, 보안 등급과 같은 사용자 정보는 전송과정을 통해 장치로 전달됩니다

구체적인 동작은 다음과 같습니다.

- 장치에 새로운 사용자를 등록합니다.
- 장치에서 일치하지 않는 지문정보를 대체합니다.
- 장치에서 미상의 사용자와 선택 해제된 사용자들의 지문정보들을 삭제합니다.

장치에서 가져오기는 **BioEntry** 와 **BioStation**으로부터 호스트 PC로 사용자 정보를 받기 위해 사용됩니다. 사용자 ID, 지문정보, 출입 그룹의 번호와 보안 등급 등과 같은 사용자 정보 등을 이 과정을 통해서 받아들일 수 있습니다.

1.2.9. 스마트카드에 대한 사이트 키

사이트 키는 공인된 카드만이 사용될 수 있도록 보장하는 스마트카드의 패스워드입니다. 0부터 281374976710655 (0xFFFFFFFF) 사이의 48비트 키가 BioEntry Smart에서 사용될 수 있습니다. BioEntry Smart와 사용자의 스마트카드에 동일한 사이트 키가 설정되어 있어야 제대로 동작합니다.

1.3. 올바른 지문 입력 방법

1.3.1. 지문입력을 위한 손가락 선택

- (1) 사용할 손가락은 검지 또는 중지의 사용을 권합니다.
- (2) 엄지, 약지, 소지는 센서에 닿 때 불안정한 상태로 정확히 중앙에 위치하기가 상대적으로 힘듭니다.

1.3.2. 지문을 센서에 바르게 입력하는 방법

- (1) 손가락이 센서를 완전히 덮어 접촉되는 면적이 많도록 깊숙이 위치시킵니다.
- (2) 지문 중심점(Core) 부분을 센서의 중앙에 댑니다.
 - 일반적으로 손가락의 위쪽 끝부분만을 대는 경향이 많습니다.
 - 지문의 중심점은 무엇입니까?
지문의 융선이 회전하여 모이는 봉우리 부분
대개 손톱의 아래쪽 반달 모양의 반대편에 위치
지문을 센서에 댑 때 손톱의 아래쪽 반달 부분이 센서 중앙에 위치하도록 권장
- (3) 센서를 짚어 누르듯이 손가락을 세워서 대면 손끝부분의 지문만 입력되므로 정상적인 등록이나 인증이 되지 않습니다.



1.3.3. 손가락 상태에 따른 대처방안

슈프리마의 지문인식 제품은 계절의 변화나 손가락의 상태 변화에 상관없이 지문 입력이 잘 되도록 설계되어 있습니다. 하지만 외부 영향에 따라 지문입력이 어려울 경우 다음 사항을 참고하시기 바랍니다.

- (1) 손가락에 물이 묻어있는 경우, 물기를 닦은 후 입력합니다.
- (2) 손가락에 먼지 등 이물질이 묻어 있는 경우, 잘 닦거나 털어내고 입력합니다.
- (3) 손가락이 너무 건조하여 입력이 안될 경우, 손끝에 가볍게 입김을 불고 입력합니다.

1.3.4. 지문입력 시 권고사항

- (1) 지문인식에서 등록 과정이 매우 중요합니다. 따라서, 처음에 지문을 등록할 때는 신경을 써서 올바르게 지문을 입력하도록 합니다.
- (2) 인증율이 떨어질 경우 다음과 같은 조치를 권장합니다.
 - 등록된 지문을 지우고 다시 등록합니다.
 - 같은 지문을 추가로 더 등록합니다.
 - 상처 등으로 입력이 어려운 손가락이 있을 수 있으므로 다른 손가락으로 시도합니다.
- (3) 손에 짐을 들거나 손가락에 상처가 나는 경우 등, 등록된 지문의 사용이 어려운 경우를 대비해 두 개 이상의 손가락 등록을 권장합니다.

1.4. 소프트웨어 설치

BioAdmin 4.0 이후부터 기존의 단일 프로그램 방식에서 서버-클라이언트 방식으로 구조가 변경되었습니다. 모든 데이터를 저장하고 있는 데이터베이스는 BioAdmin 서버에서 관리하게 되며, BioAdmin 클라이언트 프로그램은 사용자 UI를 표시하고 데이터를 관리할 수 있는 도구로의 역할을 하게 됩니다. 또한 BioAdmin 서버에는 다수의 BioAdmin 클라이언트가 접속하여 데이터를 관리할 수 있습니다.

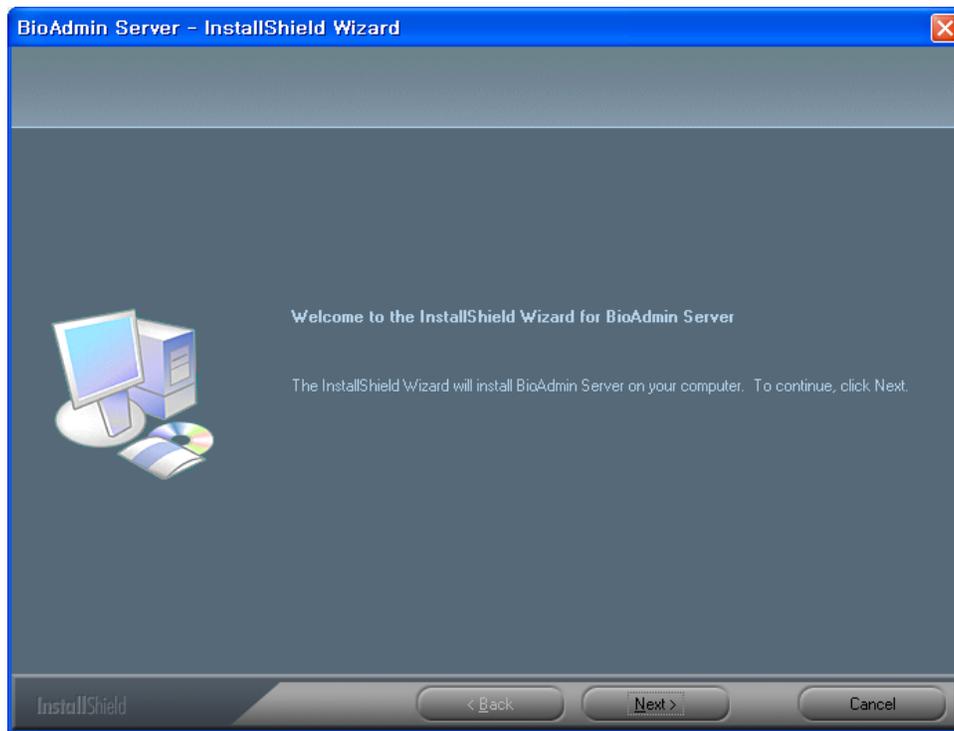
이 절에서는 서버와 클라이언트 프로그램의 설치 및 사용을 위한 환경 설정에 관한 내용을 다루게 됩니다.

1.4.1. 1단계: BioAdmin 서버 설치하기

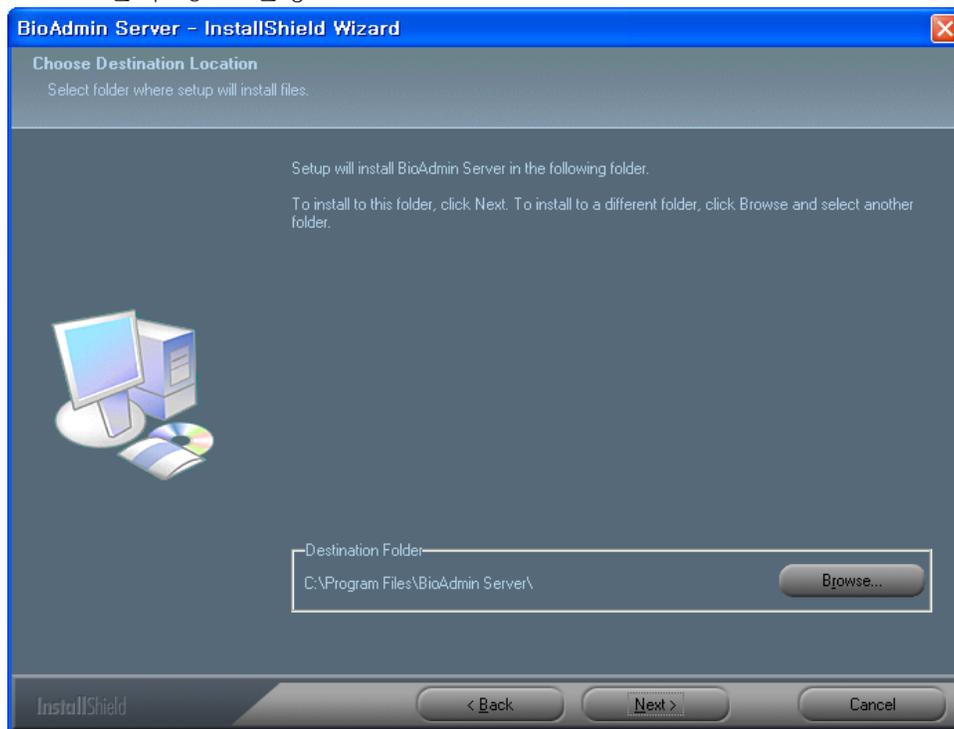
- 먼저 서버로 사용할 PC를 선정합니다. 서버는 항상 켜있는 상태로 서버에 직접 연결된 BioStation으로부터 로그 데이터를 실시간으로 받아서 DB에 저장하는 역할 및 다수의 BioAdmin 클라이언트로부터 여러 가지 작업 요청을 받기 때문에 만약 등록하게 될 사용자가 더 많거나, 한번에 처리하고자 하는 로그 데이터 수가 증가하게 되면 처리 속도가 떨어질 수 있습니다.
- BioAdmin 서버로 사용할 PC를 결정 하였다면 서버 프로그램의 설치를 시작합니다. 이후 설치에 대한 설명은 서버 프로그램이 설치되는 PC에 자체 DB를 사용하는 것으로 가정하며 MySQL이나 SQL 서버를 사용하는 경우에는 1. 4. 3 절을 참고하시기 바랍니다.

이름	크기	종류
BioAdminServerSetupV40Korean.exe	16,772KB	응용 프로그램

- 설치 초기 화면
 - 설치를 시작합니다.

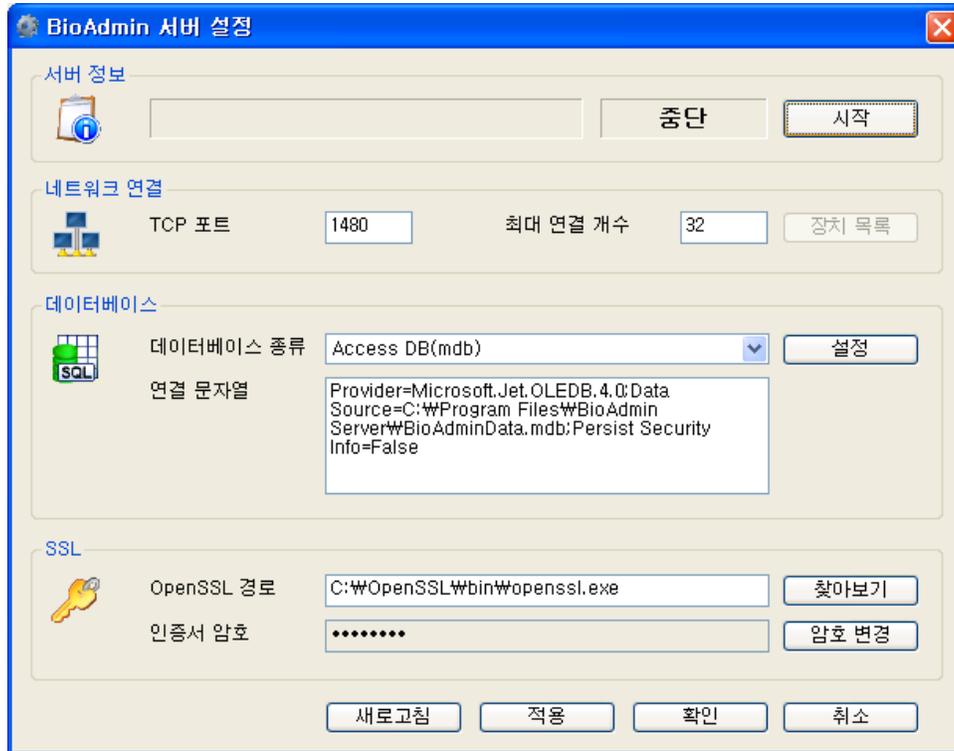


▪ 설치 경로 설정



서버가 설치될 하드 디스크 드라이브 상의 경로를 선택합니다. 기본은 C:\Program Files\BioAdmin Server\ 입니다. 이 과정을 마친 후 필요한 파일들을 설치 디스크로부터 PC로 복사를 시작합니다.

- 서버 환경 설정 및 DB 설정
프로그램 파일의 복사가 완료된 뒤에 서버를 구동하기 위한 설정 화면이 나타납니다. 기본적으로는 이미 설정되어 있는 상태를 유지하시면 됩니다.



- 서버 정보

현재 서버의 버전 및 상태를 표시합니다. '중지' 버튼을 눌러 서버를 잠시 중단하거나 '시작'을 눌러 다시 시작할 수 있습니다.

서버가 중단되어 있는 상태에서는 네트워크에 연결되어 있는 **BioStation**의 로그 수집도 중단되며, **BioAdmin** 클라이언트들도 접속할 수 없는 상태가 됩니다.

서버의 환경을 변경하거나, **DB**의 설정을 변경한 경우에는 반드시 서버를 중지시킨 뒤 시작해 주십시오. 재 시작하기 전에는 변경된 설정 사항이 적용되지 않습니다.

- 네트워크 연결

네트워크 관련 사항들을 설정합니다.

- TCP 포트

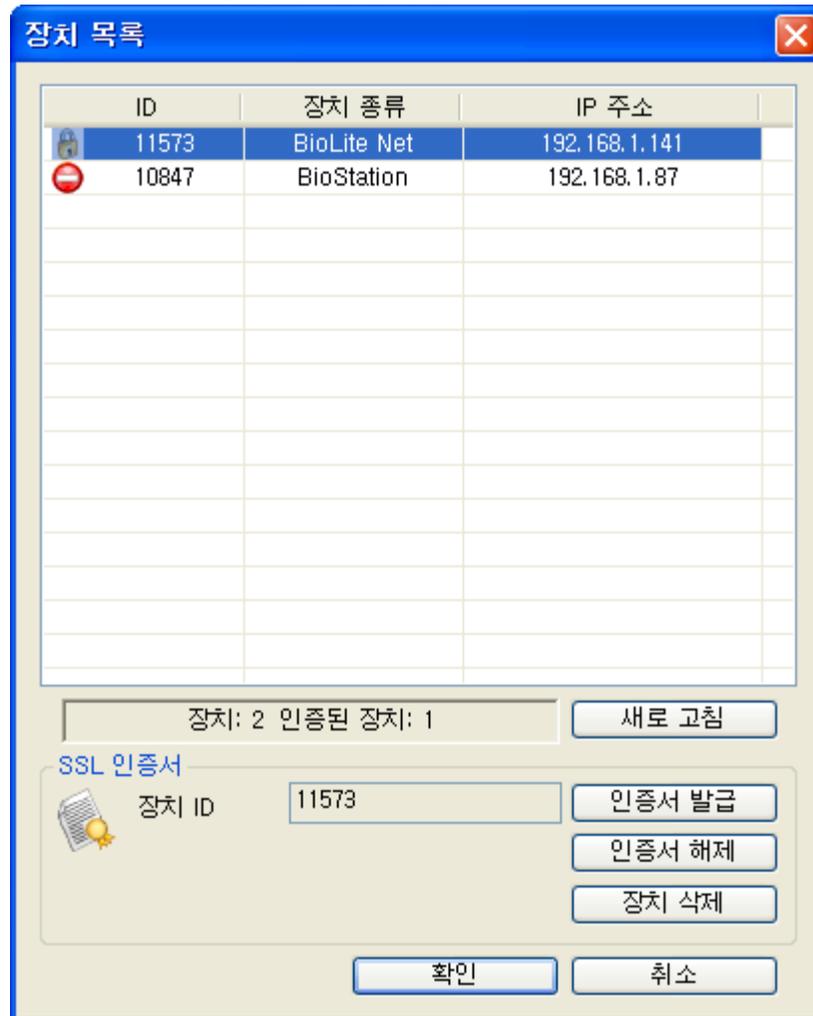
BioStation이나 **BioAdmin** 클라이언트가 서버에 접속할 때 사용할 통신 포트입니다. 다른 소프트웨어에서 사용하지 않는 포트를 설정해 주십시오. 일반적으로는 기본값인 1480번을 사용하시면 됩니다.

- 최대 연결 개수

한번에 연결할 수 있는 **BioStation** 및 **BioAdmin** 클라이언트의 수입니다. 여기에 설정된 제한 수량 이상은 동시에 접속할 수 없습니다. 필요에 따라서 증가시켜 사용할 수 있지만, 최대 128을 초과할 수 없습니다. 기본 값인 32개를 넘지 않는다면 숫자를 줄여서 설정하지 않아도 됩니다.

▪ 장치 목록

현재 서버에 접속되어 있는 **BioStation**의 목록을 표시합니다. 이 목록에는 연결된 **BioStation**의 IP 및 인증서 발급 여부가 표시되며, 인증서의 발급 및 삭제를 할 수 있습니다. 현재 서버가 중지되어 있다면 이 항목은 비 활성화 상태가 되어 사용할 수 없습니다.



▪ 데이터베이스

BioAdmin 서버에서 데이터를 저장하는데 사용할 데이터베이스를 설정합니다. **BioAdmin** 서버는 내부적으로 **Microsoft Access Database**를 사용하며, 외부 DB를 사용하고 있지 않다면 기본값을 그대로 사용하시면 됩니다. 이 외에 추가로 **MySQL** 및 **SQL** 서버를 지원합니다.

단, MySQL 및 SQL 서버의 경우 이미 설정하여 사용 중이거나, 사용 가능한 상태여야 합니다. BioAdmin에서는 추가로 MySQL 및 SQL 서버의 설치를 지원하지 않습니다.

데이터베이스와 관련된 보다 자세한 사항은 1.4.3 절을 보십시오.

▪ SSL

BioAdmin 서버가 BioStation 및 BioAdmin 클라이언트와의 통신을 암호화 하기 위한 설정입니다.

새로 고침 버튼을 눌러 현재 저장된 상태를 다시 표시합니다.

적용 버튼을 눌러 현재 상태를 저장합니다. 저장된 사항은 서버를 중지 후 다시 시작해야 적용 됩니다.

확인 버튼을 눌러 현재 상태를 저장하고 'BioAdmin 서버 설정'을 종료 합니다.

취소 버튼을 눌러 변경을 취소하고 마지막 저장된 상태를 유지합니다. 'BioAdmin 서버 설정'을 종료 합니다.

● OpenSSL 설정

BioAdmin 서버는 BioStation과의 통신에, 그리고 BioAdmin 클라이언트와의 통신에 SSL 인증을 통한 암호화를 사용합니다. 이 암호화 방식은 서버 인증이라고도 합니다. 클라이언트와 서버간의 통신, BioStation과 서버간의 통신에서 정보를 암호화 함으로써 도중에 해킹을 통해 정보가 유출 되더라도 정보의 내용을 보호할 수 있게 해 주는 보안 솔루션입니다

openssl.exe의 경로를 설정해 줍니다. 기본적으로는 아래 경로에서 해당 파일을 발견할 수 있지만, 설치 경로가 다른 경우에는 '찾아보기'를 클릭하여 올바른 경로를 설정해 줍니다.

기본 openssl.exe의 경로: (C:\OpenSSL\bin\openssl.exe)

인증서 암호는 발급된 인증서가 유효한 것인지 판단하는 것으로 8자 이상 입력해야 하며 영문, 숫자 및 특수문자를 포함할 수 있습니다. 처음 설치할 때 인증서 암호를 변경할 것을 강력히 권장합니다.



The image shows a Windows dialog box titled "인증서 암호 변경" (Certificate Password Change). It has a blue title bar with a close button (X) in the top right corner. The dialog contains two text input fields, both with masked characters (dots). The first field is labeled "새 암호" (New Password) and the second is labeled "다시 입력" (Re-enter). To the right of the first field is a button labeled "확인" (OK), and to the right of the second field is a button labeled "취소" (Cancel).

만약 BioAdmin 서버를 설치하여 사용하던 도중에 인증서 암호를 변경하게 되는 경우에는 다음 절차를 따라야 합니다.

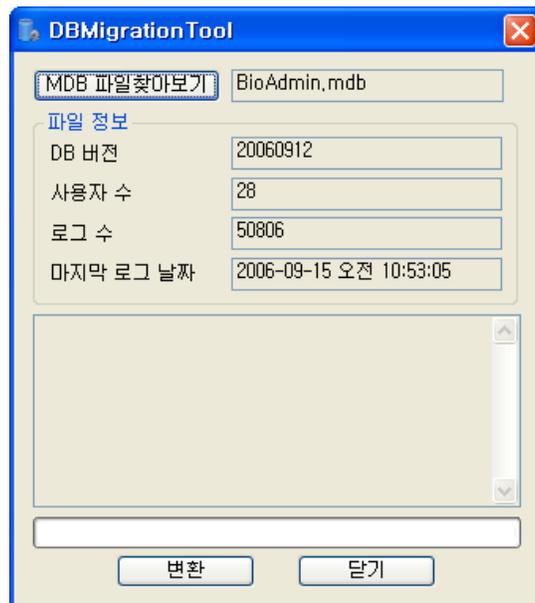
- 현재 연결되어 있는 모든 BioStation의 SSL 옵션을 사용 안 함으로 설정

합니다.

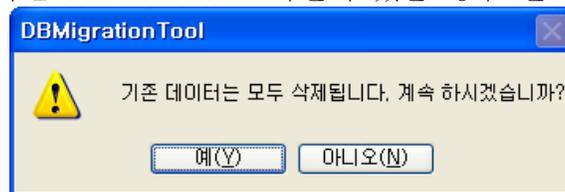
- BioAdmin 서버를 중지 합니다.
- 인증서 암호를 변경합니다.
- BioAdmin 서버를 시작 합니다.
- BioStation이 서버에 접속을 시작하면 인증서를 발급합니다.
BioAdmin 클라이언트를 사용한다면 인증 대기 중인 단말기에 대해서 마우스 오른쪽 버튼을 클릭한 뒤 '장치 등록'을 선택합니다.
- 인증서가 정상적으로 발행되어 BioStation에 저장 되었다면 BioStation은 인증서의 적용을 위해서 재 시작하게 됩니다.

● 이전 데이터의 변환

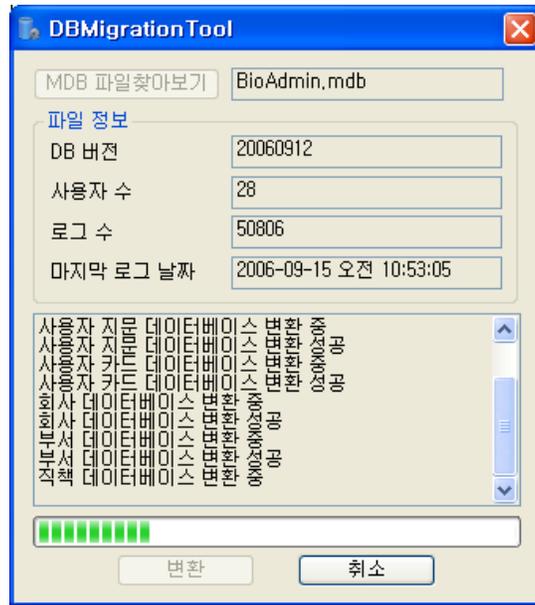
DB 설정이 완료된 뒤에 이미 사용 중이던 3.X버전의 BioAdmin이 있을 경우에는 필요한 데이터를 변환하는 작업이 필요합니다. 이전의 데이터가 필요 없는 경우에는 '닫기'를 눌러 다음으로 진행합니다.



기존에 사용하던 BioAdmin.mdb 파일이 있을 경우 선택해 줍니다.



변환 버튼을 클릭하면 (D) 절에서 설정한 DB에 기존에 사용하던 데이터를 변환하여 저장하기 시작합니다. 데이터를 변환하기 이전에 저장되어 있는 데이터는 삭제되기 때문에 이를 원치 않을 경우에는 먼저 백업을 작성해 둘 것을 권장합니다. 이 작업에는 데이터의 양에 따라서 몇 분 ~ 몇 십분 정도 시간이 소요될 수 있습니다.



변환이 완료되면 **확인**을 눌러 변환 과정을 종료 합니다.

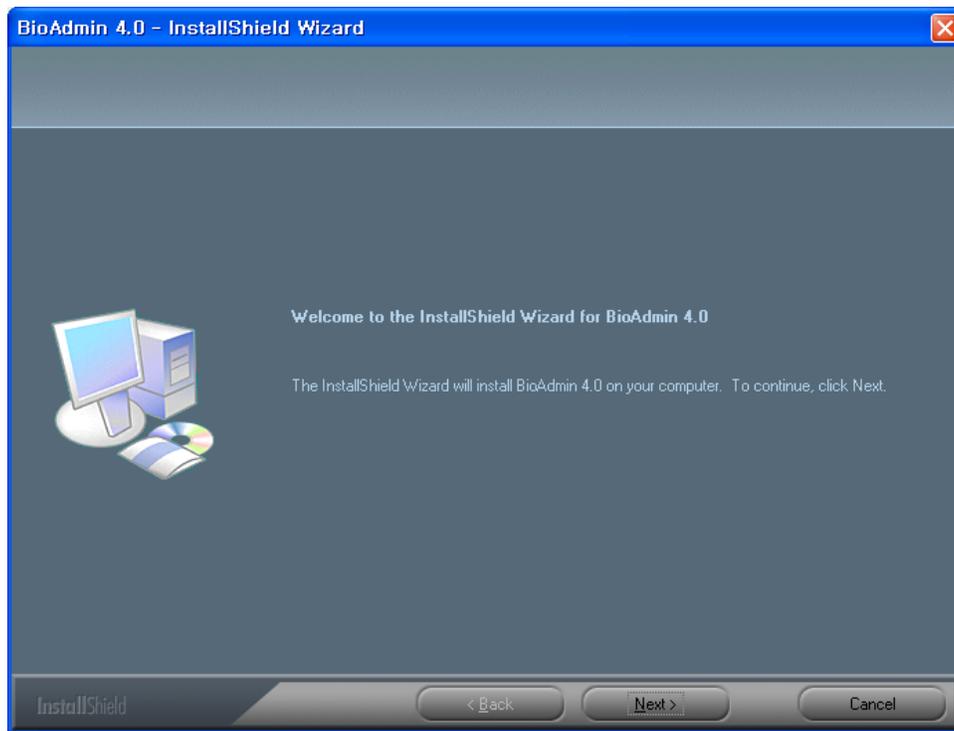
- **설치 완료**

설치가 완료되었습니다. Windows 2000 이상의 운영체제를 사용하는 경우 백그라운드 서비스로 BioAdmin 서버의 구동이 시작됩니다. 이후 PC의 전원을 켜다면 특별한 조치를 하지 않는 한 항상 동작하게 됩니다.

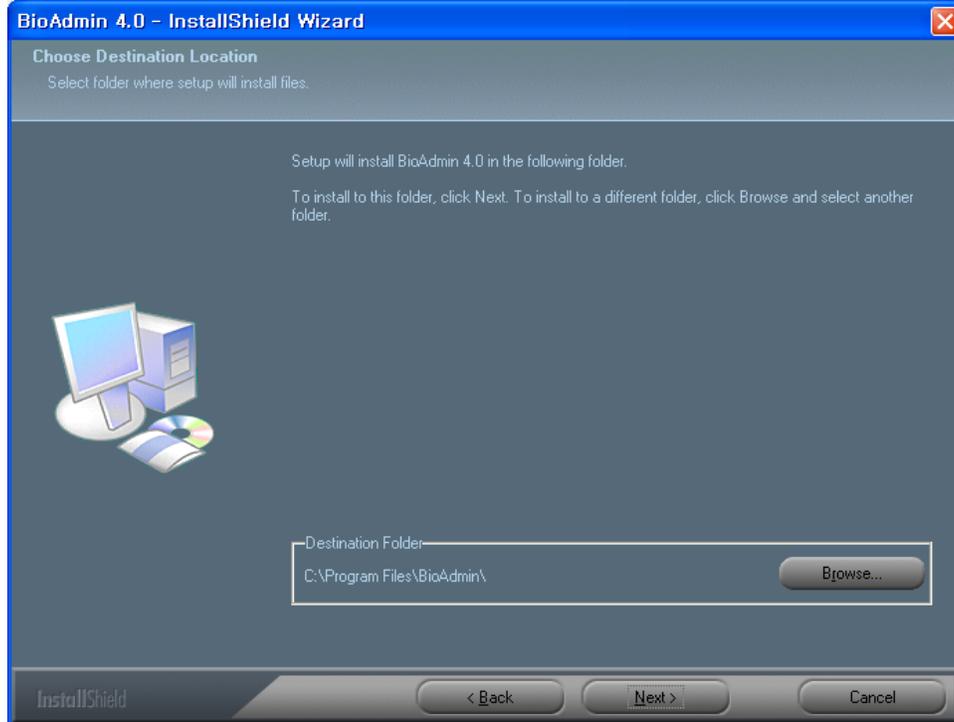
1.4.2. 클라이언트 설치 하기

클라이언트 프로그램은 서버로 사용 중인 PC를 포함, 서버에 접속할 수 있는 환경을 가진 PC라면 큰 제한 없이 설치가 가능합니다. 클라이언트의 설치에는 다음 절차를 진행해 주십시오.

- **설치를 시작합니다.**



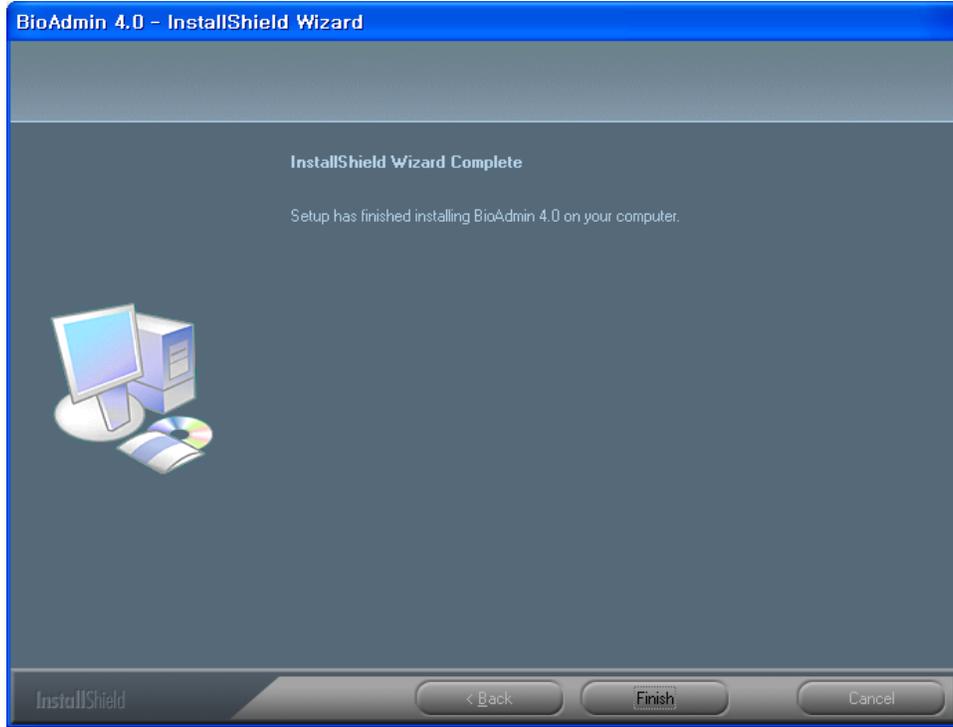
- 설치 경로 설정



클라이언트가 설치될 하드 디스크 드라이브 상의 경로를 선택합니다. 기본은 C:\Program Files\BioAdmin\ 입니다. 이 후 필요한 파일들을 설치 디스크로부터

터 PC로 복사를 시작합니다.

- 설치 완료



설치가 완료되었습니다. 설치 프로그램을 종료하고 BioAdmin 클라이언트 프로그램을 실행할 수 있습니다.

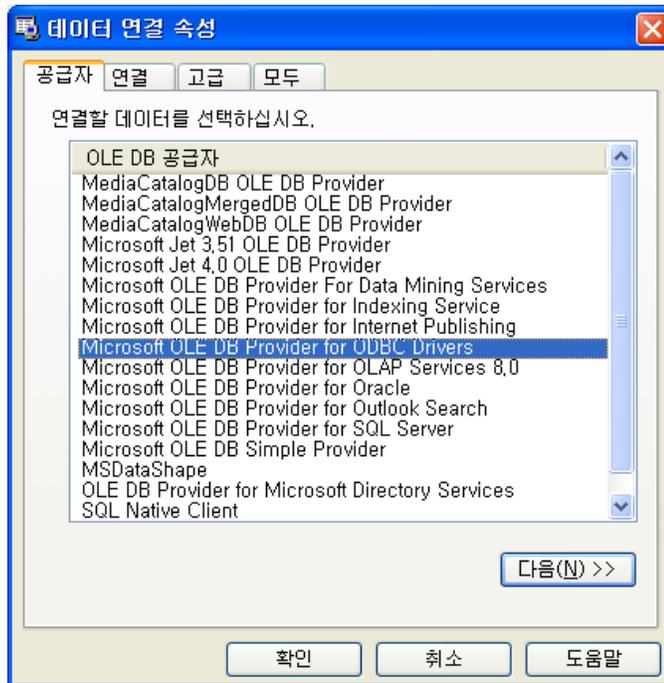
1.4.3. 별도 DB의 설정

서버에서 사용할 데이터베이스를 변경하는 경우 다음 절차를 진행해 주십시오.

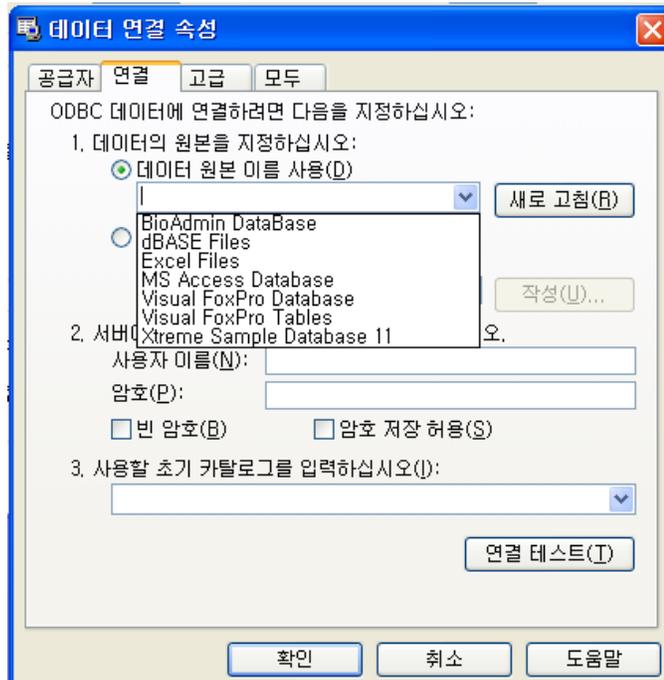
- MySQL을 사용하기

이미 사용중인 MySQL 서버가 있다면 BioAdmin 서버의 내장된 데이터 베이스를 사용하는 대신에 MySQL 서버를 사용할 수 있습니다.

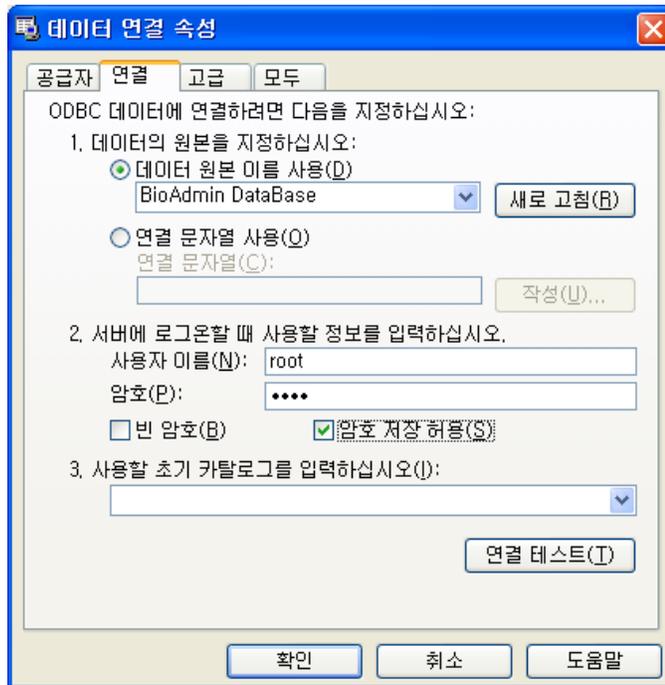
- BioAdmin 서버 설정을 실행하십시오.
- 데이터베이스의 **설정** 버튼을 클릭하십시오.
- 데이터 연결 속성 윈도우가 나타납니다. **Microsoft OLE DB Provider for ODBC Drivers** 항목을 선택하고 다음을 클릭합니다.



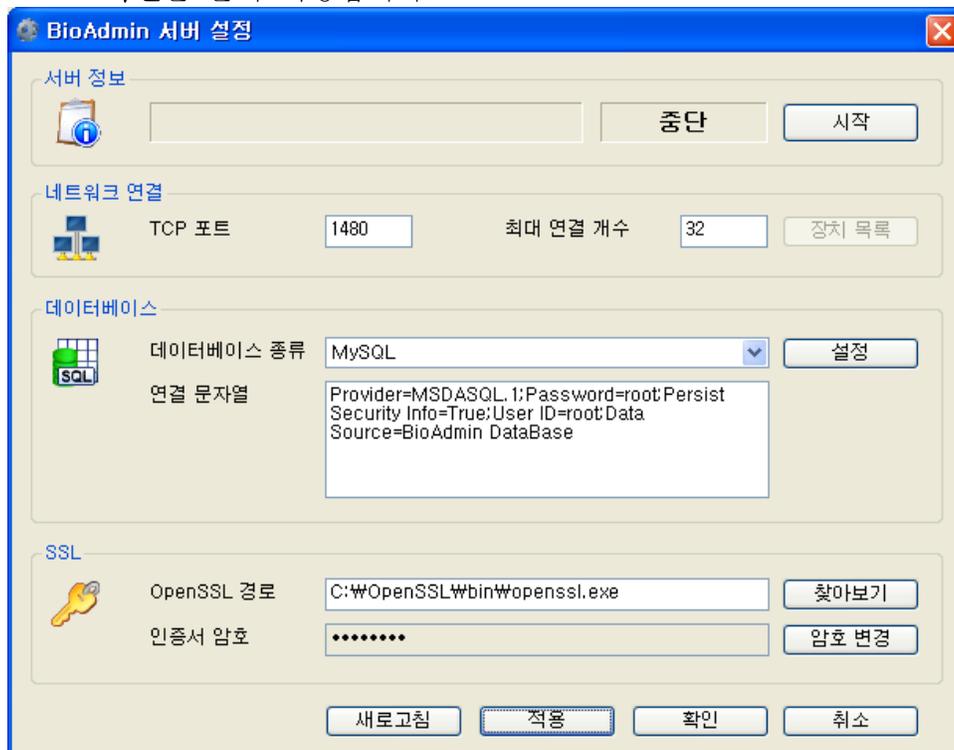
- ODBC 데이터 연결이 있다면 해당 연결을 선택합니다.



- DB 서버를 사용할 사용자 이름 및 암호를 입력합니다. 이때, 암호가 없다면 빈 암호에, 암호가 있다면 '암호 저장 허용'에 체크하여 주십시오



- 연결 테스트를 눌러 제대로 설정 되었는지 확인합니다.
- 확인을 눌러 저장합니다.



- 데이터 베이스 종류를 **MySQL**을 선택하십시오.

- MySQL 서버에 사용할 DB가 생성되어 있다면 **BioAdmin** 서버 설정에서 적용을 누른 뒤 서버를 중지 후 다시 시작합니다.

BioAdmin 서버 설정

서버 정보



네트워크 연결

 TCP 포트 최대 연결 개수

데이터베이스

 데이터베이스 종류 MySQL

연결 문자열
 Provider=MSDASQL.1;Password=root;Persist Security Info=True;User ID=root;Data Source=BioAdmin DataBase

SSL

 OpenSSL 경로

인증서 암호

BioAdmin 서버 설정

서버 정보

 **BioAdmin Server V4.3 (210.219.240.10)**

네트워크 연결

 TCP 포트 최대 연결 개수

데이터베이스

 데이터베이스 종류 MySQL

연결 문자열
 Provider=MSDASQL.1;Password=root;Persist Security Info=True;User ID=root;Data Source=BioAdmin DataBase

SSL

 OpenSSL 경로

인증서 암호

- 서버의 동작 상태가 **시작됨**으로 변경된 것을 확인한 뒤 **확인**을 클릭하여 설정을 종료합니다.

● SQL 서버를 사용하기

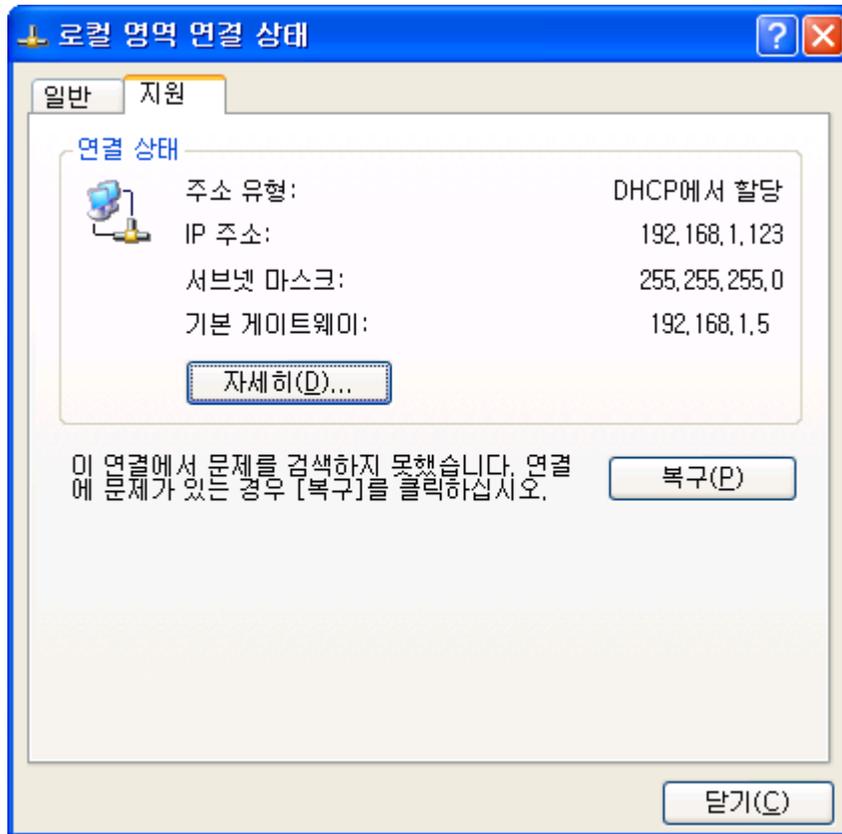
이미 사용중인 MS-SQL 서버가 있다면 BioAdmin 서버의 내장된 데이터 베이스를 사용하는 대신에 SQL 서버를 사용할 수 있습니다. 설정을 하기 전에 사용할 데이터 베이스를 먼저 생성하는 작업을 실행해야 합니다.

- **BioAdmin** 서버 **설정**을 실행하십시오.
- 데이터베이스의 **설정** 버튼을 클릭하십시오.
- **데이터 연결 속성** 윈도우가 나타납니다.
- **Microsoft OLE DB Provider for SQL Server** 항목을 선택하고 '다음'을 클릭합니다.
- SQL 서버 이름을 입력합니다.
- DB 서버를 사용할 사용자 이름 및 암호를 입력합니다. 이때, 암호가 없다면 **빈 암호**에, 암호가 있다면 **암호 저장 허용**에 체크하여 주십시오
- 서버에서 데이터베이스를 선택합니다. 이 항목을 위해서 SQL 서버에서 먼저 사용할 데이터 베이스를 생성해 놓으셔야 합니다.
- **연결 테스트**를 눌러 제대로 설정 되었는지 확인합니다.
- **확인**을 눌러 저장합니다.
- 데이터 베이스 종류를 **SQL Server**를 선택하십시오.
- **BioAdmin** 서버 **설정**에서 **적용**을 누른 뒤 서버를 중지 후 다시 시작합니다.
- 서버의 동작 상태가 **시작됨**으로 변경된 것을 확인한 뒤 **확인**을 클릭하여 설정을 종료합니다.

1.4.4. 소프트웨어 설치 확인

● 네트워크의 구성

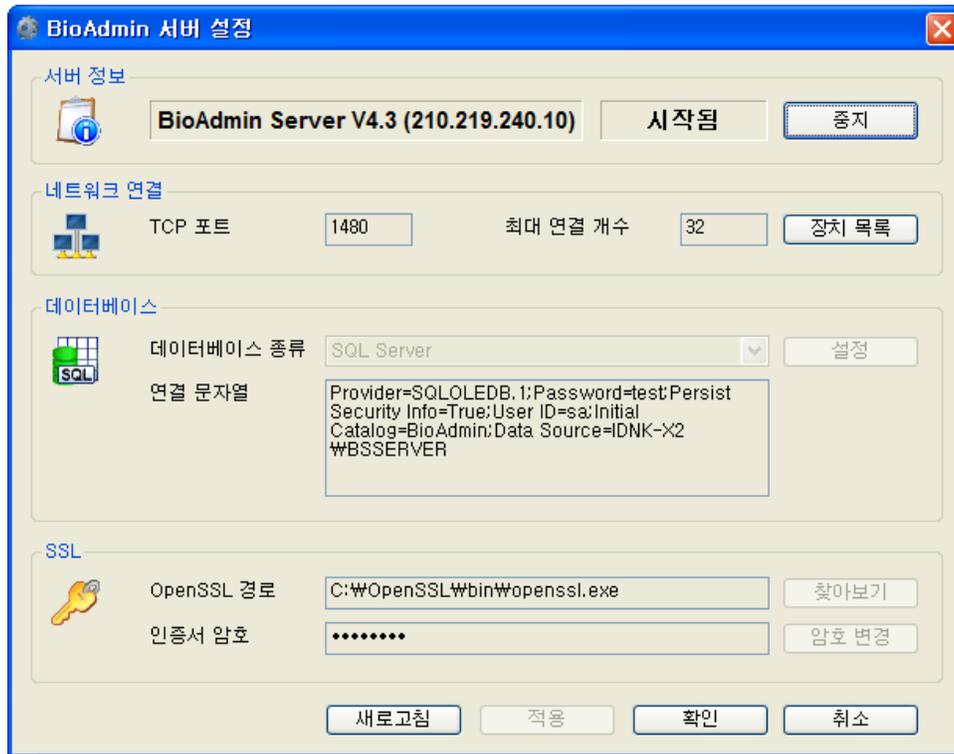
BioStation의 네트워크 메뉴에서 서버를 사용하도록 설정합니다. 서버가 설치된 PC의 IP의 경우 네트워크 관리자에게 문의하거나 운영체제의 네트워크 연결 페이지에서 확인이 가능합니다. 보다 자세한 BioStation의 설정은 BioStation 설치 가이드를 참조해 주십시오.



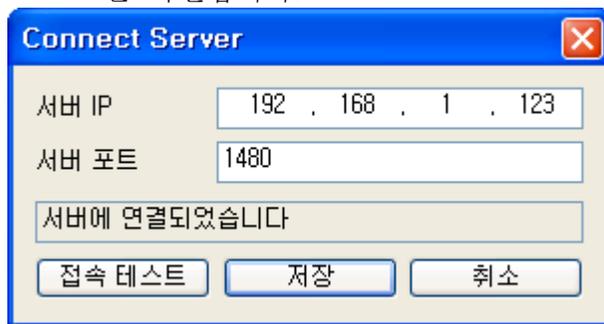
- BioStation의 설정을 변경한 뒤 수 분이 지나면 BioStation으로부터 BioAdmin 서버로 접속을 시도합니다.
- BioAdmin 서버 설정 화면의 '장치 목록'을 통해서 확인할 수 있습니다.
- 이 상태는 접속은 완료했지만, 아직 BioAdmin 서버가 BioStation을 관리하고 있지는 않은 상태입니다. 인증서를 발급하는 과정을 통하면 BioAdmin 서버와 BioStation간의 연결 작업은 완료 됩니다.
- 연결 작업이 완료된 이후에는 BioAdmin 서버가 BioStation으로부터 필요한 정보를 다운로드 합니다. 이 작업에는 BioStation에 저장된 데이터의 양에 따라 수 분 ~ 수십 분이 소요될 수 있으며, 이 동안에는 BioAdmin 클라이언트에서 해당 BioStation을 원활히 제어하지 못할 수도 있습니다.

● 구동 확인

BioAdmin 서버 및 BioAdmin 클라이언트를 모두 설치하였다면 BioAdmin 서버 설정 프로그램을 통해서 현재 서버의 상태를 확인 합니다.



- BioAdmin 서버의 버전 및 상태를 확인한 뒤에 설치된 BioAdmin 클라이언트를 실행하여 서버 IP 및 포트를 입력한 뒤 접속 테스트를 통하여 상태를 확인합니다.

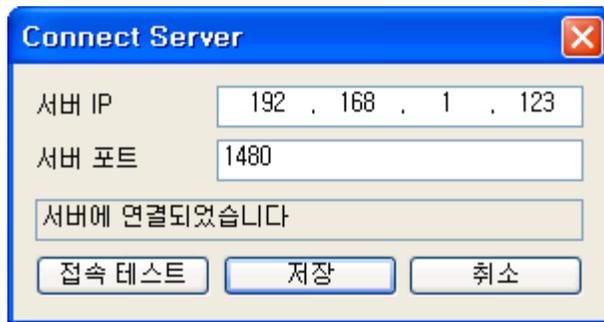


- 서버와 접속이 잘 이루어 진다면 BioAdmin 서버 및 BioAdmin 클라이언트의 사용 준비가 완료 되었습니다.

Note : 간혹 정상적으로 서버가 설치 되었음에도 불구하고, 서버에 연결이 되지 않는 경우가 있습니다. 이때는 서버를 종료 후 재실행 해 주시면 연결이 됩니다.
 서버를 종료하기 위해서는 윈도우의 '시작' 버튼을 눌러 '프로그램' 목록의 'BioAdmin Server' 항목 내에 'Uninstall BioAdmin server service' 를 클릭합니다. 화면 상에는 아무런 변화가 없지만, 서버가 종료된 상태로써, 재실행을 위해 같은 위치에 있는 'Install BioAdmin server service' 를 클릭합니다.

1.5. BioAdmin 에 로그인 하기

1.5.1. 서버에 접속

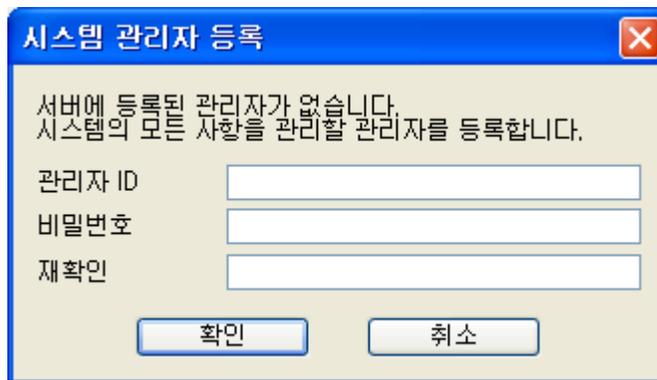


The image shows a 'Connect Server' dialog box with a blue title bar and a close button (X) in the top right corner. It contains the following fields and buttons:

- 서버 IP: 192 . 168 . 1 . 123
- 서버 포트: 1480
- 서버에 연결되었습니다 (Server connected message)
- Buttons: 접속 테스트 (Connect Test), 저장 (Save), 취소 (Cancel)

- 서버 IP 와 서버포트를 입력합니다.
- 접속 테스트 버튼을 눌러 서버와 접속 가능한 상태인지 확인할 수 있습니다.
- 저장 버튼을 누르면 설정한 서버 정보를 저장한 동 서버에 접속합니다.

1.5.2. 초기 시스템 관리자 등록

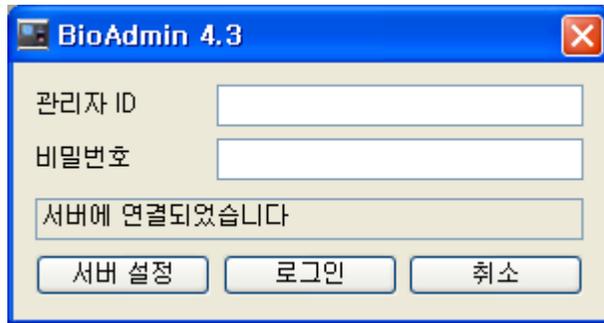


The image shows a '시스템 관리자 등록' (System Administrator Registration) dialog box with a blue title bar and a close button (X) in the top right corner. It contains the following fields and buttons:

- 서버에 등록된 관리자가 없습니다. 시스템의 모든 사항을 관리할 관리자를 등록합니다. (No administrator is registered on the server. Register an administrator to manage all system matters.)
- 관리자 ID: [Empty text box]
- 비밀번호: [Empty text box]
- 재확인: [Empty text box]
- Buttons: 확인 (Confirm), 취소 (Cancel)

- 관리자 ID와 패스워드 입력 후 확인 버튼을 누릅니다. 이때 ID 와 패스워드는 관리자 임의대로 설정하면 됩니다.
- 초기 시스템 관리자 등록은 서버를 설치한 후에 처음으로 BioAdmin 소프트웨어에 접속할 때 초기의 관리자 계정을 만드는 작업입니다. 따라서, 초기 시스템 관리자를 한 번 등록 하고 난 이후에 다시 BioAdmin 소프트웨어에 접속할 때에는 이 작업을 하지 않고 곧바로 BioAdmin 소프트웨어로 로그인 할 수 있습니다.

1.5.3. BioAdmin 소프트웨어에 로그인



- 관리자 ID 와 패스워드를 입력 한 후 로그인 버튼을 눌러 BioAdmin 소프트웨어에 로그인 합니다.
- 1.5.2 에서와 같이 초기 시스템 관리자를 등록하고 난 후 처음으로 BioAdmin 소프트웨어에 로그인 할 때에는 초기 시스템 관리자 등록 시 사용했던 ID 와 패스워드로 BioAdmin 소프트웨어에 로그인 할 수 있습니다.
- 서버 설정 버튼을 누르면 설정된 서버 정보를 보거나 이를 수정할 수 있습니다.

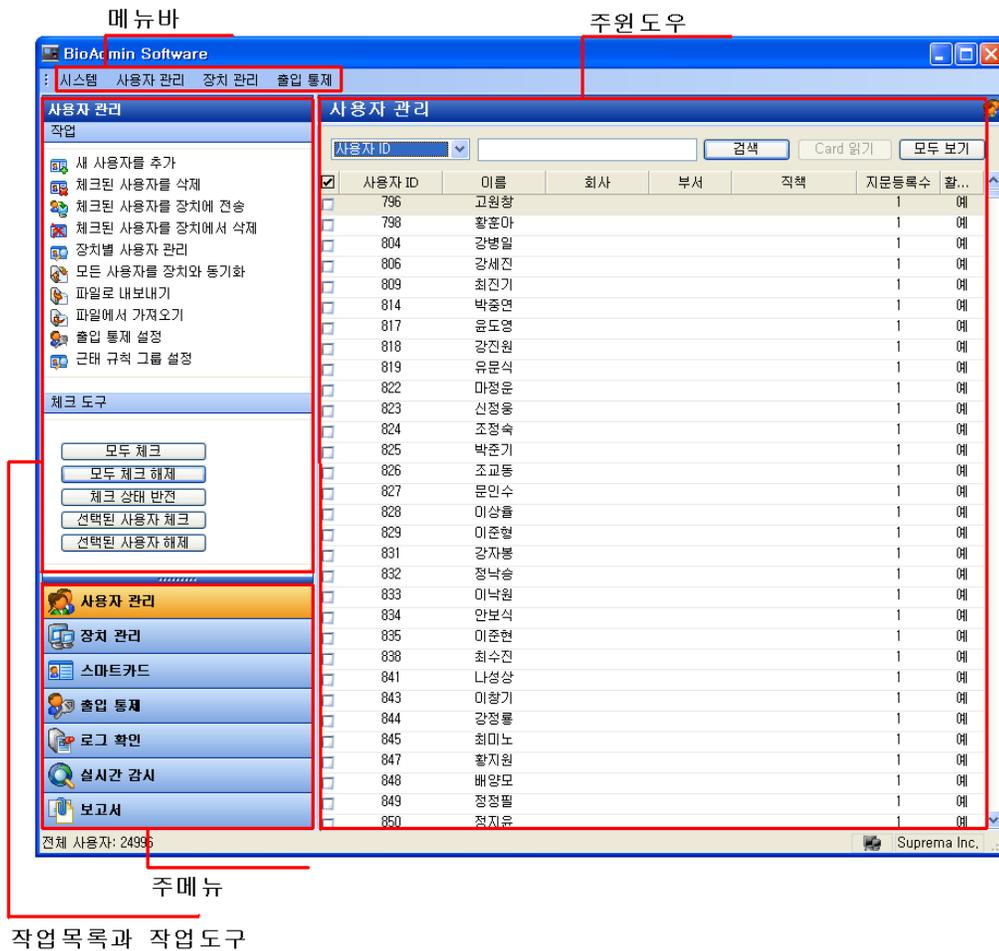
1.6. BioAdmin 사용자 별 권한

BioAdmin 소프트웨어를 사용할 수 있는 사용자는 그 권한에 따라 관리자, 열람 사용자, 일반 사용자로 나누어 집니다.

- 관리자: BioAdmin 소프트웨어의 모든 항목을 설정 및 열람할 수 있는 사용자 입니다.
- 열람 사용자: BioAdmin 소프트웨어의 모든 항목을 열람할 수 있는 사용자 입니다. 열람 사용자는 각종 항목을 설정하거나 변경할 수는 없으며, 설정된 값을 열람만 할 수 있습니다.
- 일반 사용자: 자기 자신의 로그 정보만을 확인할 수 있는 사용자 입니다. BioAdmin 소프트웨어에 지문이나, 아이디가 등록된 사용자들 중, 비밀번호를 설정한 사용자는 자신의 ID 및 비밀번호를 사용하여 로그인 할 수 있으며, 본인의 로그 내용 및 보고서 내용을 확인할 수 있습니다.

1.7. BioAdmin 구성

BioAdmin 소프트웨어는 메뉴 바, 주 메뉴, 작업목록과 도구목록, 그리고 주 윈도우 4개 요소로 구성되어 있습니다.



작업목록과 작업 도구

1.7.1. 메뉴 바

메뉴 바는 BioAdmin 소프트웨어가 지원하는 명령어 항목들을 포함하는데 이들은 4개 카테고리로 분류됩니다:

- 시스템: 관리자 계정 관리, 자료백업 / 자료복구, 모든 장치 잠금 / 모든 장치 잠금 해제, 1.x 버전 자료 가져오기, 옵션, BioAdmin 정보, 종료
- 사용자 관리: 새 사용자 추가, 회사명 관리, 부서명 관리, 직책 명 관리와 사용자 항목 설정.
- 장치 관리: 새 장치 추가, 새 컨트롤러 추가, 시간 설정, 펌웨어 업그레이드, 패스워드 초기화 코드 가져오기/ 패스워드 초기화, 사이트 키 설정
- 출입 통제: 시간대 설정, 휴일 군 설정, 출입 시간 설정, 출입 구역 설정과 출입 그룹 설정.

1.7.2. 주 메뉴

사용자 관리, 장치관리, 스마트카드, 출입 통제, 실시간 감시, 로그 확인, 보고서 와 같은 주요 메뉴는 왼쪽 창 아래 버튼으로 액세스 할 수 있습니다.

1.7.3. 작업 목록과 도구 목록

작업 윈도우는 선택된 주 메뉴의 부메뉴들을 보여줍니다.

도구 윈도우는 사용자 선택 도구, 장치 트리 와 로그 부분 선택 도구들을 보여줍니다.

1.7.4. 주 윈도우

각 메뉴에 대응하는 정보가 주 윈도우에서 갱신됩니다. 주 윈도우에는 다음의 정보와 컨트롤이 포함됩니다.:

- 현재 선택된 장치로부터 검색된 정보
- 사용자 데이터베이스나 로그 데이터와 같은 호스트 PC에 저장된 정보
- 정보를 운영하거나 설정하는 컨트롤

1.8. 사용자 데이터베이스

사용자 데이터베이스는 사용자 ID, 사용자 이름, 지문정보 등을 포함하는 사용자 정보 일체를 말합니다. BioAdmin 소프트웨어는 사용자 데이터베이스를 중점적으로 관리하는 것에 기반을 두고 있습니다.

즉, 사용자 데이터베이스가 생성되고, 갱신되고 호스트 PC에 저장됩니다. 그리고 나서 전송을 통해 네트워크에 연결된 BioEntry 와 BioStation 장치들에게 선택적으로 분배됩니다.

Note : 선택과 체크의 구분 - 선택은 선택도구 박스에서 사용자ID 앞의 각각의 사용자를 선택할 때 (즉, Shift 버튼을 누른 후 화살표 ↓를 사용해서 사용자를 선택 또는 Shift 버튼을 누른 후 마우스로 마지막 사용자 ID를 클릭하면 다수의 사용자를 선택하실 수 있습니다.) 사용하는 단어이며, 체크는 각각의 선택된 사용자ID를 체크하는 것을 말합니다. 체크도구를 통해 모두 체크, 모두체크 해제, 체크상태 반전, 선택된 사용자 체크, 선택된 사용자 해제의 작업을 손쉽게 사용할 수 있습니다.

2. 시작하기 전에 결정할 사항

2.1. 바이오 정보 보호 가이드 라인

바이오 정보 보호 가이드 라인은 지문이나 홍채 인식 등의 바이오인식 시장이 급격하게 확대됨에 따라 개인의 바이오정보와 인권의 보호를 위해 2007년 9월 정보통신부와 한국정보보호진흥원에서 정하고, 이를 준수하도록 보호원칙을 제시하였으며, 이에 따라 지문인식 시스템을 운영하는 것을 권장합니다

바이오 정보 보호 가이드 라인은 관리자가 선택하여 시스템에 적용할 수 있으며, 이 옵션을 사용하게 되면 호스트 PC 와 BioStation 및 BioEntry Plus에 저장하는 사용자 지문 데이터를 사용자가 정의한 암호화 키를 사용하여 암호화 한 후 저장합니다. 지문에서 추출한 특징 데이터의 템플릿 자료를 암호화 함으로서 한층 강화된 보안 수준을 실현할 수 있습니다.

자세한 사항은 11.1.7 옵션절의 보안옵션 항목을 참고 하십시오.

바이오 정보 보호 가이드 라인에 대한 자세한 정보는 한국정보보호진흥원 홈페이지 (KISA 홈페이지 <http://www.1336.or.kr>) 에서 확인할 수 있습니다.

2.2. 지문 옵션

BioEntry Pass™/BioEntry Smart™, BioStation™, BioEntry Plus™ 단말기에 ISO 19479-2 표준 템플릿 지원이 추가되었습니다.

이 옵션은 사용 중인 단말기의 사용자 정보가 없는 상태에서만 변경이 가능하며, BioAdmin™에서도 저장되어 있는 템플릿을 모두 삭제한 뒤에 옵션을 적용하게 됩니다.

자세한 사항은 11.1.7 옵션절의 지문 옵션 항목을 참고 하십시오.

2.3. 출입 그룹 설정

BioAdmin V4.1부터 BioStation™ 과 BioEntry Plus™에 대해서 새로운 형식의 Access Control 정보를 사용할 수 있습니다. 이전 버전의 출입 통제의 경우 BioEntry Plus™를 지원하지 않기 때문에 출입 통제 방식을 어떤 버전을 사용할 것인지 충분히 고려하여 결정해야 합니다. 일단 새로운 버전의 Access Control 설정을 사용하게 되면 이전 버전은 사용할 수 없게 됩니다.

단, BioEntry Pass™ / BioEntry Smart™의 경우에는 새로운 버전의 Access Control 설정을 사용해도 적용되지 않습니다.

출입 통제 설정과 관련하여 11.1.7 옵션 절의 버전 관리 항목을 참고 하십시오. 또한, Access Group의 설정과 관련된 사항은 7. 출입 통제 절을 참고 하십시오.

2.4. Mifare 카드 사용

BioStation Mifare 모델과 BioEntry Plus Mifare 모델은 1K / 4K Mifare Card를 지원 합니다. 이는 BioEntry Smart에 사용되는 Smart Card와 호환되지 않으며 사용 전 설정도 약간 차이가 있습니다.

자세한 설정 방법에 대해서는 6. 스마트 카드 / Mifare 카드 항목을 참조 하십시오.

3. 빠른 시작

이 장에서는 외부 시스템과 통합된 BioEntry, BioEntry Plus 와 BioStation 장치를 작동시키는 기본적인 과정에 대해서 설명합니다.

3.1. BioStation 과 함께 빠른 시작

이 절에서는 BioStation 을 작동시키는 기본적인 과정에 대해 기술하고 있습니다.

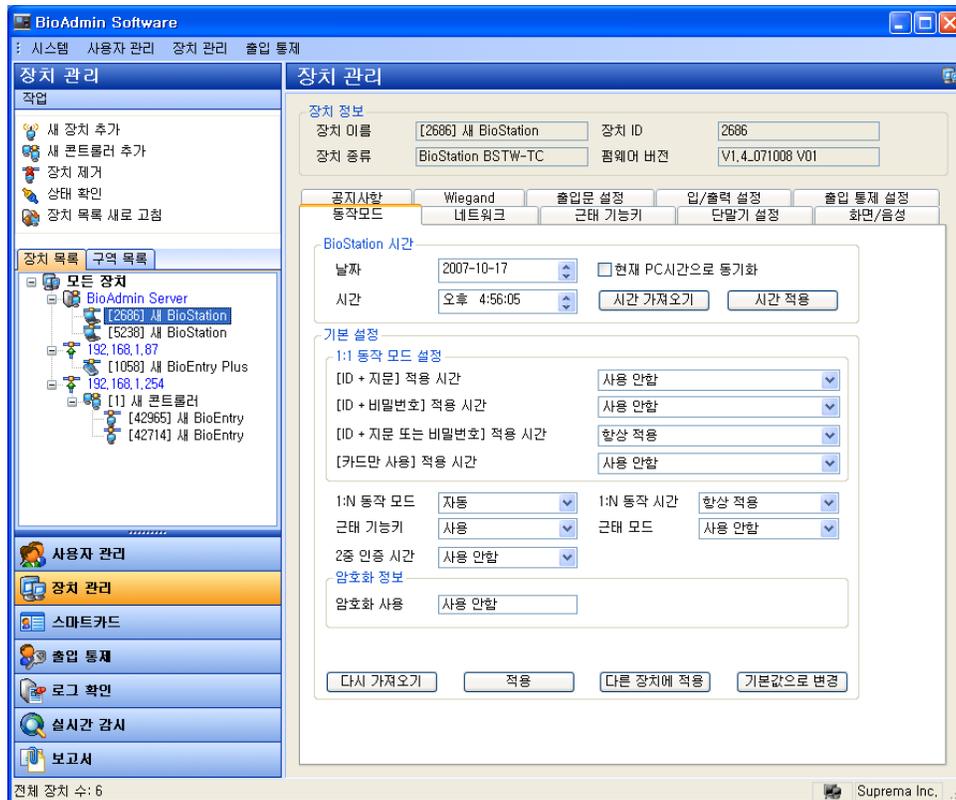
3.1.1. 1단계 : 하드웨어 설치

BioStation 은 유,무선 랜을 이용하여 네트워크를 설정할 수 있습니다. 나아가, Serial 통신을 통하여 RS232,422,485 통신을 설정할 수 있으며, USB 인터페이스를 통해 호스트 PC와 연결할 수 있습니다.

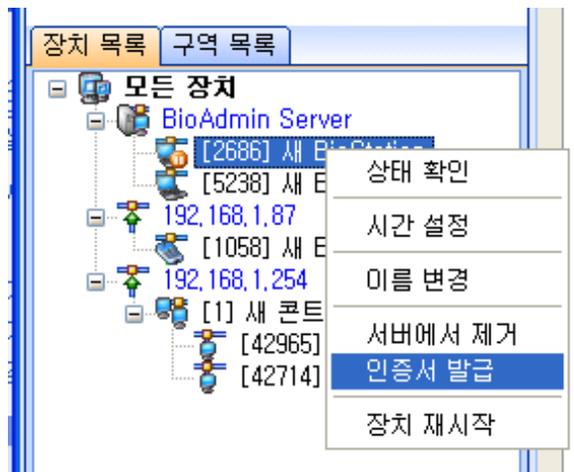
설치에 관한 상세한 정보는 BioStation 설치 안내서를 참조하시기 바랍니다.

3.1.2. 2단계 : 새 장치 검색

- BioAdmin 소프트웨어를 실행합니다.
- 관리자 ID와 패스워드를 입력합니다.
- 주 메뉴상에서 **장치관리**를 선택하면 주 윈도우에 장치 관리 페이지가 나타납니다.

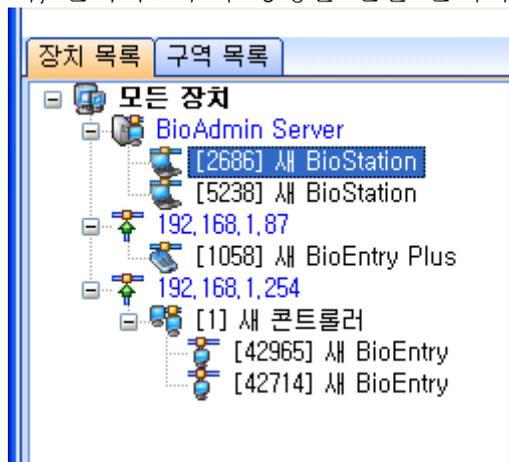


- 서버에 접속된 BioStation들은 BioAdmin을 시작할 때 자동으로 목록에 추가되며, '장치 목록 새로 고침'을 선택해도 새로 연결된 장치를 볼 수 있습니다. BioStation을 서버에 접속하도록 설정했다 하더라도, 서버에 실제로 연결이 완료되어 목록에 보이기 까지는 몇 분 정도 시간이 걸릴 수 있습니다.
 - 인증되지 않은 BioStation: BioStation의 아이콘에 오렌지 색으로 일시 정지 표시가 나타나며, 현재 BioStation으로 데이터를 전송하거나 받을 수 없음을 나타냅니다.



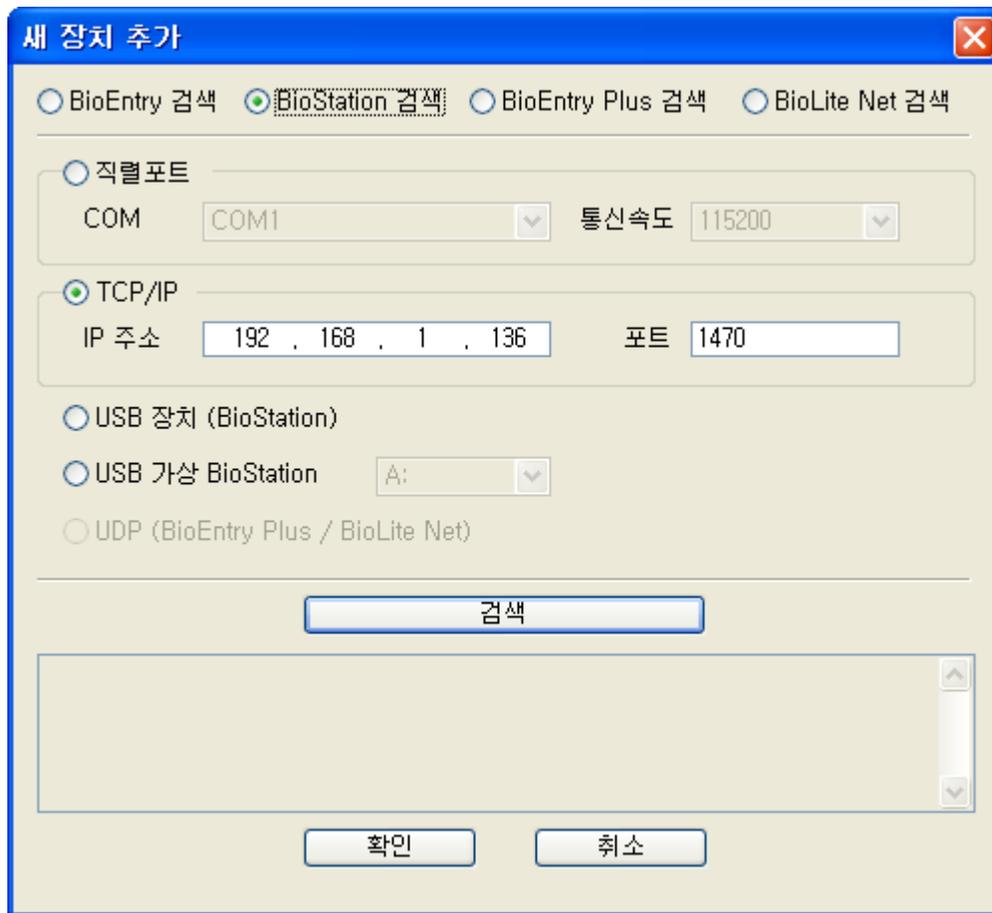
해당 BioStation에서 마우스 우 버튼을 클릭하여 ‘인증서 발급’ 메뉴를 통해 인증서를 발급한 뒤에 정상적으로 사용할 수 있게 됩니다. 단, 인증서를 발급한 뒤에는 BioStation이 재 시작되므로 목록에 표시되기 까지 몇 분 정도 시간이 소요됩니다.

- 인증된 BioStation: BioAdmin Server에 접속된 BioStation의 아이콘에 다른 표시가 없으면 현재 BioAdmin Server와 정상적으로 통신하고 있는 상태이며, 관리자로부터 명령을 받을 준비가 되어 있음을 나타냅니다.

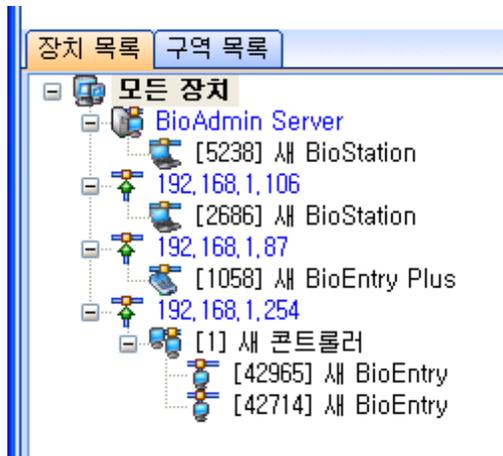


- 새 장치 검색 메뉴를 선택하고, BioStation 검색을 클릭한 뒤 직렬포트와 TCP/IP 그리고 USB장치(BioStation) 중 사용할 통신을 선택한 후에 검색버튼을 누릅니다.

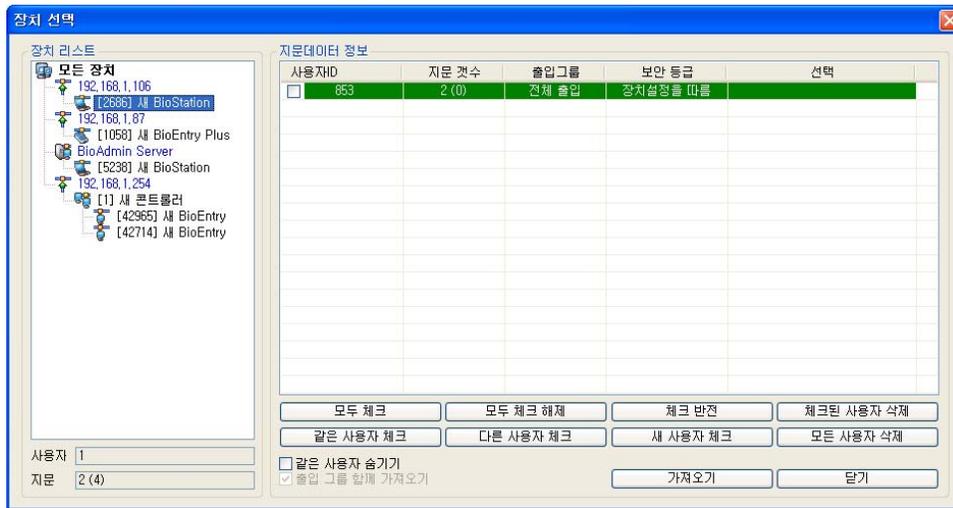
Note : 검색결과에서 장치를 찾게 되면
 예) 192.168.1.101 (port : 1470) 검색 중
 장치발견 : 새 BioStation – 장치번호
 장치 검색을 마칩니다.
 몇 개의 장치가 발견되었습니다. 라는 결과 리포트가 쓰여진 후 확인 버튼을 누르시면 장치가 선택됩니다.



- 장치와 잘 연결되었다면, 새로운 장치 ID와 장치와 연결된 통신방식까지 장치 트리 윈도우에 나타납니다.



- 주 메뉴상의 사용자 관리 버튼을 선택하고 작업 윈도우상에서 장치 별 사용자 관리를 선택합니다.
- 장치를 선택하면 사용자ID, 지문 개수, 출입그룹, 보안등급, 선택 등 지문 데이터 정보가 표시됩니다.

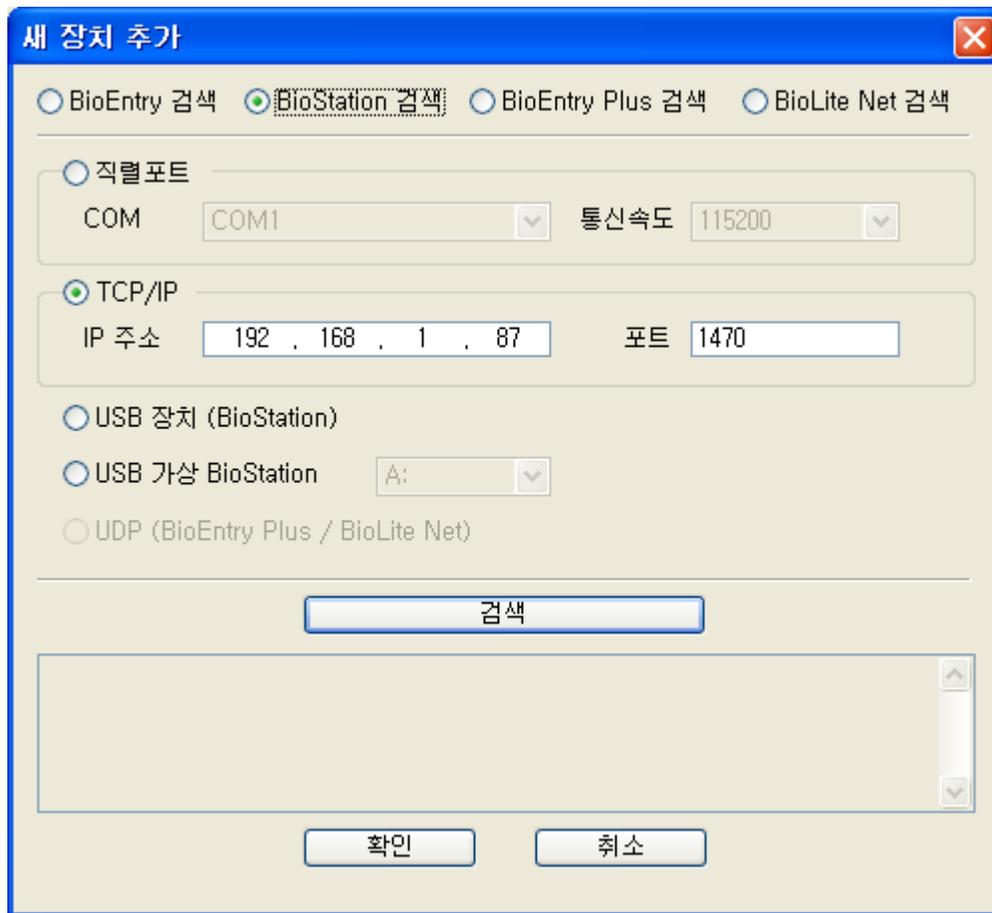


3.1.3. 3단계 : 장치 연결

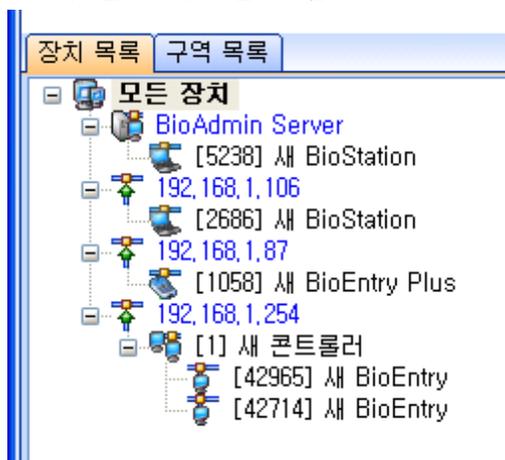
- 장치 관리 메뉴를 선택하면 주 윈도우에 장치 관리 페이지가 나타납니다.

BioAdmin 소프트웨어의 네트워크 설정은 크게 네트워크, 시리얼통신, USB 연결 3가지로 나누어지며, 설정 값을 변경 하며 장치에 설정 값을 적용하도록 합니다.

네트워크 설정은 로컬영역 연결과 무선 네트워크 연결을 위한 설정 값을 지정 하는 것이며, 포트는 1470을 지정하여야 만 합니다.



사용자는 IP 주소와 포트 번호 (1470)를 알아야 합니다. 장치가 올바르게 연결 되면, IP 주소는 한 그룹으로, 장치ID는 장치 트리 윈도우상에서 각 괄호[****]와 함께 나타날 것입니다.



- 무선 네트워크 설정
프리셋 이름, 네트워크 이름 (SSID), 네트워크 인증, 데이터 암호화, 네트워크

크 키 등을 무선 네트워크 설정에서 설정한 후 운영하도록 합니다.

DHCP의 적용으로 BioAdmin에서 자동으로 IP주소 받기 설정하여 장치에서 자동으로 IP주소를 받을 수 있으며, 그 IP주소를 확인하여 장치관리에서 장치를 검색할 수 있습니다.

수동으로 IP 주소 설정 시에는 할당 IP주소 , 게이트웨이 , 서브 넷 마스크를 설정하셔서 장치를 검색할 수 있습니다.

BioStation 무선랜 설정

프리셋 이름: Office

네트워크이름(SSID): BS_AP

무선 네트워크 키

네트워크 인증: WPA_PSK

데이터 암호화: TKIP/AES

네트워크 키: *****

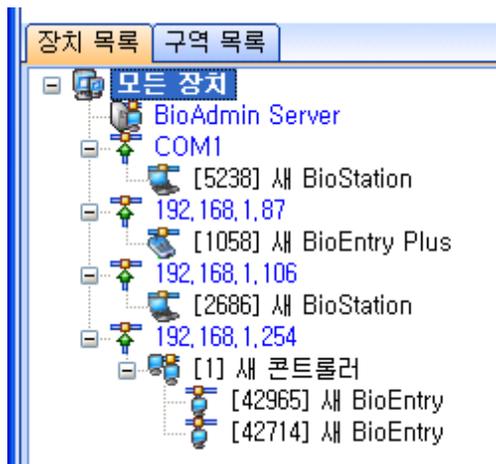
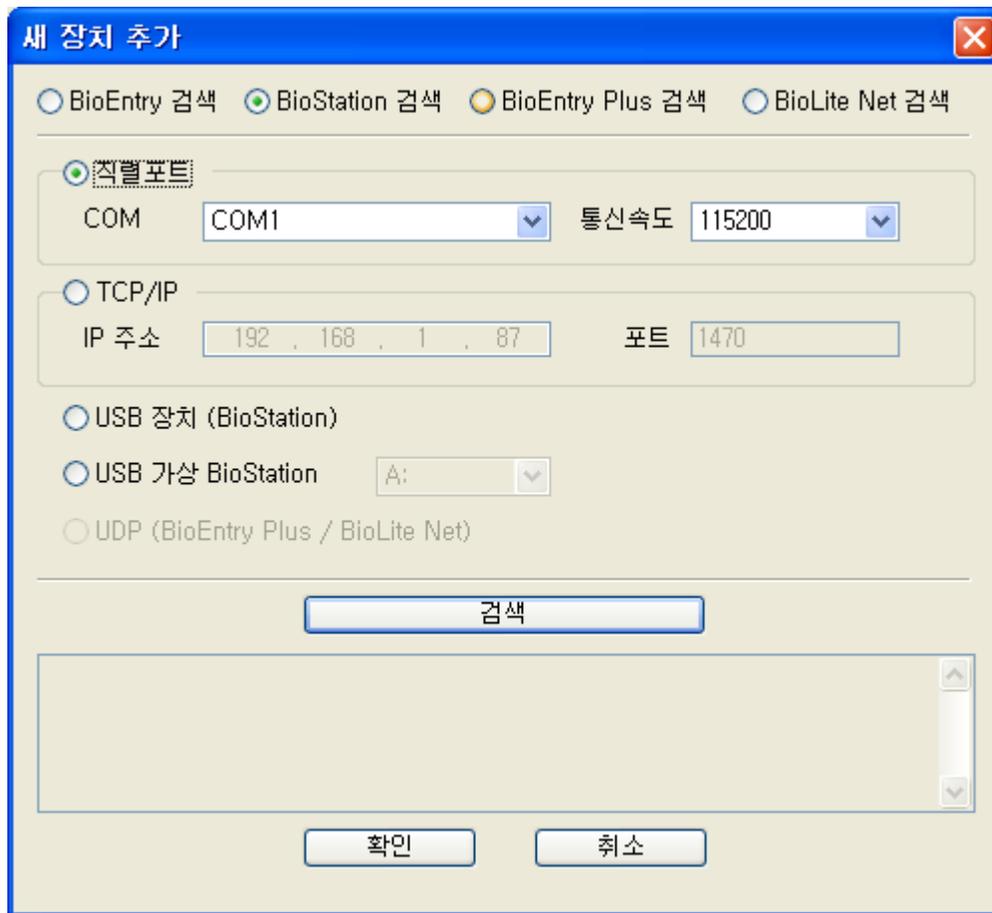
네트워크 키 확인: *****

확인 취소

- Serial 통신

RS422/485 네트워크상에서 새로운 장치가 자동적으로 탐지될 수도 있고 장치 관리에서 새 장치 검색 메뉴에 의해 추가될 수 있습니다. 장치가 네트워크와 올바르게 연결되었다면, 장치 ID가 장치 트리 윈도우상의 포트아래 각괄호 [****] 와 함께 나타날 것입니다.

RS485 / RS232 통신 인터페이스에서 통신속도는 반송파가 1초당 상태를 바꾸는 횟수를 나타냅니다. BioStation 장치와 통신하는데 초기 설정 값으로 115200을 설정하나, 문제가 발생하면, 통신속도를 좀 더 낮은 값으로 바꾸는 것이 해결책이 될 수도 있습니다.

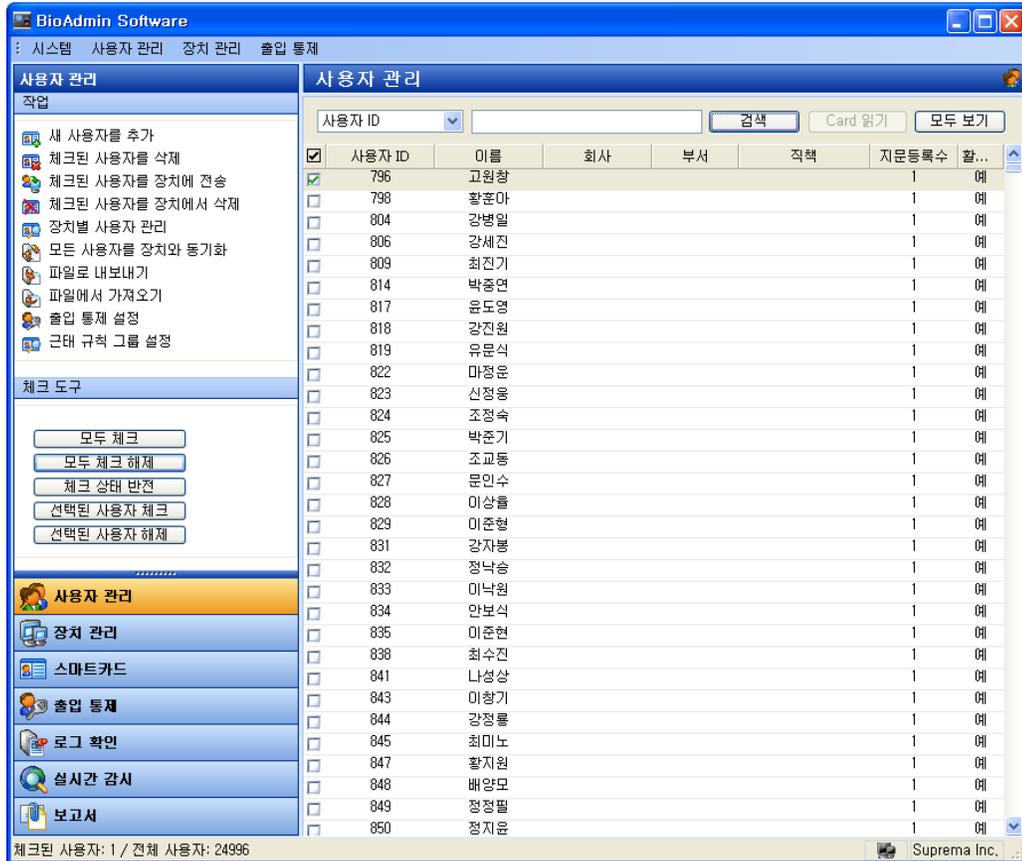


장치가 네트워크로부터 연결 해제된다 해도 장치 리스트 윈도우상에는 남아 있습니다. **장치 제거** 메뉴는 네트워크 윈도우에서 장치를 제거하는데 사용됩니다. 장치의 이름은 **장치이름 변경** 메뉴로 변경할 수 있으며, 장치ID는 하나로 고정되어 변경될 수 없습니다.

3.1.4. 4단계 : 사용자 관리

- 사용자 관리 메뉴를 선택하면 주 윈도우에 사용자 관리 페이지가 나타납니다.

Note : 사용자 관리에서 사용자에게 대한 정보는 기본정보와 지문정보로 나뉘어 이해할 수 있습니다. 기본정보는 사용자ID, 이름, 회사, 부서, 직책, 전화번호 등의 정보이며, 지문정보는 사용자의 지문에 대한 정보입니다.

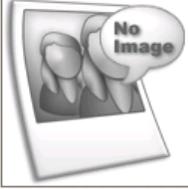


- 작업 윈도우상의 새 사용자를 추가 메뉴를 선택하면 팝업 윈도우가 나타납니다.

사용자 정보 [X]

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

개인 정보


 사용자 ID: 사진 및 개인 인증화면 편집
 이름:
 회사: ...
 부서: ...
 직책: ...

상세정보

전화번호:
 핸드폰:
 이메일:
 성별: ...
 생년월일: ...
 시작일: ...
 만료 일시: 시

출입 통제

출입 상태: 활성화
 그룹 1: ...
 그룹 2: ...
 그룹 3: ...
 그룹 4: ...

인증 제한 (BioStation 전용)

제한 횟수: 회
 인증 간격(분): 분

추가 정보

비밀번호: 사용자 등급: ...

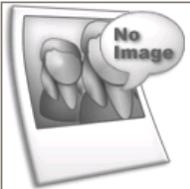
확인 취소

- 사용자 정보 탭에 사용자 정보를 입력합니다.

사용자 정보

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

개인 정보


 사용자 ID: 853 사진 및 개인 인증화면 편집
 이름: 서동석
 회사: 슈프리마 ...
 부서: R&D ...
 직책: 선임연구원 ...

상세정보

전화번호:
 핸드폰:
 이메일:
 성별: 남자 ▼
 생년월일: 1970-06-14 ▼
 시작일: 1970-01-01 ▼
 만료 일시: 2030-12-31 ▼ 0 시

출입 통제

출입 상태: 활성화
 그룹 1: 전체 출입 ▼
 그룹 2: 사용 안함 ▼
 그룹 3: 사용 안함 ▼
 그룹 4: 사용 안함 ▼

인증 제한 (BioStation 전용)

제한 횟수: 0 회
 인증 간격(분): 0 분

추가 정보

비밀번호: 사용자 등급: 일반 ▼

확인 취소

- 콤보 박스를 이용해 회사, 부서와 직책을 선택할 수 있습니다.
- 새로운 회사, 부서 또는 직책 정보를 추가하려면 버튼을 누르거나, 정보 입력 창에 회사, 부서 또는 직책 명을 입력 후 추가 버튼을 누릅니다.
- 추가된 정보를 저장하려면 저장 버튼을 누릅니다.

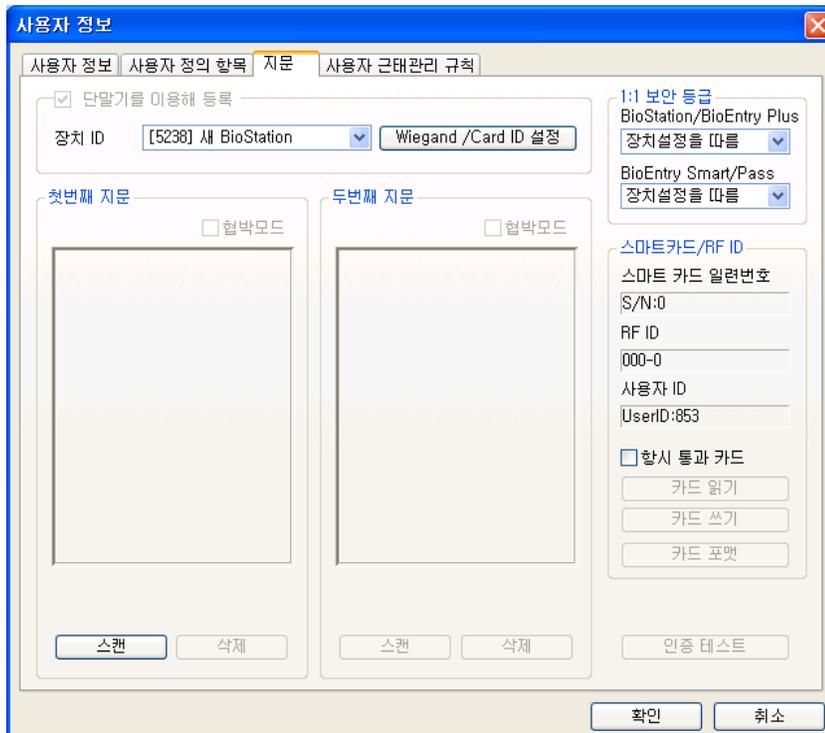
회사명 관리

회사명관리

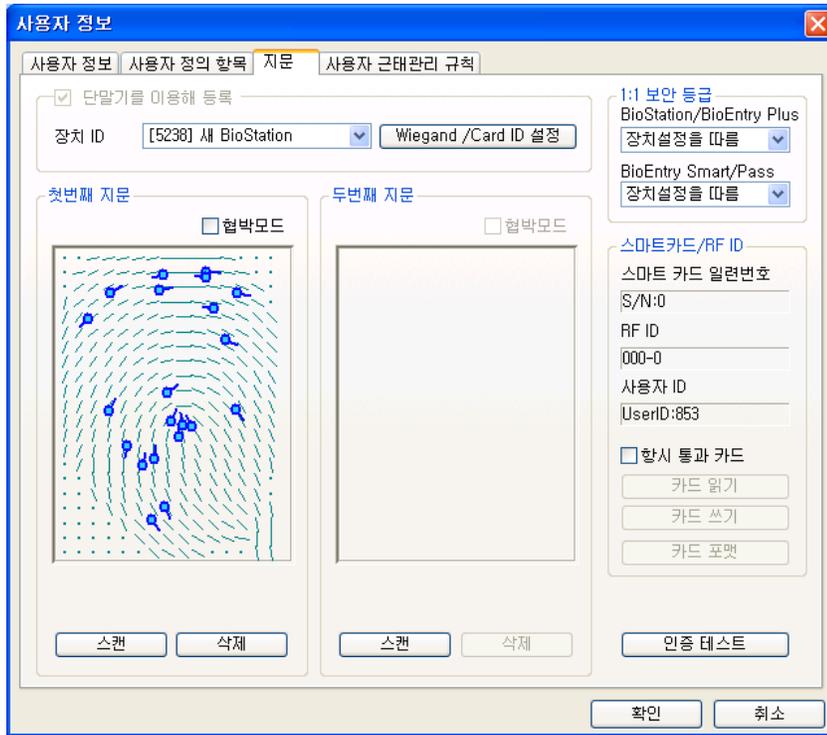
슈프리마

- 상세정보의 전화번호, 핸드폰, 이메일, 성별, 생년월일을 입력할 수 있으며, 사용자 정보 생성일이 등록일로 자동 입력 됩니다. 사용자의 만료일을 설정할 수 있습니다.

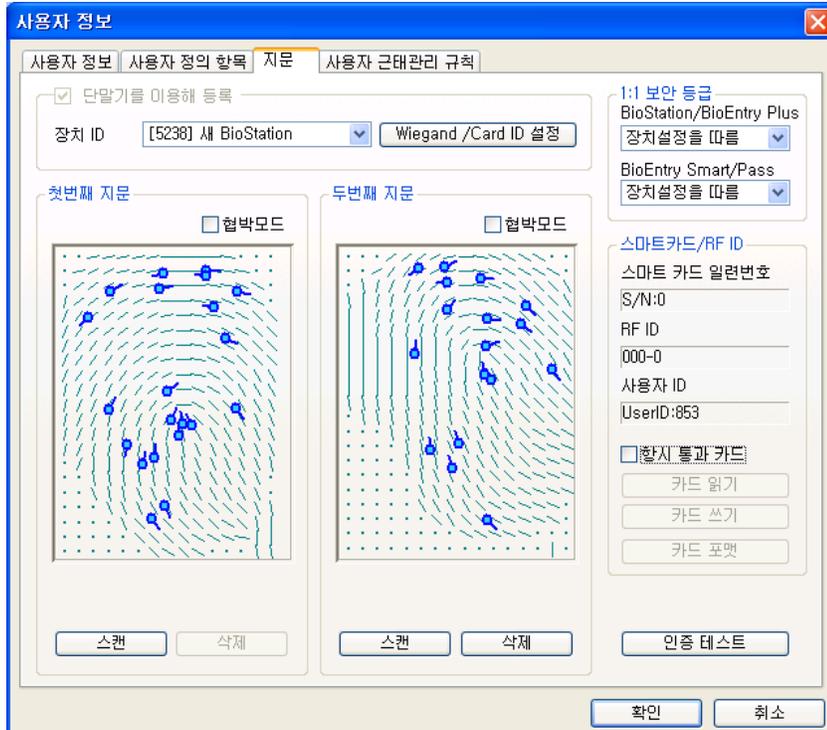
- 개인별 출입통제를 설정하고자 하는 경우, 출입 상태를 활성화 하고 전체출입/전체제한 또는 출입통제 메뉴에서 미리 설정한 출입그룹 중에 하나를 선택합니다.
- 제한횟수는 인증이 가능한 횟수를 제한하고, 인증 간격을 설정 하는 경우, 한번의 인증 후 설정된 시간이 지나야만 다시 인증이 가능합니다.
- 추가정보로 개인 비밀번호를 설정할 수 있으며, 비밀번호 인증을 허용할 때 사용합니다.
- **BST** 사용자 등급에서 해당 사용자를 **일반사용자** 및 관리자로 권한을 부여합니다.
- 사용자에 대한 더욱 상세한 정보는 '사용자 정의 항목' 탭에서 직접 생성하여 입력할 수 있습니다.
- 사용자 지문정보를 등록하기 위해 **지문** 탭을 클릭합니다.
- 지문을 입력하는 절차는 **USB** 지문스캐너에 의한 방법과 **BioStation** 장치를 이용한 입력방법 두 가지로 나뉩니다.
- **USB** 지문 스캐너로 지문정보를 입력하는 방법은 아래와 같습니다.



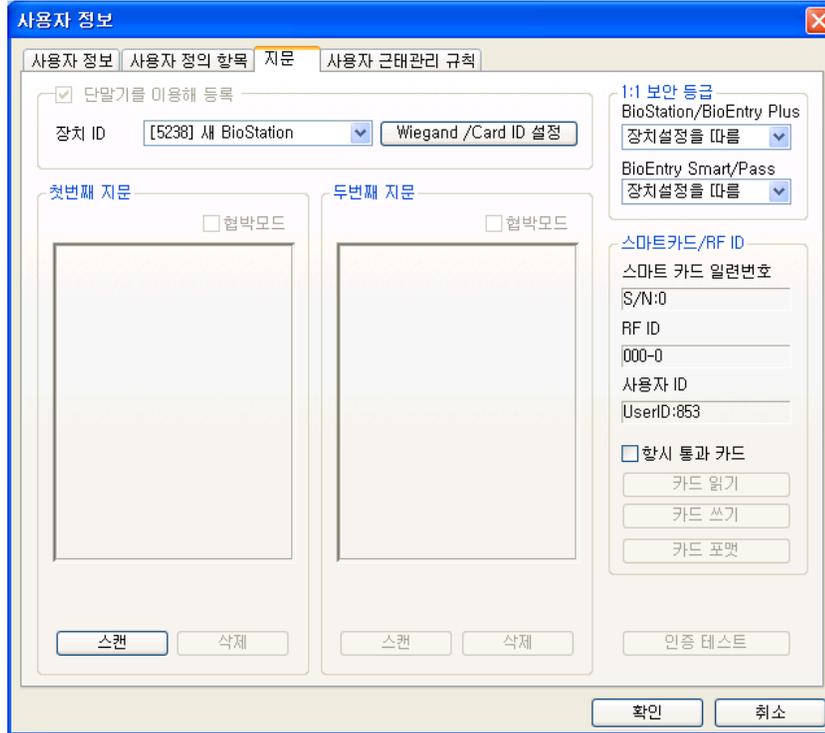
- 스캔 버튼을 누르고 **USB** 지문 스캐너에 손가락을 두 번 대어 첫 번째 지문정보를 입력합니다.



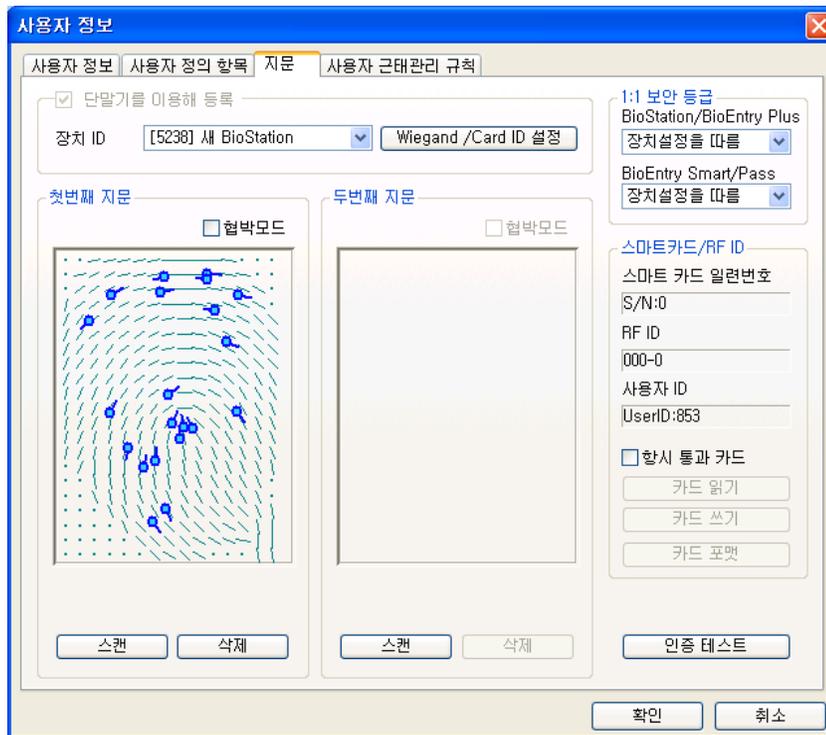
- 첫 번째 지문정보와 같은 방법으로 두 번째 지문정보를 입력합니다.



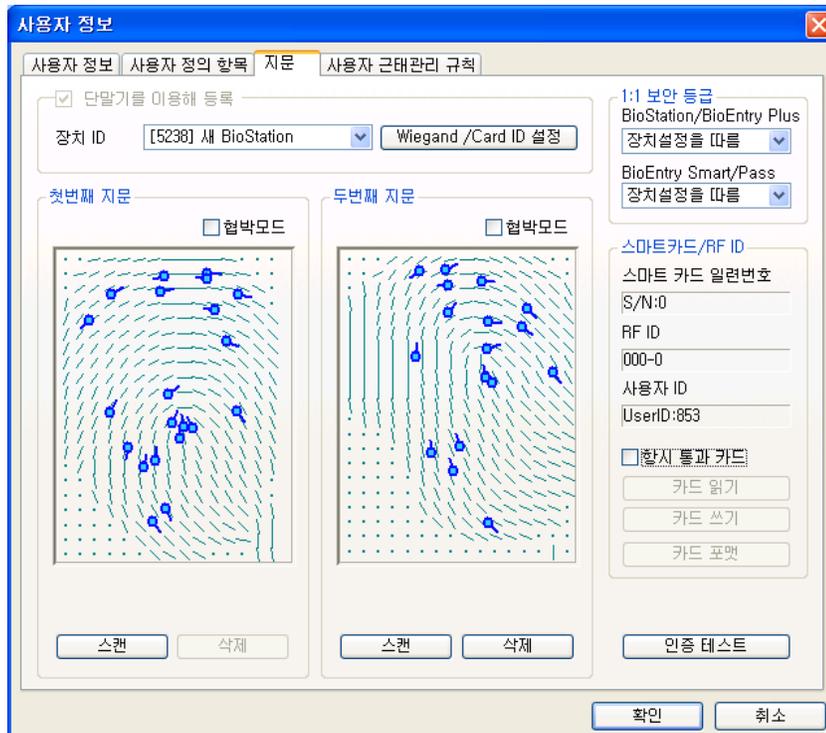
- BioStation 장치에 의한 지문정보를 입력하는 방법입니다.



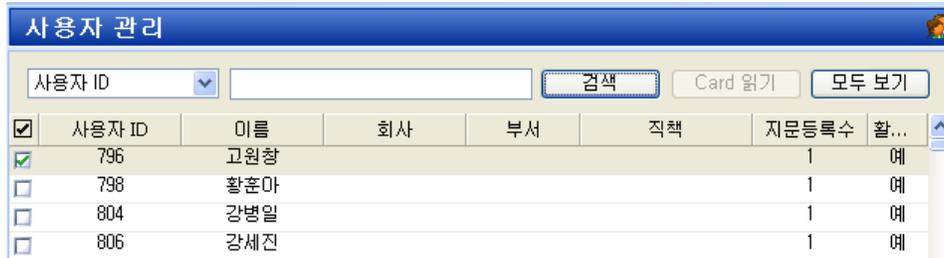
- 독립적으로 사용하실 경우에는 **BioStation**을 이용해 등록을 체크하면 스캔 버튼을 누르고 장치에 손가락을 두 번 대어 첫 번째 지문정보를 입력합니다. 장치가 2대 이상의 네트워크로 구성되어 있을 경우, **BioStation ID**를 설정하여 스캔 버튼을 누르고 장치에 손가락을 두 번 대어 첫 번째 지문정보를 입력합니다.
- 바이오 정보보호가 설정되어 있는 경우, 미리 입력된 해당 정보가 출력되며, 사용자가 동의를 해야만 지문입력이 가능합니다. 자세한 사항은 11.1.7. 옵션부분의 설명을 참조하시기 바랍니다.



- 앞서 언급한 독립적으로 사용하거나, 네트워크로 구성할 때도 마찬가지로 첫 번째 지문정보를 입력하는 과정과 같이 두 번째 지문정보를 입력합니다.

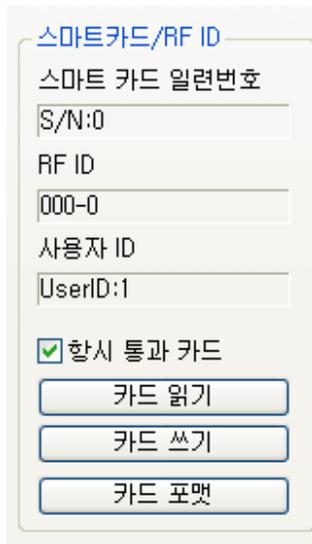


- 등록 과정을 종료하려면 **확인** 버튼을 클릭합니다. 그러면 사용자 리스트 윈도우에서 등록된 사용자에 대한 정보를 볼 수 있습니다. 이는 사용자 정보가 호스트 PC상의 데이터베이스에 추가되었음을 의미합니다.



3.1.5. 5단계 : 사용자의 Mifare 카드 발급하기

- 2.4. Mifare 카드 사용 절에서 **BioStation Mifare/ BioEntry Plus Mifare**를 선택한 경우 **BioStation Mifare**를 사용하여 사용자 Mifare 카드를 발급할 수 있습니다.
- 사용자 리스트 상의 등록된 사용자를 더블 클릭합니다. 그러면 사용자 정보 윈도우가 나타나 등록된 사용자의 정보를 보여줍니다.
- 사용자 정보 윈도우에서 **지문** 탭을 클릭합니다.
- Mifare 카드를 PC USB 스마트카드 장치에 놓고 **카드쓰기** 버튼을 클릭합니다.

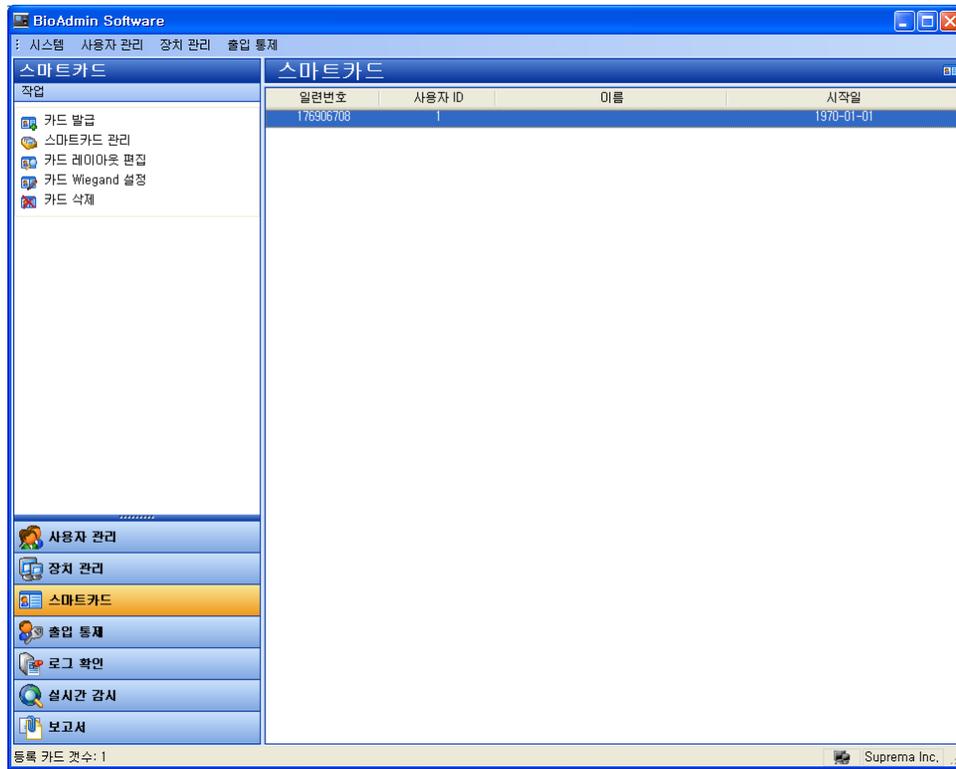


- 처음 시도 할 때 사이트 키 관리 윈도우가 나타납니다. 키 입력 필드가 공백이면 초기 설정 값이 사용됩니다. 알맞은 사이트 키를 입력하고 **확인** 버튼을 눌러 발급 과정을 마칩니다.

- 사용자 리스트 윈도우에서 사용자 데이터가 저장된 스마트카드의 일련 번호를 볼 수 있습니다.

단, 이 일련 번호는 PC USB 스마트 카드 장치를 사용하는 경우에만 발급 시에 읽어올 수 있으며, BioStation Mifare나 BioEntry Plus Mifare를 사용하는 경우에는 카드읽기를 통해서만 가능합니다.

- 스마트카드 메뉴를 선택하면 리스트에 추가된 카드를 볼 수 있습니다.



3.1.6. 6단계 : 사용자 근태관리 규칙

미리 설정된 근태 관리 규칙 그룹을 사용자에게 적용 하여 보고서 생성 시 참조할 수 있도록 합니다.

사용자 정보

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

근태 규칙 그룹: 일반직원 [모든 사용자에게 적용]

일일 규칙 내용

일요일	휴일
월요일	평일(아근가능)
화요일	평일(아근불가)
수요일	평일(아근가능)
목요일	평일(아근불가)
금요일	평일(아근가능)
토요일	토요일
휴 일	휴일
휴일군	모든 휴일

월간 규칙 내용

월간 규칙: 격주토요일휴무

첫번째 주	일	월	화	수	목	금	토	일반 근무일
두번째 주	일	월	화	수	목	금	토	휴일
세번째 주	일	월	화	수	목	금	토	일반 근무일
네번째 주	일	월	화	수	목	금	토	휴일
다섯번째 주	일	월	화	수	목	금	토	일반 근무일
여섯번째 주	일	월	화	수	목	금	토	휴일

확인 | 취소

3.1.7. 7단계 : 체크된 사용자를 장치에 전송 메뉴로 사용자 등록

체크된 사용자를 장치에 전송은 호스트 PC에서 BioStation 장치로 사용자 데이터베이스를 전송하는데 사용됩니다. 사용자 ID, 지문정보, 출입 그룹과 보안 등급과 같은 사용자 정보가 이 과정을 통해 전송됩니다.

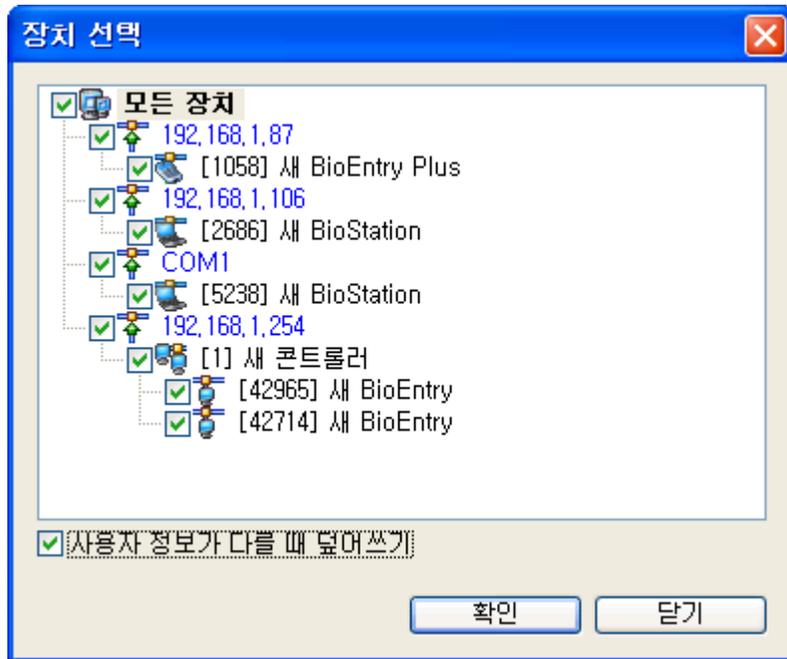
- 등록된 사용자 확인하기

사용자 관리

사용자 ID: [796] [검색] Card 읽기 모두 보기

<input checked="" type="checkbox"/>	사용자 ID	이름	회사	부서	직책	지문등록수	합...
<input checked="" type="checkbox"/>	796	고원창				1	예
<input type="checkbox"/>	798	황훈아				1	예
<input type="checkbox"/>	804	강병일				1	예
<input type="checkbox"/>	806	강세진				1	예

- 체크된 사용자를 장치에 전송 버튼을 클릭하고 장치로 체크 후 선택 버튼을 클릭합니다.



장치 별 사용자 관리 버튼을 눌러 장치를 클릭합니다. 사용자 정보영역이 노란색으로 표시되어 있다면, 사용자 정보가 장치로 성공적으로 전송되었음을 나타냅니다.

3.1.8. 8단계 : 실시간 감시

- 실시간 감시 메뉴를 선택하면 실시간 감시 화면이 주 윈도우 화면에 나타납니다.
- 실시간 감시 설정 메뉴를 선택하고 실시간 감시여부를 더블 클릭합니다. 저장하려면 **확인** 버튼을 클릭합니다.
연결된 모든 **BioStation** 장치들에 대한 실시간 감시를 시작하려면 실시간 감시 시작을 선택합니다.



3.1.9. 9단계 : 로그 확인

- 로그확인 메뉴를 선택하면 로그 리스트 윈도우가 주 윈도우에 표시됩니다. 로그 가져오기 / 예약 전송 설정 클릭, 장치를 체크한 후 선택버튼을 누르면 호스트 PC상의 로그 데이터베이스에 추가된 이벤트 로그 데이터를 볼 수 있습니다.

날짜	장치 ID	이벤트	근태이벤트	사용자 ID	이름	종류
2007-02-26 10:14:23	1539	시스템 시작		0		BioStation
2007-02-26 10:15:28	1539	시스템 시작		0		BioStation
2007-02-26 11:12:16	1539	1:N인증 실패		0		BioStation
2007-02-26 11:16:25	1539	1:N인증 실패		0		BioStation
2007-02-26 11:16:34	1539	1:N인증 실패		0		BioStation
2007-02-26 11:16:53	1539	등록 성공		853	서동석	BioStation
2007-02-26 11:17:00	1539	1:N인증 성공		853	서동석	BioStation
2007-02-26 11:17:00	1539	릴레이 On		0		BioStation
2007-02-26 11:17:03	1539	릴레이 Off		0		BioStation
2007-02-26 11:17:03	1539	1:N인증 성공		853	서동석	BioStation
2007-02-26 11:17:03	1539	릴레이 On		0		BioStation
2007-02-26 11:17:06	1539	릴레이 Off		0		BioStation

3.1.10. 10단계 : 보고서 리포트

보고서 메뉴를 선택하면 보고서 목록화면이 주 윈도우에 표시됩니다. 조건설정에서 회사명, 부서명, 사용자 ID, 사용자명을 입력하여 설정할 수 있으며, 기간을 설정하여 일일 보고서와 개인별 보고서로 필요한 보고서 종류를 선택해서 리포트 할 수 있습니다.

로그 가져오기는 장치에 저장된 로그를 가져오는 버튼이며, 보고서 목록 갱신 버튼은 장치에서 가져온 로그를 보고서 형태로 날짜 별, 개인별로 나열하여 출력하기 이전 화면을 구현시키는 버튼입니다. 마지막으로 보고서 미리 보기 버튼으로 리포트형태의 보고서를 미리 보기 위한 버튼입니다. 인쇄 버튼을 눌러 인쇄를 합니다.

3.2. BioEntry Plus와 함께 빠른 시작

3.2.1. 1단계 : 하드웨어 설치

BioEntry Plus는 유선 랜을 이용하여 네트워크를 설정할 수 있습니다. 설치에 관한 상세한 정보는 BioStation의 설치 안내서를 참조하시기 바랍니다.

Note : BioEntry Plus 는 장치의 상태에 따라 LED의 색상이 다르게 나타납니다.

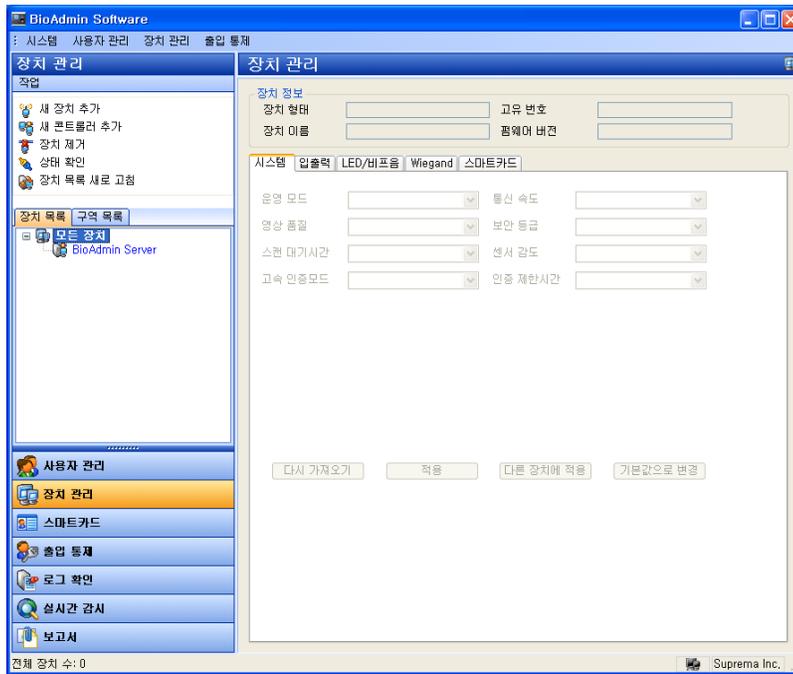
각 색상에 따른 자세한 설명은 BioEntry Plus Install Guide V1.0 의 10 페이지를 참조하시기 바랍니다.

3.2.2. 2단계 : 새 장치 검색

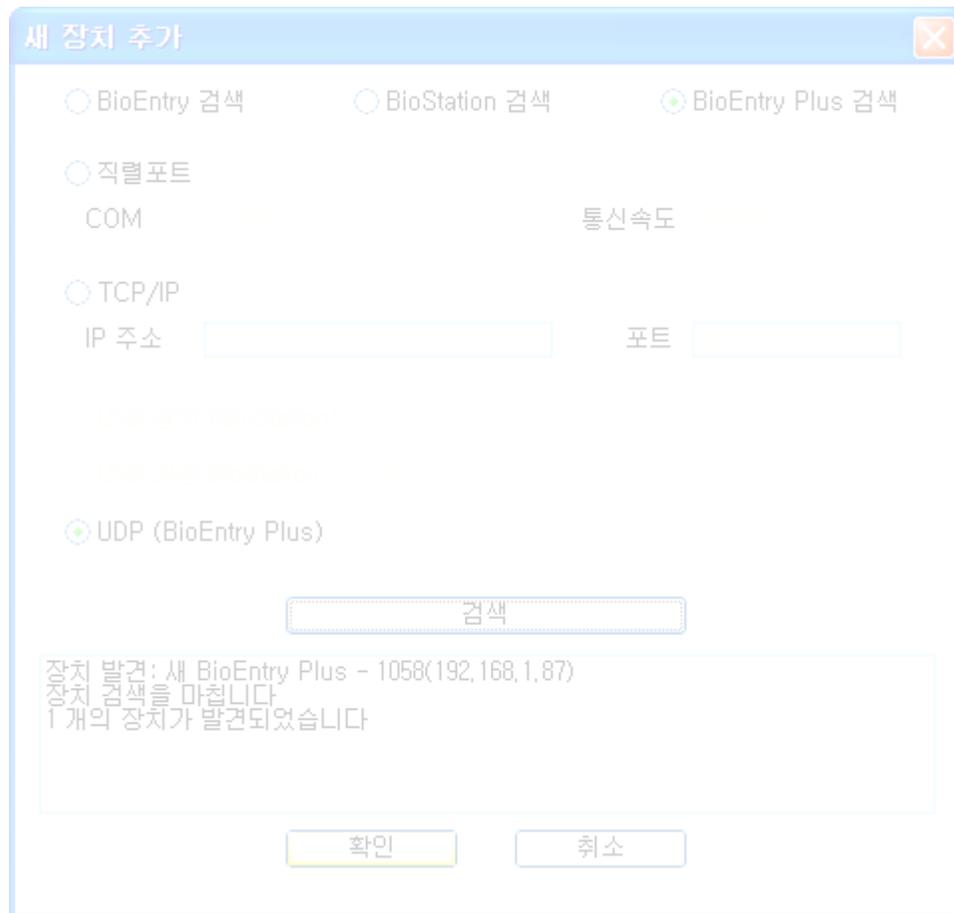
- BioAdmin 소프트웨어를 실행합니다.
- 관리자 ID와 패스워드를 입력합니다.
- 메인 메뉴에서 '장치관리'를 선택합니다.
- 서버에 접속된 BioEntry Plus들은 BioAdmin을 시작할 때 자동으로 목록에 추가되며, '장치 목록 새로 고침'을 선택해도 새로 연결된 장치를 볼 수 있습니다. BioEntry Plus를 서버에 접속하도록 설정했다 하더라도, 서버에 실제로 연결이 완료되어 목록에 보이기까지는 몇 분 정도 시간이 걸릴 수 있습니다.

3.2.3. 3단계 : 새 장치에 연결

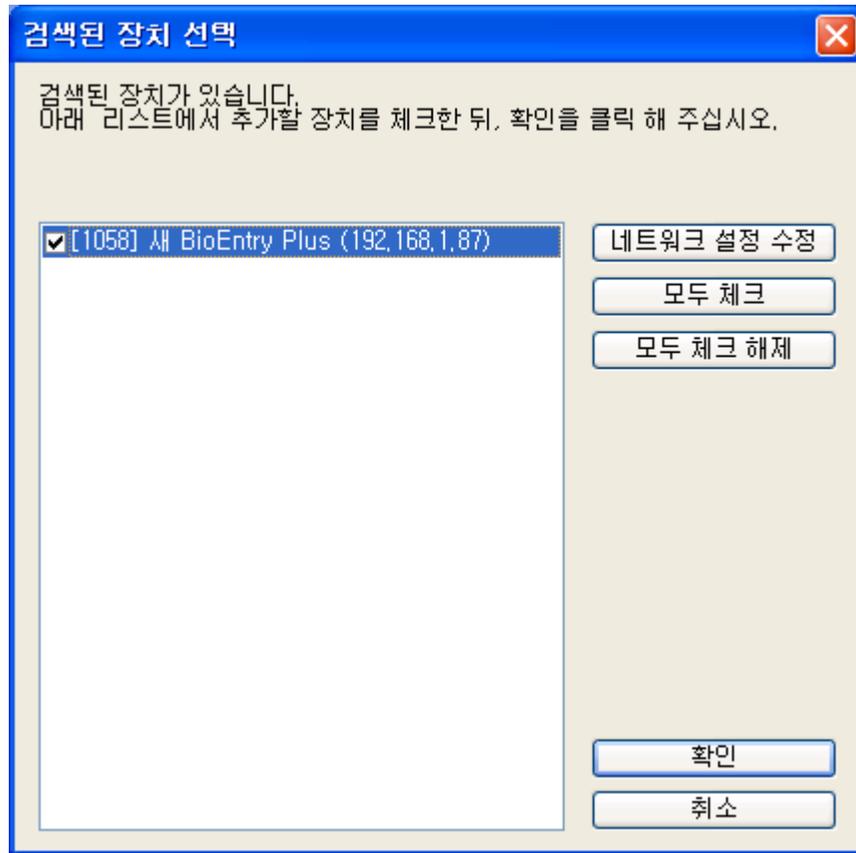
- 메인 메뉴에서 장치 관리를 선택합니다.



- '새 장치 추가' 를 선택하고 'BioEntry Plus 검색' 을 선택합니다.
- 'UDP (BioEntry Plus) 를 선택하고 '검색' 을 클릭합니다.
- 새롭게 설치된 BioEntry Plus 가 검색되면 확인을 누릅니다.



- 검색된 장치 리스트가 나오면 설치를 원하는 장치를 선택하고 확인을 클릭합니다.



Note : BioEntry Plus 는 DHCP 를 지원하므로, 자동 할당된 아이피를 부여 받아 표시되며 장치의 고유ID로 구분할 수 있습니다.
 이때, 고정 IP 를 사용하는 네트워크 환경에서 설치된 경우, 장치는 임의의 지정된 IP를 나타내며, 새로 설치된 장치가 2대 이상일 때는 1대씩 리스트에 나타나기 때문에 각각 등록을 하셔야 합니다.
 등록 후 해당 장치의 네트워크 탭에서 부여된 고정 IP와 서버의 IP 주소를 입력하여 설정합니다.
 네트워크 설정 수정을 통해 검색된 장치의 네트워크 정보를 수정합니다.

3.2.4. 4단계 : 사용자 관리

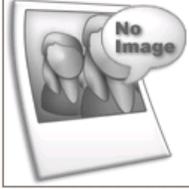
- 사용자 관리 메뉴를 선택하면 주 윈도우에 사용자 관리 페이지가 나타납니다.

Note : 사용자 관리에서 사용자에게 대한 정보는 기본정보와 지문정보로 나뉘어 이해할 수 있습니다. 기본정보는 사용자ID, 이름, 회사, 부서, 직책, 전화번호 등의 정보이며, 지문정보는 사용자의 지문에 대한 정보입니다.

사용자 정보

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

개인 정보


 사용자 ID: 1 사진 및 개인 인증화면 편집
 이름:
 회사: 사용 안함
 부서: 사용 안함
 직책: 사용 안함

상세정보

전화번호:
 핸드폰:
 이메일:
 성별: 남자
 생년월일: 2007-10-17
 시작일: 1970-01-01
 만료 일시: 2030-12-31 0 시

출입 통제

출입 상태: 활성화
 그룹 1: 전체 출입
 그룹 2: 사용 안함
 그룹 3: 사용 안함
 그룹 4: 사용 안함

인증 제한 (BioStation 전용)

제한 횟수: 0 회
 인증 간격(분): 0 분

추가 정보

비밀번호: 사용자 등급: 일반

확인 취소

- ‘새 사용자를 추가’ 를 클릭해서 신규 사용자를 등록합니다.
- 사용자 정보 탭에 사용자 정보를 입력합니다.

사용자 정보

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

개인 정보

사용자 ID: 사진 및 개인 인증화면 편집

이름:

회사: ...

부서: ...

직책: ...

상세정보

전화번호:

핸드폰:

이메일:

성별:

생년월일:

시작일:

만료 일시: 시

출입 통제

출입 상태: 활성화

그룹 1:

그룹 2:

그룹 3:

그룹 4:

인증 제한 (BioStation 전용)

제한 횟수: 회

인증 간격(분): 분

추가 정보

비밀번호:

사용자 등급:

확인 취소

- 콤보 박스를 이용해 회사, 부서와 직책을 선택할 수 있습니다.
- 새로운 회사, 부서 또는 직책 정보를 추가하려면 버튼을 누르거나, 정보 입력 창에 회사, 부서 또는 직책 명을 입력 후 **추가** 버튼을 누릅니다.
- 추가된 정보를 저장하려면 **닫기** 버튼을 누릅니다.

회사명 관리

슈프리마

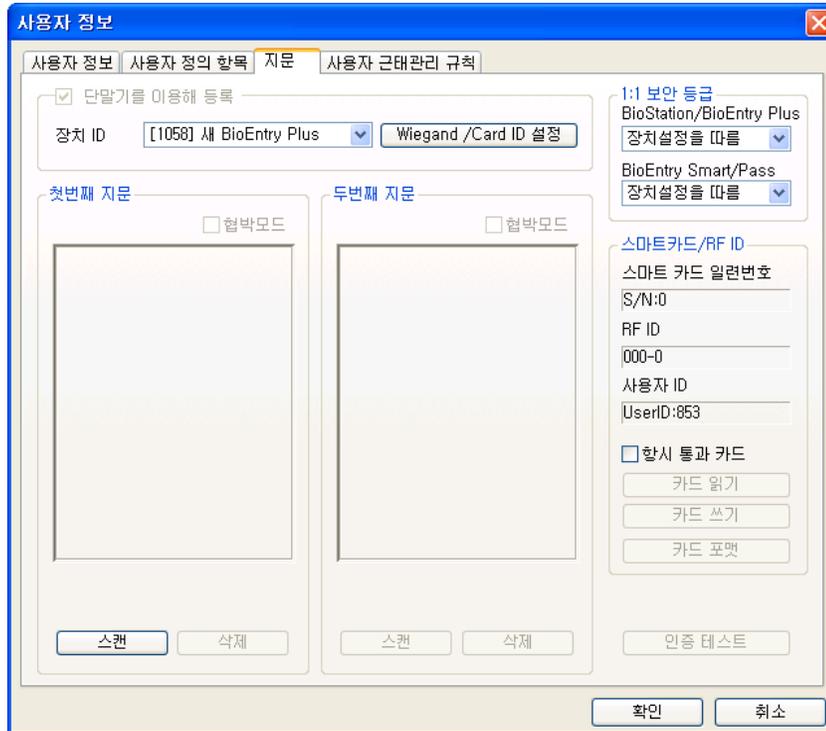
- 상세정보의 전화번호, 핸드폰, 이메일, 성별, 생년월일을 입력할 수 있으며, 사용자 정보 생성일이 등록일로 자동 입력 됩니다. 사용자의 만료일을 설정할 수 있습니다.
- 개인별 출입통제를 설정하고자 하는 경우, 출입 상태를 활성화 하고 전체출입/전체제한 또는 출입통제 메뉴에서 미리 설정한 출입그룹 중에 하나를 선택합

니다.

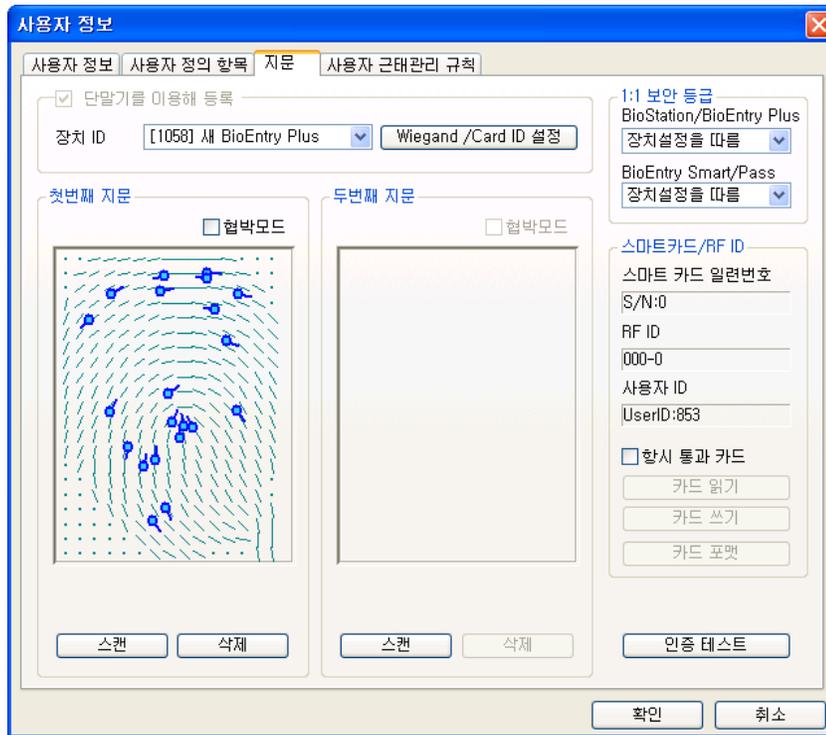
- 추가정보로 개인 비밀번호를 설정할 수 있으며, 비밀번호 인증을 허용할 때 사용합니다.
- **BST** 사용자 등급에서 해당 사용자를 **일반사용자** 및 관리자로 권한을 부여합니다.
- 제한횟수는 인증이 가능한 횟수를 제한하고, 인증 간격을 설정 하는 경우, 한번의 인증 후 설정된 시간이 지나야만 다시 인증이 가능합니다.
- 사용자에 대한 더욱 상세한 정보는 '사용자 정의 항목' 탭에서 직접 생성하여 입력할 수 있습니다.

- 사용자 지문정보를 등록하기 위해 **지문** 탭을 클릭합니다.
- 지문을 입력하는 절차는 **USB** 지문스캐너에 의한 방법과 **BioEntry Plus** 장치를 이용한 입력방법 두 가지로 나뉩니다. (**BioStation**과 동일 합니다.)
- 바이오 정보보호가 설정되어 있는 경우, 미리 입력된 해당 정보가 출력되며, 사용자가 동의를 해야만 지문입력이 가능합니다. 자세한 사항은 **11.1.7** 옵션 부분의 설명을 참조하시기 바랍니다.

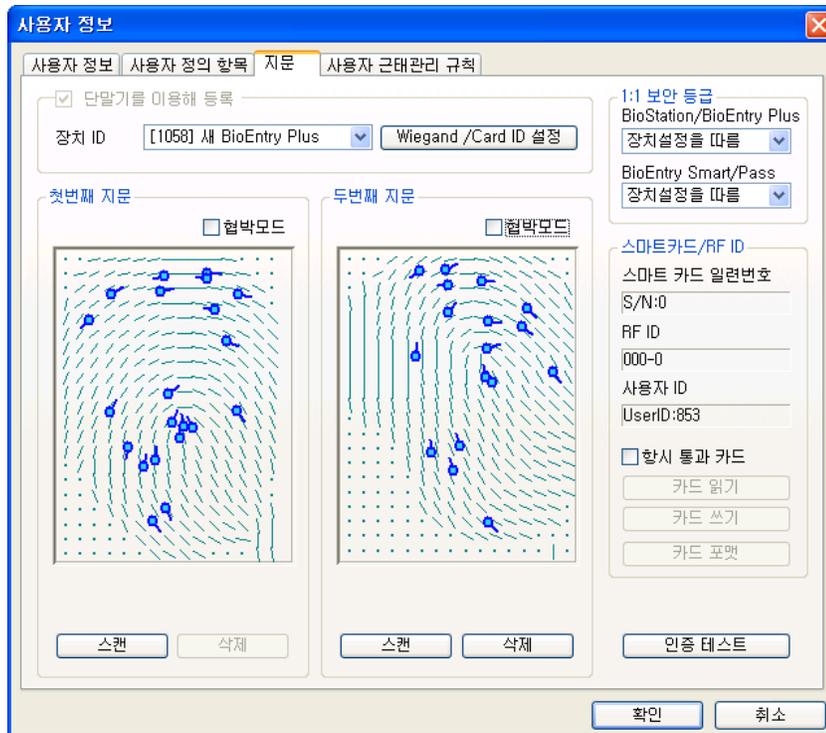
USB 지문 스캐너로 지문정보를 입력하는 방법은 아래와 같습니다.



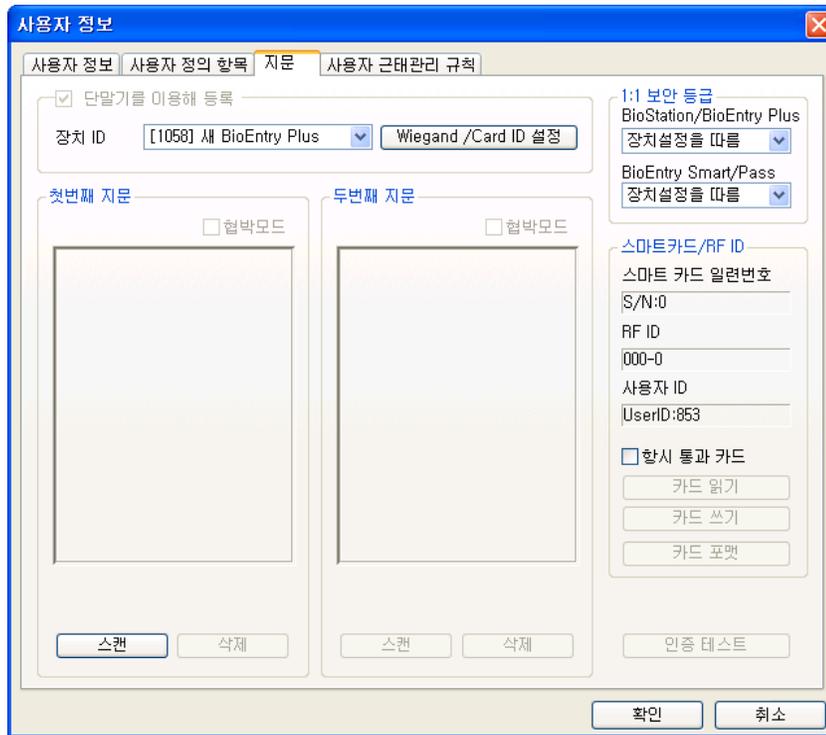
- 스캔 버튼을 누르고 **USB** 지문 스캐너에 손가락을 두 번 대어 첫 번째 지문정보를 입력합니다.



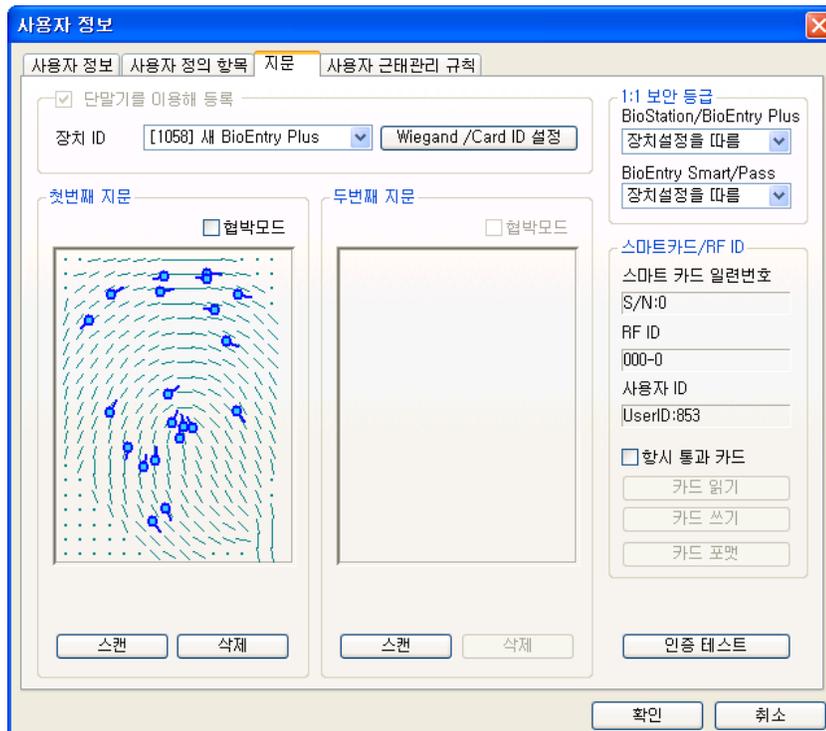
- 첫 번째 지문정보와 같은 방법으로 두 번째 지문정보를 입력합니다.



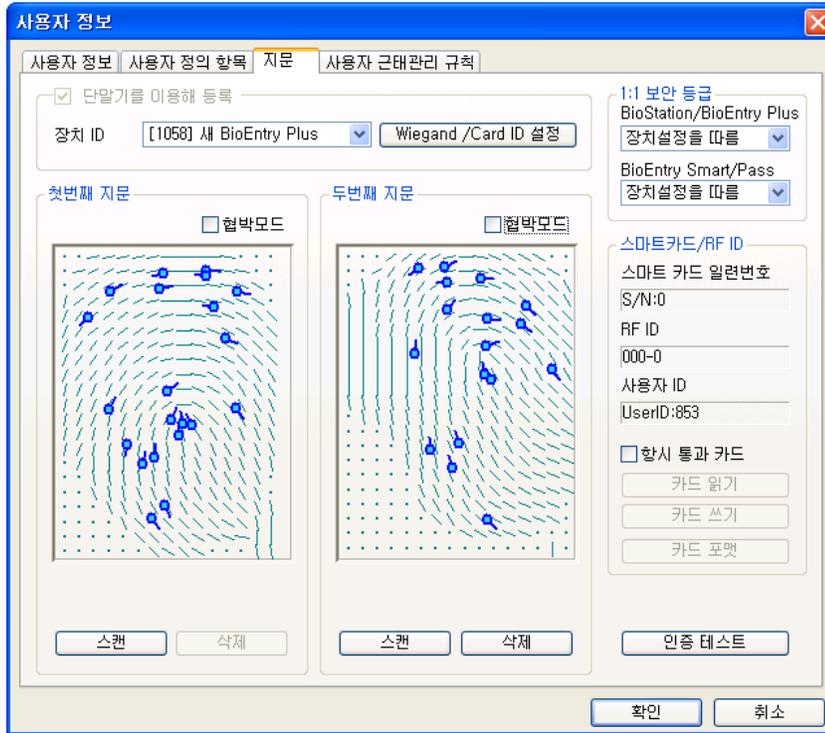
- BioEntry Plus 장치에 의한 지문정보를 입력하는 방법입니다.



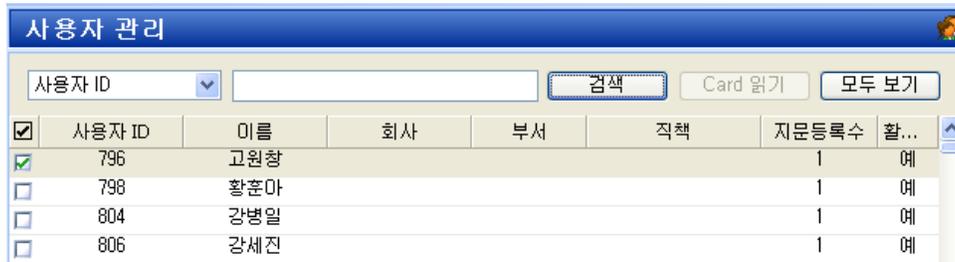
- 독립적으로 사용하실 경우에는 **BioEntry Plus**을 이용해 등록을 체크하면 스캔 버튼을 누르고 장치에 손가락을 두 번 대어 첫 번째 지문정보를 입력합니다. 장치가 2대 이상의 네트워크로 구성되어 있을 경우, **BioEntry Plus ID**를 설정하여 스캔 버튼을 누르고 장치에 손가락을 두 번 대어 첫 번째 지문정보를 입력합니다.



- 앞서 언급한 독립적으로 사용하거나, 네트워크로 구성할 때도 마찬가지로 첫 번째 지문정보를 입력하는 과정과 같이 두 번째 지문정보를 입력합니다.



- 등록 과정을 종료하려면 **확인** 버튼을 클릭합니다. 그러면 사용자 리스트 윈도우에서 등록된 사용자에 대한 정보를 볼 수 있습니다. 이는 사용자 정보가 호스트 PC상의 데이터베이스에 추가되었음을 의미합니다.



3.2.5. 5단계 : 사용자의 Mifare 카드 발급하기

- 2.4. Mifare 카드 사용 절에서 BioStation Mifare/ BioEntry Plus Mifare를 선택한 경우 BioEntry Plus Mifare를 사용하여 사용자 Mifare 카드를 발급할 수 있습니다.
- 사용자 리스트 상의 등록된 사용자를 더블 클릭합니다. 그러면 사용자 정보 윈도우가 나타나 등록된 사용자의 정보를 보여줍니다.
- 사용자 정보 윈도우에서 **지문** 탭을 클릭합니다.
- Mifare 카드를 PC USB 스마트카드 장치에 놓고 **카드쓰기** 버튼을 클릭합니다.

스마트카드/RF ID

스마트 카드 일련번호

S/N:0

RF ID

000-0

사용자 ID

UserID:1

항상 통과 카드

카드 읽기

카드 쓰기

카드 포맷

- 처음 시도 할 때 사이트 키 관리 윈도우가 나타납니다. 키 입력 필드가 공백이면 초기 설정 값이 사용됩니다. 알맞은 사이트 키를 입력하고 **확인** 버튼을 눌러 발급 과정을 마칩니다.

사이트키 입력

현재 사이트키

사이트키 변경

사이트키 변경

사이트키 확인

확인

취소

- 사용자 리스트 윈도우에서 사용자 데이터가 저장된 스마트카드의 일련 번호를 볼 수 있습니다.

스마트카드/RF ID

스마트 카드 일련번호
S/N:176906708

RF ID
000-0

사용자 ID
UserID:1

항상 통과 카드

카드 읽기

카드 쓰기

카드 포맷

단, 이 일련 번호는 PC USB 스마트 카드 장치를 사용하는 경우에만 발급 시에 읽어올 수 있으며, BioStation Mifare나 BioEntry Plus Mifare를 사용하는 경우에는 카드읽기를 통해서만 가능합니다.

- 스마트카드 메뉴를 선택하면 리스트에 추가된 카드를 볼 수 있습니다.

일련번호	사용자 ID	이름	시작일
176906708	1		1970-01-01

3.2.6.

6단계 : 사용자 근태관리 규칙

미리 설정된 근태 관리 규칙 그룹을 사용자에게 적용 하여 보고서 생성 시 참조할

수 있도록 합니다.

3.2.7.

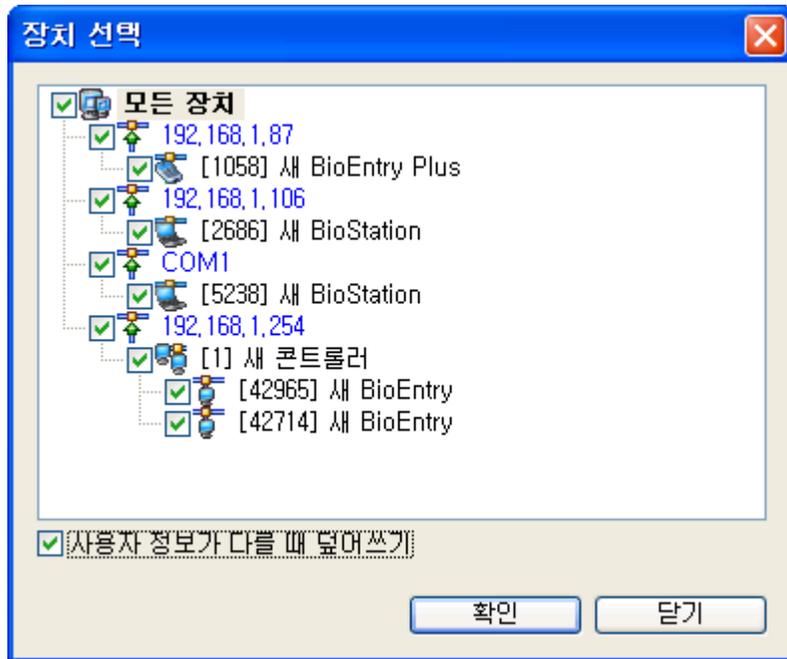
7단계 : 체크된 사용자를 장치에 전송 메뉴로 사용자 등록

체크된 사용자를 장치에 전송은 호스트 PC에서 BioEntry Plus 장치로 사용자 데이터베이스를 전송하는데 사용됩니다. 사용자 ID, 지문정보, 출입 그룹과 보안 등급과 같은 사용자 정보가 이 과정을 통해 전송됩니다.

- 등록된 사용자 확인하기

<input checked="" type="checkbox"/>	사용자 ID	이름	회사	부서	직책	지문등록수	활...
<input checked="" type="checkbox"/>	796	고원창				1	예
<input type="checkbox"/>	798	황훈아				1	예
<input type="checkbox"/>	804	강병일				1	예
<input type="checkbox"/>	806	강세진				1	예

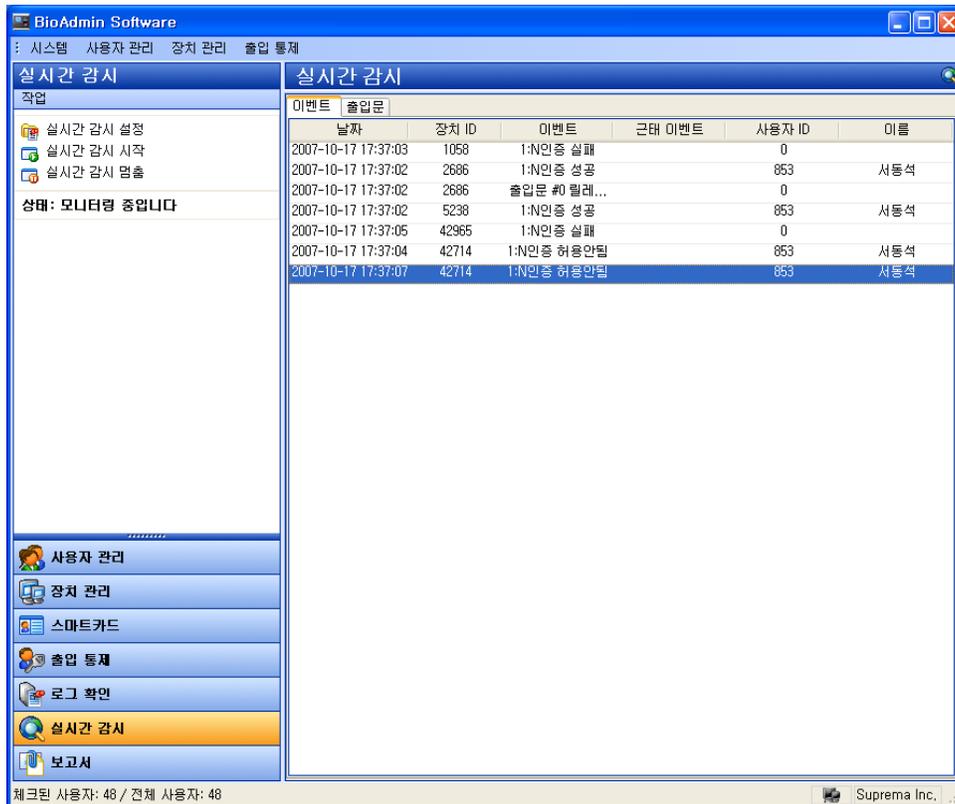
- 체크된 사용자를 장치에 전송 버튼을 클릭하고 장치로 체크 후 선택 버튼을 클릭합니다.



장치 별 사용자 관리 버튼을 눌러 장치를 클릭합니다. 사용자 정보영역이 노란색으로 표시되어 있다면, 사용자 정보가 장치로 성공적으로 전송되었음을 나타냅니다.

3.2.8. 8단계 : 실시간 감시

- 실시간 감시 메뉴를 선택하면 실시간 감시 화면이 주 윈도우 화면에 나타납니다.
- 실시간 감시 설정 메뉴를 선택하고 실시간 감시여부를 더블 클릭합니다. 저장하려면 확인 버튼을 클릭합니다. 연결된 모든 BioEntry Plus 장치들에 대한 실시간 감시를 시작하려면 실시간 감시 시작을 선택합니다.
- 출입문 감시 - 만약 출입문 설정이 되어 있다면 출입문 감시 페이지를 통해서 각 출입문의 상태를 파악할 수 있으며 출입문 제어 및 경보 해제를 할 수 있습니다. 이곳에서 해제한 경보나 이벤트 등은 실제 장치에 적용되지 않고, PC상에서 표시되는 사항만 해제하게 되며, 출입문 제어만 실제 장치에 적용됩니다.



3.2.9. 9단계 : 로그 확인

- 로그확인 메뉴를 선택하면 로그 리스트 윈도우가 주 윈도우에 표시됩니다.
- 로그 가져오기 / 예약 전송 설정 클릭 , 장치를 체크한 후 선택버튼을 누르면 호스트 PC상의 로그 데이터베이스에 추가된 이벤트 로그 데이터를 볼 수 있습니다

날짜	장치 ID	이벤트	근태이벤트	사용자 ID	이름	종류
2007-02-26 10:14:23	1539	시스템 시작		0		BioStation
2007-02-26 10:15:28	1539	시스템 시작		0		BioStation
2007-02-26 11:12:16	1539	1:N인증 실패		0		BioStation
2007-02-26 11:16:25	1539	1:N인증 실패		0		BioStation
2007-02-26 11:16:34	1539	1:N인증 실패		0		BioStation
2007-02-26 11:16:53	1539	등록 성공		853	서동석	BioStation
2007-02-26 11:17:00	1539	1:N인증 성공		853	서동석	BioStation
2007-02-26 11:17:00	1539	릴레이 On		0		BioStation
2007-02-26 11:17:03	1539	릴레이 Off		0		BioStation
2007-02-26 11:17:03	1539	1:N인증 성공		853	서동석	BioStation
2007-02-26 11:17:03	1539	릴레이 On		0		BioStation
2007-02-26 11:17:06	1539	릴레이 Off		0		BioStation

3.2.10. 10단계 : 보고서 리포트

- 보고서 메뉴를 선택하면 보고서 목록화면이 주 윈도우에 표시됩니다. 조건설정에서 회사명, 부서명, 사용자 ID, 사용자명을 입력하여 설정할 수 있으며, 기간을 설정하여 일일 보고서와 개인별 보고서로 필요한 보고서 종류를 선택해서 리포트 할 수 있습니다.

- 로그 가져오기는 장치에 저장된 로그를 가져오는 버튼이며, 보고서 목록 갱신 버튼은 장치에서 가져온 로그를 보고서 형태로 날짜 별, 개인별로 나열하여 출력하기 이전 화면을 구현시키는 버튼입니다. 마지막으로 보고서 미리 보기 버튼으로 리포트형태의 보고서를 미리 보기 위한 버튼입니다. 인쇄 버튼을 눌러 인쇄를 합니다.

3.3. BioLite Net 과 함께 빠른 시작

3.3.1. 1단계 : 하드웨어 설치

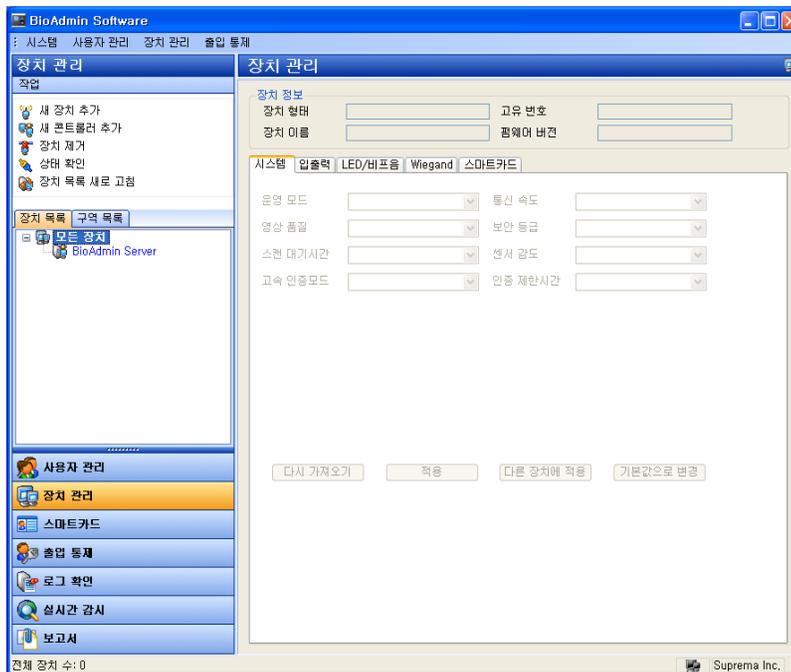
BioLite Net 은 유선 랜을 이용하여 네트워크를 설정할 수 있습니다. 설치에 관한 상세한 정보는 BioStation의 설치 안내서를 참조하시기 바랍니다.

3.3.2. 2단계 : 새 장치 검색

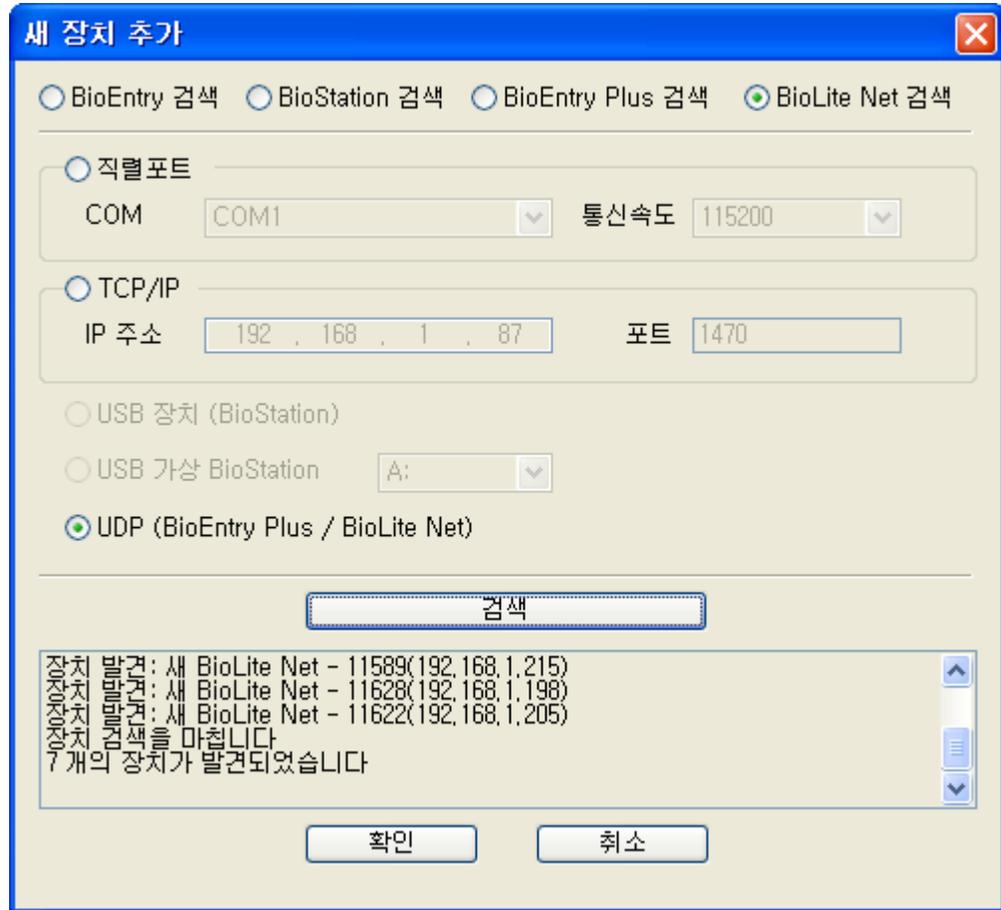
- BioAdmin 소프트웨어를 실행합니다.
- 관리자 ID와 패스워드를 입력합니다.
- 메인 메뉴에서 '장치관리'를 선택합니다.
- 서버에 접속된 BioLite Net들은 BioAdmin을 시작할 때 자동으로 목록에 추가되며, '장치 목록 새로 고침'을 선택해도 새로 연결된 장치를 볼 수 있습니다. BioLite Net을 서버에 접속하도록 설정했다 하더라도, 서버에 실제로 연결이 완료되어 목록에 보이기까지는 몇 분 정도 시간이 걸릴 수 있습니다.

3.3.3. 3단계 : 새 장치에 연결

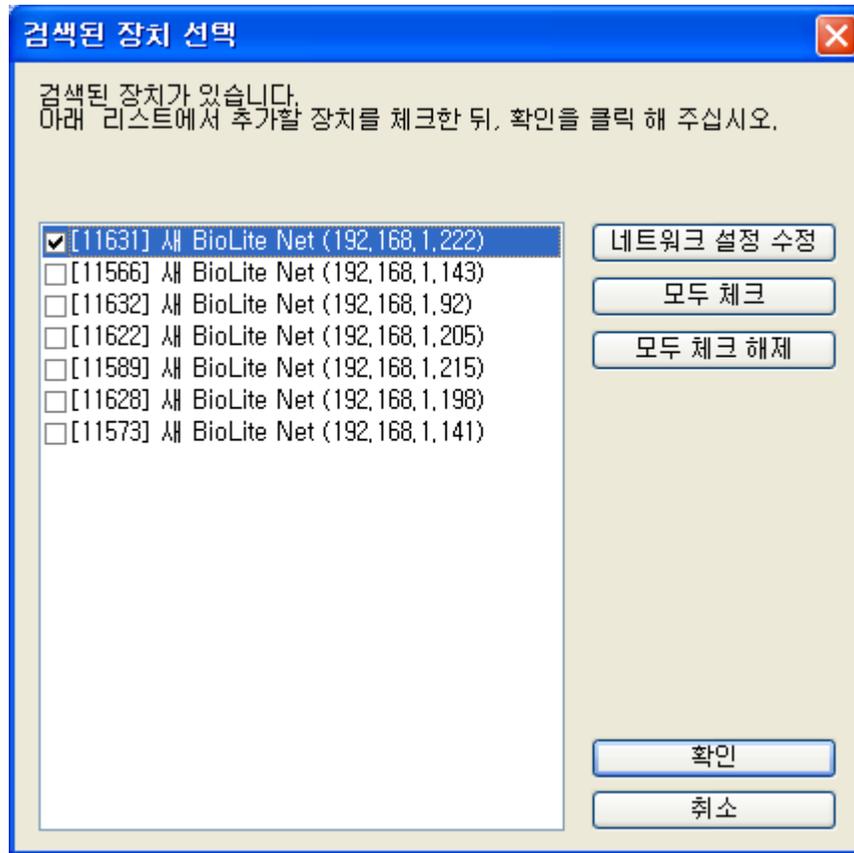
- 메인 메뉴에서 장치 관리를 선택합니다.



- '새 장치 추가' 를 선택하고 'BioLite Net 검색' 을 선택합니다.
- 'UDP (BioEntry Plus / BioLite Net) 를 선택하고 '검색' 을 클릭합니다.
- 새롭게 설치된 BioLite Net 이 검색되면 확인을 누릅니다.



- 검색된 장치 리스트가 나오면 설치를 원하는 장치를 선택하고 확인을 클릭합니다.



Note : BioLite Net 은 DHCP 를 지원하므로, 자동 할당된 아이피를 부여 받아 표시되며 장치의 고유ID로 구분할 수 있습니다.
 이때, 고정 IP 를 사용하는 네트워크 환경에서 설치된 경우, 장치는 임의의 지정된 IP를 나타내며, 새로 설치된 장치가 2대 이상일 때는 1대씩 리스트에 나타나기 때문에 각각 등록을 하셔야 합니다.
 등록 후 해당 장치의 네트워크 탭에서 부여된 고정 IP와 서버의 IP 주소를 입력하여 설정합니다.
 네트워크 설정 수정을 통해 검색된 장치의 네트워크 정보를 수정합니다.

3.3.4. 4단계 : 사용자 관리

- 사용자 관리 메뉴를 선택하면 주 윈도우에 사용자 관리 페이지가 나타납니다.

Note : 사용자 관리에서 사용자에게 대한 정보는 기본정보와 지문정보로 나뉘어 이해할 수 있습니다. 기본정보는 사용자ID, 이름, 회사, 부서, 직책, 전화번호 등의 정보이며, 지문정보는 사용자의 지문에 대한 정보입니다.

사용자 정보

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

개인 정보


 사용자 ID: 1 사진 및 개인 인증화면 편집
 이름:
 회사: 사용 안함
 부서: 사용 안함
 직책: 사용 안함

상세정보

전화번호:
 핸드폰:
 이메일:
 성별: 남자
 생년월일: 2007-10-17
 시작일: 1970-01-01
 만료 일시: 2030-12-31 0 시

출입 통제

출입 상태: 활성화
 그룹 1: 전체 출입
 그룹 2: 사용 안함
 그룹 3: 사용 안함
 그룹 4: 사용 안함

인증 제한 (BioStation 전용)

제한 횟수: 0 회
 인증 간격(분): 0 분

추가 정보

비밀번호: 사용자 등급: 일반

확인 취소

- ‘새 사용자를 추가’ 를 클릭해서 신규 사용자를 등록합니다.
- 사용자 정보 탭에 사용자 정보를 입력합니다.

사용자 정보

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

개인 정보

사용자 ID: 사진 및 개인 인증화면 편집

이름:

회사: ...

부서: ...

직책: ...

상세정보

전화번호:

핸드폰:

이메일:

성별:

생년월일:

시작일:

만료 일시: 시

출입 통제

출입 상태: 활성화

그룹 1:

그룹 2:

그룹 3:

그룹 4:

인증 제한 (BioStation 전용)

제한 횟수: 회

인증 간격(분): 분

추가 정보

비밀번호:

사용자 등급:

확인 취소

- 콤보 박스를 이용해 회사, 부서와 직책을 선택할 수 있습니다.
- 새로운 회사, 부서 또는 직책 정보를 추가하려면 버튼을 누르거나, 정보 입력 창에 회사, 부서 또는 직책 명을 입력 후 **추가** 버튼을 누릅니다.
- 추가된 정보를 저장하려면 **닫기** 버튼을 누릅니다.

회사명 관리

슈프리마

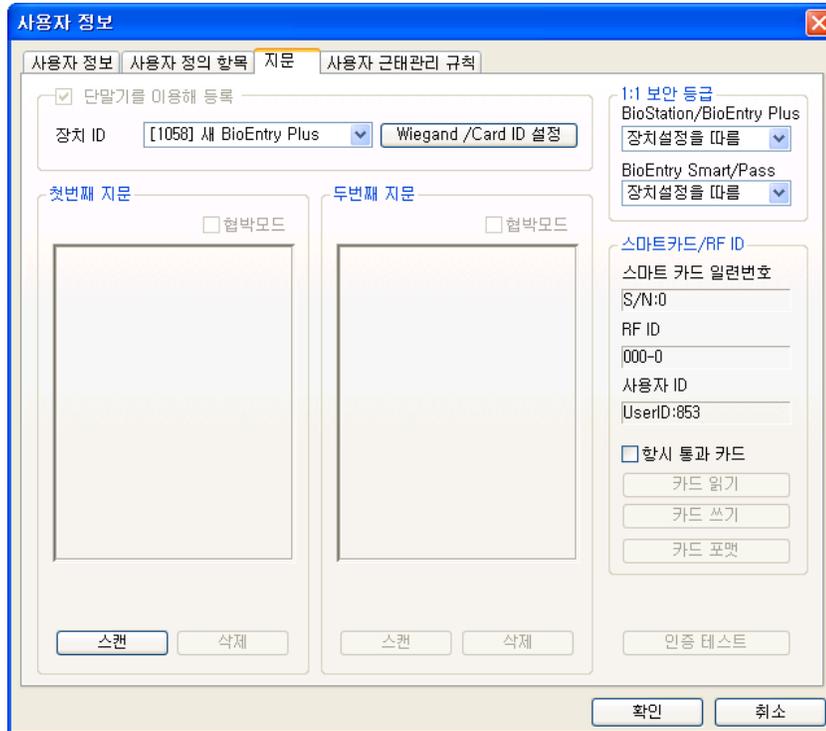
- 상세정보의 전화번호, 핸드폰, 이메일, 성별, 생년월일을 입력할 수 있으며, 사용자 정보 생성일이 등록일로 자동 입력 됩니다. 사용자의 만료일을 설정할 수 있습니다.
- 개인별 출입통제를 설정하고자 하는 경우, 출입 상태를 활성화 하고 전체출입/전체제한 또는 출입통제 메뉴에서 미리 설정한 출입그룹 중에 하나를 선택합

니다.

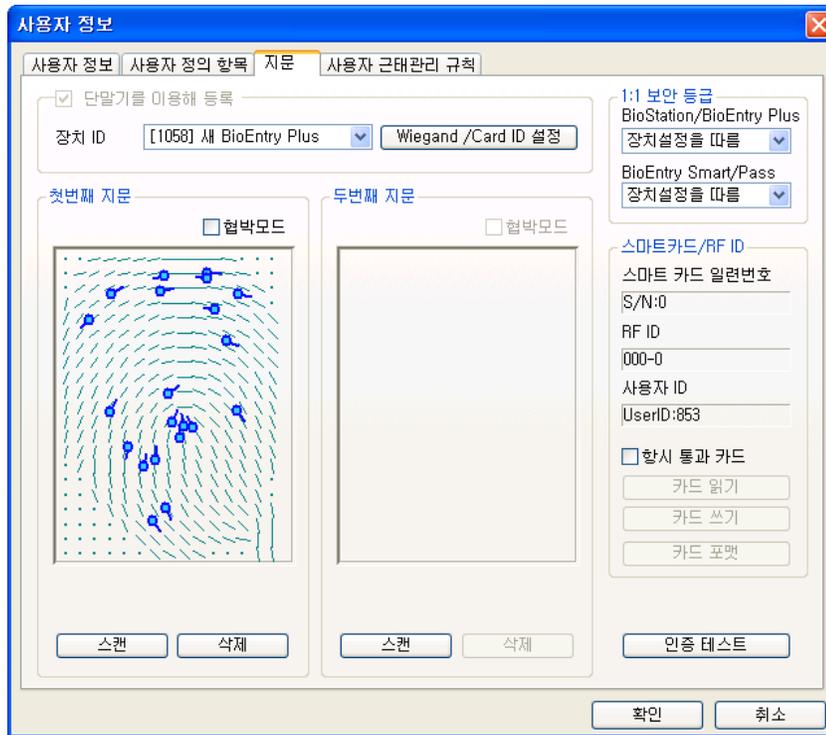
- 추가정보로 개인 비밀번호를 설정할 수 있으며, 비밀번호 인증을 허용할 때 사용합니다.
- **BST** 사용자 등급에서 해당 사용자를 **일반사용자** 및 관리자로 권한을 부여합니다.
- 제한횟수는 인증이 가능한 횟수를 제한하고, 인증 간격을 설정 하는 경우, 한번의 인증 후 설정된 시간이 지나야만 다시 인증이 가능합니다.
- 사용자에 대한 더욱 상세한 정보는 '사용자 정의 항목' 탭에서 직접 생성하여 입력할 수 있습니다.

- 사용자 지문정보를 등록하기 위해 **지문** 탭을 클릭합니다.
- 지문을 입력하는 절차는 **USB** 지문스캐너에 의한 방법과 **BioEntry Plus** 장치를 이용한 입력방법 두 가지로 나뉩니다. (**BioStation**과 동일 합니다.)
- 바이오 정보보호가 설정되어 있는 경우, 미리 입력된 해당 정보가 출력되며, 사용자가 동의를 해야만 지문입력이 가능합니다. 자세한 사항은 **11.1.7** 옵션 부분의 설명을 참조하시기 바랍니다.

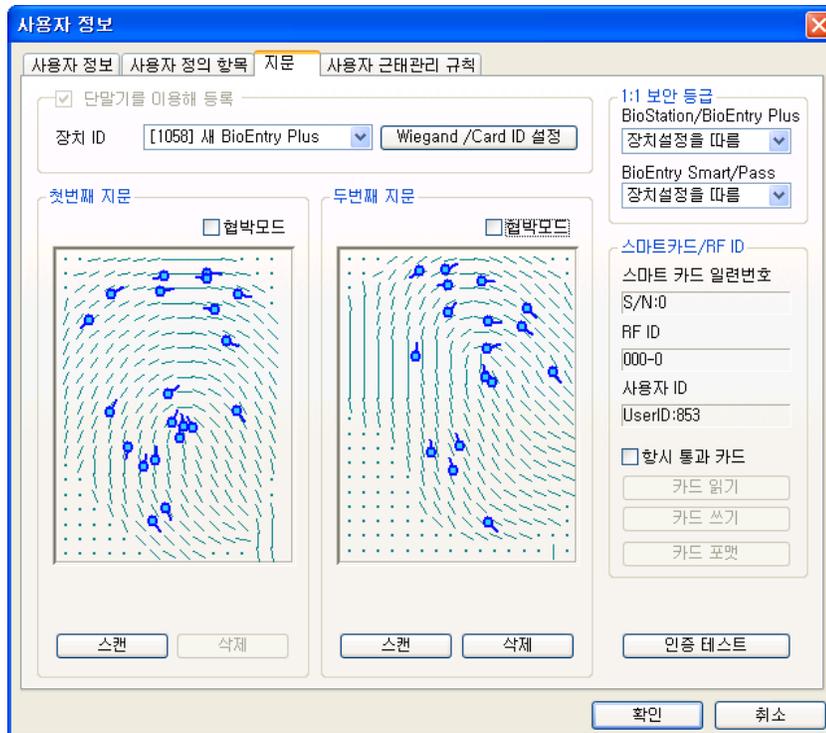
USB 지문 스캐너로 지문정보를 입력하는 방법은 아래와 같습니다.



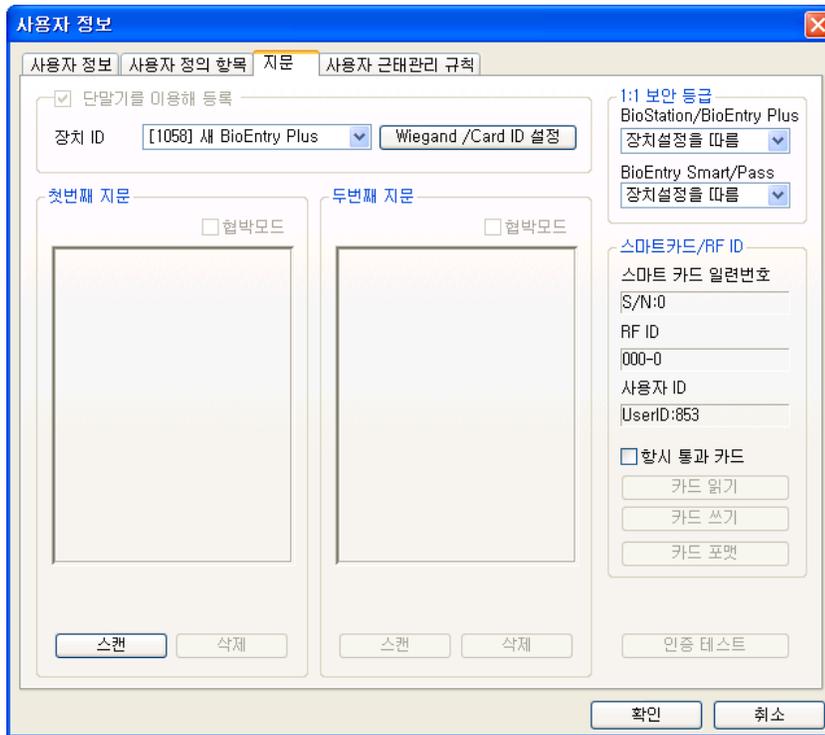
- 스캔 버튼을 누르고 **USB** 지문 스캐너에 손가락을 두 번 대어 첫 번째 지문정보를 입력합니다.



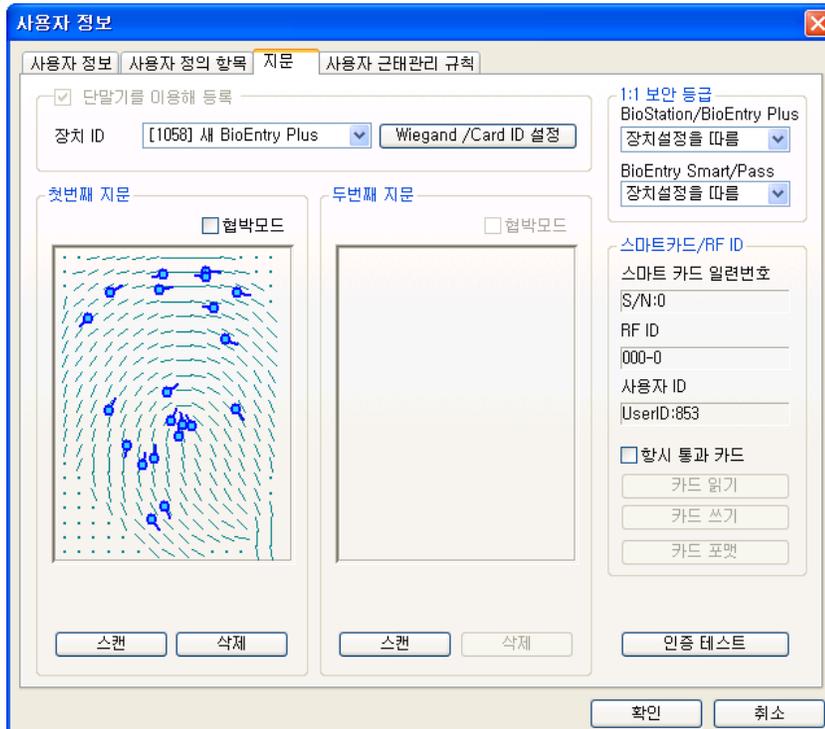
- 첫 번째 지문정보와 같은 방법으로 두 번째 지문정보를 입력합니다.



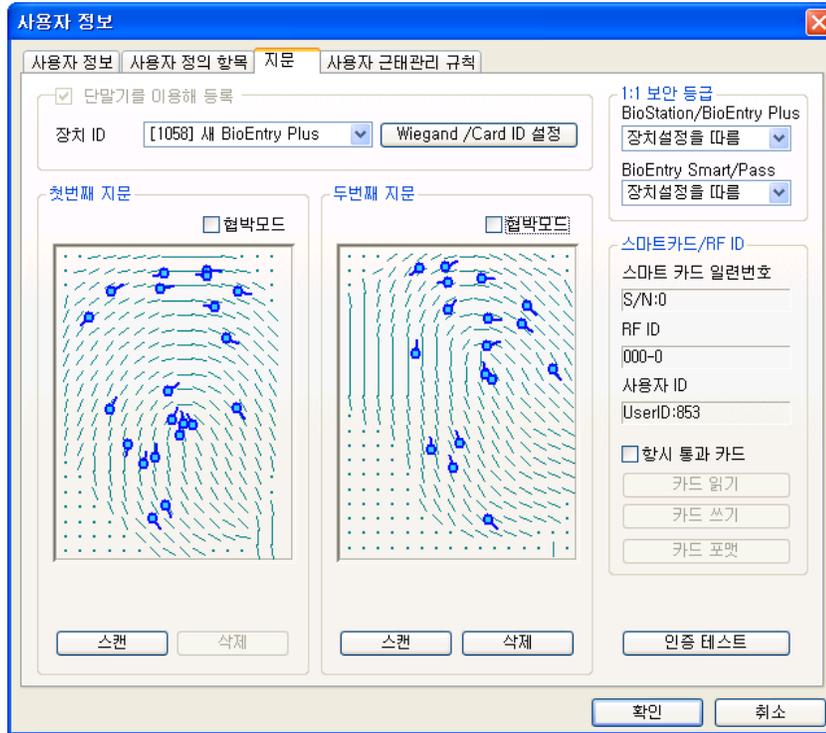
- BioLite Net 장치에 의한 지문정보를 입력하는 방법입니다.



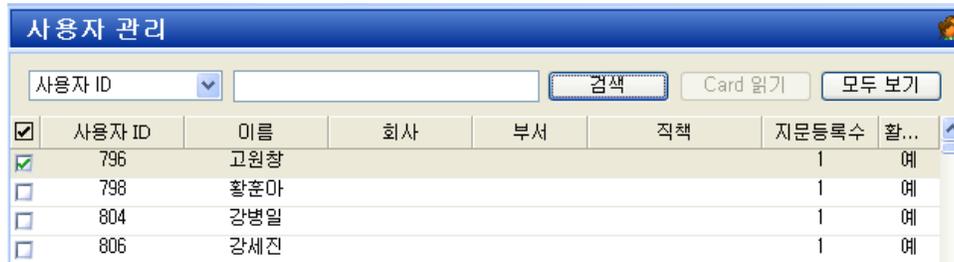
- 독립적으로 사용하실 경우에는 **BioLite Net**을 이용해 등록을 체크하면 스캔 버튼을 누르고 장치에 손가락을 두 번 대어 첫 번째 지문정보를 입력합니다. 장치가 2대 이상의 네트워크로 구성되어 있을 경우, **BioLite Net ID**를 설정하여 스캔 버튼을 누르고 장치에 손가락을 두 번 대어 첫 번째 지문정보를 입력합니다.



- 앞서 언급한 독립적으로 사용하거나, 네트워크로 구성할 때도 마찬가지로 첫 번째 지문정보를 입력하는 과정과 같이 두 번째 지문정보를 입력합니다.



- 등록 과정을 종료하려면 **확인** 버튼을 클릭합니다. 그러면 사용자 리스트 윈도우에서 등록된 사용자에 대한 정보를 볼 수 있습니다. 이는 사용자 정보가 호스트 PC상의 데이터베이스에 추가되었음을 의미합니다.



3.3.5. 5단계 : 사용자의 Mifare 카드 발급하기

- 2.4. Mifare 카드 사용 절에서 BioStation Mifare/ BioEntry Plus Mifare를 선택한 경우 BioLite Net Mifare를 사용하여 사용자 Mifare 카드를 발급할 수 있습니다.
- 사용자 리스트 상의 등록된 사용자를 더블 클릭합니다. 그러면 사용자 정보 윈도우가 나타나 등록된 사용자의 정보를 보여줍니다.
- 사용자 정보 윈도우에서 **지문** 탭을 클릭합니다.
- Mifare 카드를 PC USB 스마트카드 장치에 놓고 **카드쓰기** 버튼을 클릭합니다.

스마트카드/RF ID

스마트 카드 일련번호

S/N:0

RF ID

000-0

사용자 ID

UserID:1

항상 통과 카드

카드 읽기

카드 쓰기

카드 포맷

- 처음 시도 할 때 사이트 키 관리 윈도우가 나타납니다. 키 입력 필드가 공백이면 초기 설정 값이 사용됩니다. 알맞은 사이트 키를 입력하고 **확인** 버튼을 눌러 발급 과정을 마칩니다.

사이트키 입력

현재 사이트키

사이트키 변경

사이트키 변경

사이트키 확인

확인

취소

- 사용자 리스트 윈도우에서 사용자 데이터가 저장된 스마트카드의 일련 번호를 볼 수 있습니다.

스마트카드/RF ID

스마트 카드 일련번호
S/N:176906708

RF ID
000-0

사용자 ID
UserID:1

항상 통과 카드

카드 읽기

카드 쓰기

카드 포맷

단, 이 일련 번호는 PC USB 스마트 카드 장치를 사용하는 경우에만 발급 시에 읽어올 수 있으며, BioStation Mifare나 BioEntry Plus Mifare, BioLite Net Mifare를 사용하는 경우에는 카드읽기를 통해서만 가능합니다.

- 스마트카드 메뉴를 선택하면 리스트에 추가된 카드를 볼 수 있습니다.

The screenshot shows the BioAdmin Software interface. On the left, there is a navigation menu with the following items: 스마트카드 (Smart Card), 사용자 관리 (User Management), 장치 관리 (Device Management), 출입 통제 (Access Control), 로그 확인 (Log Check), 실시간 감시 (Real-time Monitoring), and 보고서 (Reports). The '스마트카드' menu is selected and expanded, showing sub-items: 카드 발급 (Card Issuance), 스마트카드 관리 (Smart Card Management), 카드 레이아웃 편집 (Card Layout Editing), 카드 Wiegand 설정 (Card Wiegand Settings), and 카드 삭제 (Card Deletion). The main window displays a table titled '스마트카드' with the following data:

일련번호	사용자 ID	이름	시작일
176906708	1		1970-01-01

At the bottom left, it says '등록 카드 갯수: 1' (Registered Card Count: 1). At the bottom right, the logo for 'Suprema Inc.' is visible.

3.3.6.

6단계 : 사용자 근태관리 규칙

미리 설정된 근태 관리 규칙 그룹을 사용자에게 적용 하여 보고서 생성 시 참조할

수 있도록 합니다.

3.3.7.

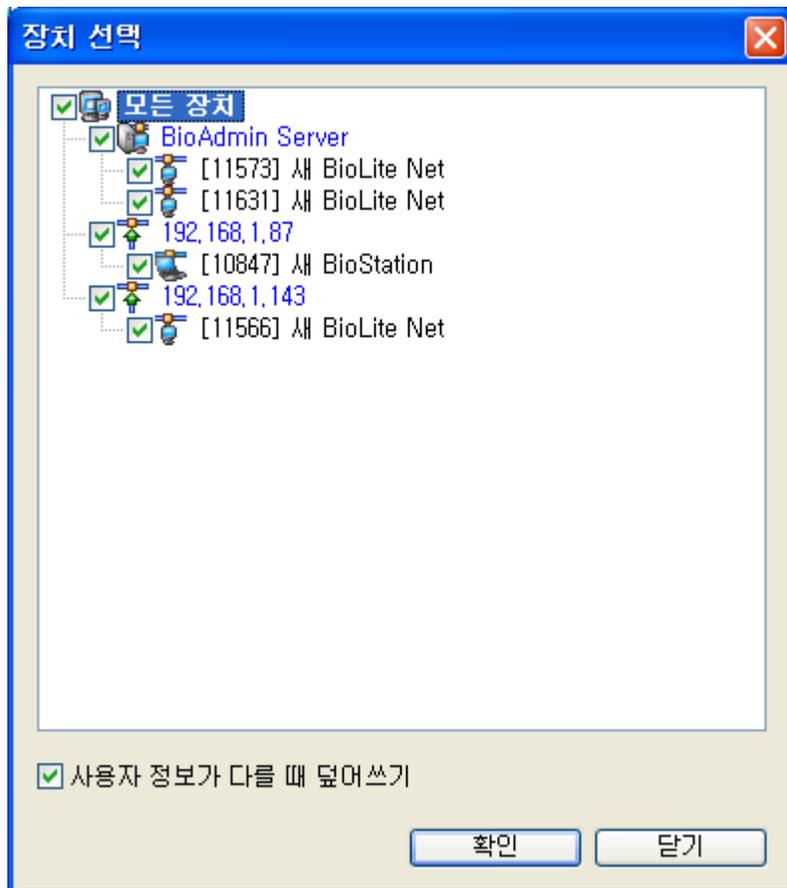
7단계 : 체크된 사용자를 장치에 전송 메뉴로 사용자 등록

체크된 사용자를 장치에 전송은 호스트 PC에서 BioLite Net 장치로 사용자 데이터베이스를 전송하는데 사용됩니다. 사용자 ID, 지문정보, 출입 그룹과 보안 등급과 같은 사용자 정보가 이 과정을 통해 전송됩니다.

- 등록된 사용자 확인하기

<input checked="" type="checkbox"/>	사용자 ID	이름	회사	부서	직책	지문등록수	활...
<input checked="" type="checkbox"/>	796	고원창				1	예
<input type="checkbox"/>	798	황훈아				1	예
<input type="checkbox"/>	804	강병일				1	예
<input type="checkbox"/>	806	강세진				1	예

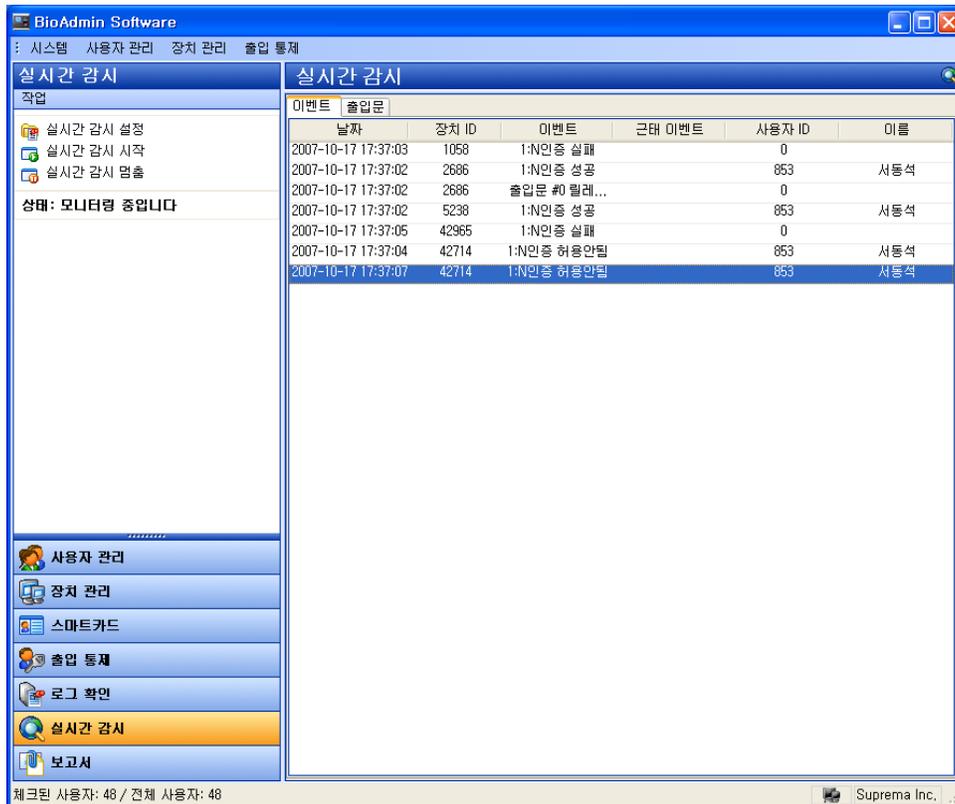
- 체크된 사용자를 장치에 전송 버튼을 클릭하고 장치로 체크 후 선택 버튼을 클릭합니다.



장치 별 사용자 관리 버튼을 눌러 장치를 클릭합니다. 사용자 정보영역이 노란색으로 표시되어 있다면, 사용자 정보가 장치로 성공적으로 전송되었음을 나타냅니다.

3.3.8. 8단계 : 실시간 감시

- 실시간 감시 메뉴를 선택하면 실시간 감시 화면이 주 윈도우 화면에 나타납니다.
- 실시간 감시 설정 메뉴를 선택하고 실시간 감시여부를 더블 클릭합니다. 저장하려면 확인 버튼을 클릭합니다. 연결된 모든 BioLite Net 장치들에 대한 실시간 감시를 시작하려면 실시간 감시 시작을 선택합니다.
- 출입문 감시 - 만약 출입문 설정이 되어 있다면 출입문 감시 페이지를 통해서 각 출입문의 상태를 파악할 수 있으며 출입문 제어 및 경보 해제를 할 수 있습니다. 이곳에서 해제한 경보나 이벤트 등은 실제 장치에 적용되지 않고, PC상에서 표시되는 사항만 해제하게 되며, 출입문 제어만 실제 장치에 적용됩니다.



3.3.9. 9단계 : 로그 확인

- 로그확인 메뉴를 선택하면 로그 리스트 윈도우가 주 윈도우에 표시됩니다.
- 로그 가져오기 / 예약 전송 설정 클릭 , 장치를 체크한 후 선택버튼을 누르면 호스트 PC상의 로그 데이터베이스에 추가된 이벤트 로그 데이터를 볼 수 있습니다

날짜	장치 ID	이벤트	근태이벤트	사용자 ID	이름	종류
2007-02-26 10:14:23	1539	시스템 시작		0		BioStation
2007-02-26 10:15:28	1539	시스템 시작		0		BioStation
2007-02-26 11:12:16	1539	1:N인증 실패		0		BioStation
2007-02-26 11:16:25	1539	1:N인증 실패		0		BioStation
2007-02-26 11:16:34	1539	1:N인증 실패		0		BioStation
2007-02-26 11:16:53	1539	등록 성공		853	서동석	BioStation
2007-02-26 11:17:00	1539	1:N인증 성공		853	서동석	BioStation
2007-02-26 11:17:00	1539	릴레이 On		0		BioStation
2007-02-26 11:17:03	1539	릴레이 Off		0		BioStation
2007-02-26 11:17:03	1539	1:N인증 성공		853	서동석	BioStation
2007-02-26 11:17:03	1539	릴레이 On		0		BioStation
2007-02-26 11:17:06	1539	릴레이 Off		0		BioStation

3.3.10. 10단계 : 보고서 리포트

- 보고서 메뉴를 선택하면 보고서 목록화면이 주 윈도우에 표시됩니다. 조건설정에서 회사명, 부서명, 사용자 ID, 사용자명을 입력하여 설정할 수 있으며, 기간을 설정하여 일일 보고서와 개인별 보고서로 필요한 보고서 종류를 선택해서 리포트 할 수 있습니다.

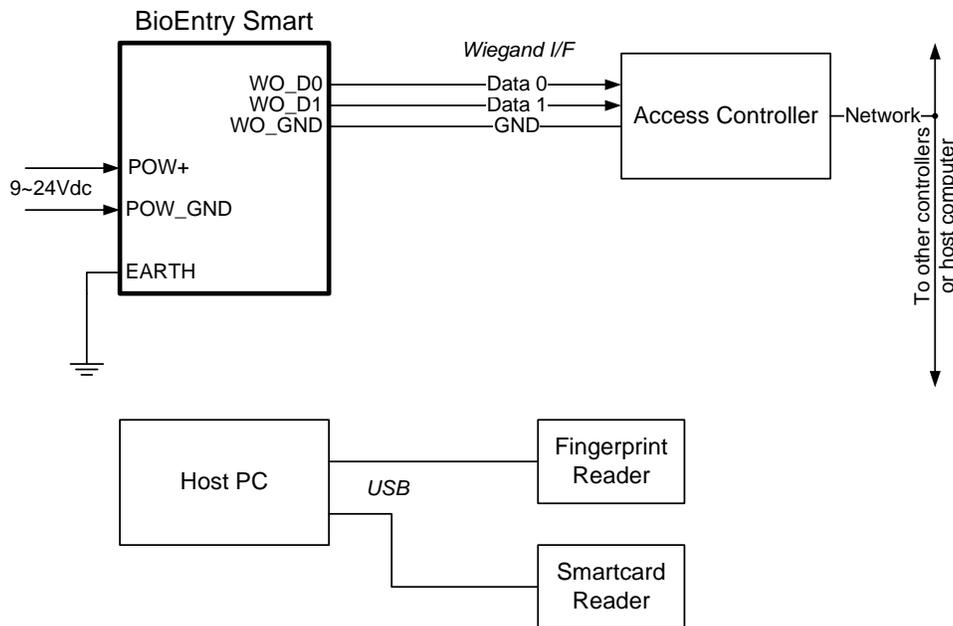
- **로그 가져오기**는 장치에 저장된 로그를 가져오는 버튼이며, **보고서 목록 갱신** 버튼은 장치에서 가져온 로그를 보고서 형태로 날짜 별, 개인별로 나열하여 출력하기 이전 화면을 구현시키는 버튼입니다. 마지막으로 **보고서 미리 보기** 버튼으로 리포트형태의 보고서를 미리 보기 위한 버튼입니다. 인쇄 버튼을 눌러 인쇄를 합니다.

3.4. BioEntry Smart와 함께 빠른 시작

이 절에서는 **USB** 지문 스캐너와 등록 장치로서 스마트카드를 사용하는 **BioEntry Smart**를 작동시키는 기본적인 과정을 설명합니다.

3.4.1. 1단계 : 하드웨어 설치

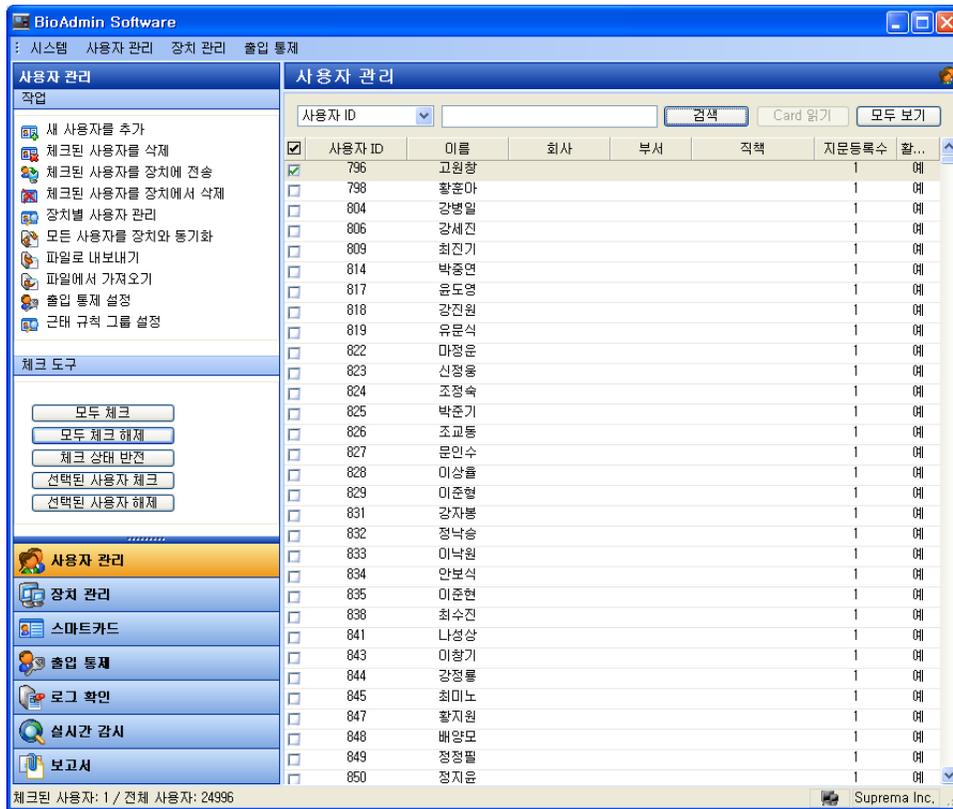
이 하드웨어 환경설정에서, 장치는 호스트 **PC**와 연결되지 않고 **Wiegand** 인터페이스를 통해 외부의 컨트롤러와 연결됩니다. 컨트롤러가 **BioEntry** 장치에서 기본으로 설정된 표준 **26비트 Wiegand** 포맷을 지원한다고 가정합니다. 아래 환경 설정에 따라 장치를 컨트롤러에 연결하십시오.



설치에 대해 더 구체적인 사항은 **BioEntry** 설치 안내서나 **BEACon** 사용설명서를 참조하시기 바랍니다.

3.4.2. 2단계 : 사용자 등록

- **BioAdmin** 소프트웨어를 실행합니다.
- 로그인ID와 패스워드를 입력합니다.
- 주 메뉴에서 **사용자 관리**를 선택하면 사용자 관리 페이지가 주 윈도우에 나타납니다.

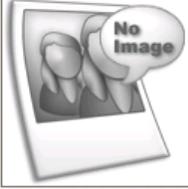


- 작업 윈도우에서 새 사용자 추가 메뉴를 선택하면 팝업 윈도우가 나타납니다.

사용자 정보 [X]

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

개인 정보

 사용자 ID: [11] 사진 및 개인 인증화면 편집

이름: []

회사: [사용 안함] ...

부서: [사용 안함] ...

직책: [사용 안함] ...

상세정보

전화번호: []

핸드폰: []

이메일: []

성별: [남자]

생년월일: [2007-10-17]

시작일: [1970-01-01]

만료 일시: [2030-12-31] [0] 시

출입 통제

출입 상태: 활성화

그룹 1: [전체 출입]

그룹 2: [사용 안함]

그룹 3: [사용 안함]

그룹 4: [사용 안함]

인증 제한 (BioStation 전용)

제한 횟수: [0] 회

인증 간격(분): [0] 분

추가 정보

비밀번호: []

사용자 등급: [일반]

[확인] [취소]

- 사용자 정보 탭에 사용자 정보를 입력합니다.

사용자 정보

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

개인 정보

사용자 ID: 853 사진 및 개인 인증화면 편집

이름: 서동석

회사: 슈프리마

부서: R&D

직책: 선임연구원

상세정보

전화번호:

핸드폰:

이메일:

성별: 남자

생년월일: 1970-06-14

시작일: 1970-01-01

만료 일시: 2030-12-31 0 시

출입 통제

출입 상태: 활성화

그룹 1: 전체 출입

그룹 2: 사용 안함

그룹 3: 사용 안함

그룹 4: 사용 안함

인증 제한 (BioStation 전용)

제한 횟수: 0 회

인증 간격(분): 0 분

추가 정보

비밀번호:

사용자 등급: 일반

확인 취소

- 개인정보에서는 회사, 부서, 직책은 콤보 박스에서 선택할 수 있습니다.
- 새로운 회사, 부서 또는 직책 정보를 추가하려면 ... 버튼을 누르거나, 정보 입력 창에 회사, 부서, 직책 명을 입력 후 **추가** 버튼을 누릅니다. 추가된 정보를 저장하려면 **저장** 버튼을 누릅니다.
- 상세정보에서는 전화번호, 핸드폰 번호 등 상세정보를 입력을 합니다.

회사명 관리

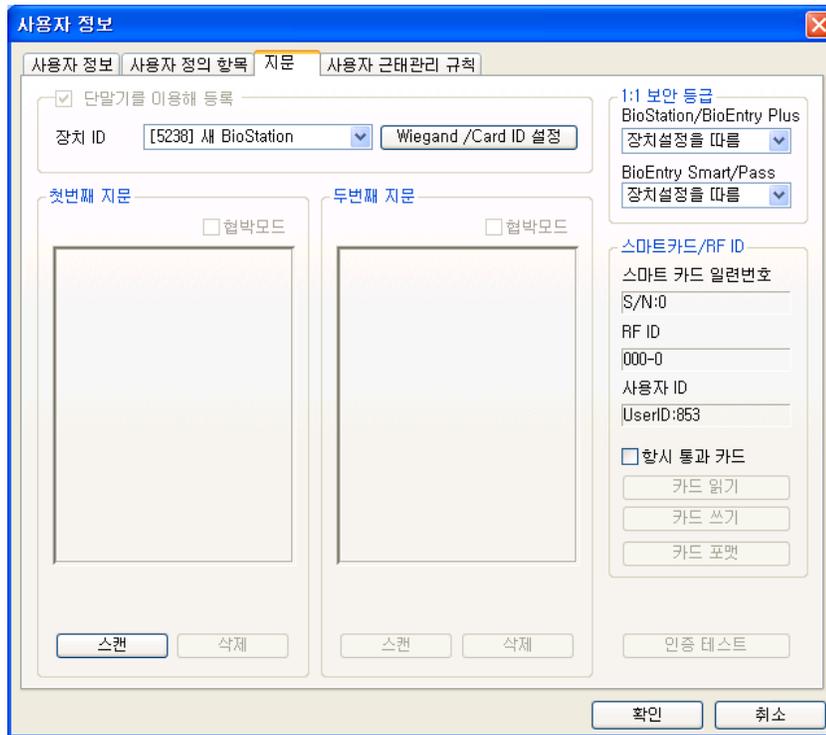
회사명관리 추가

슈프리마 수정

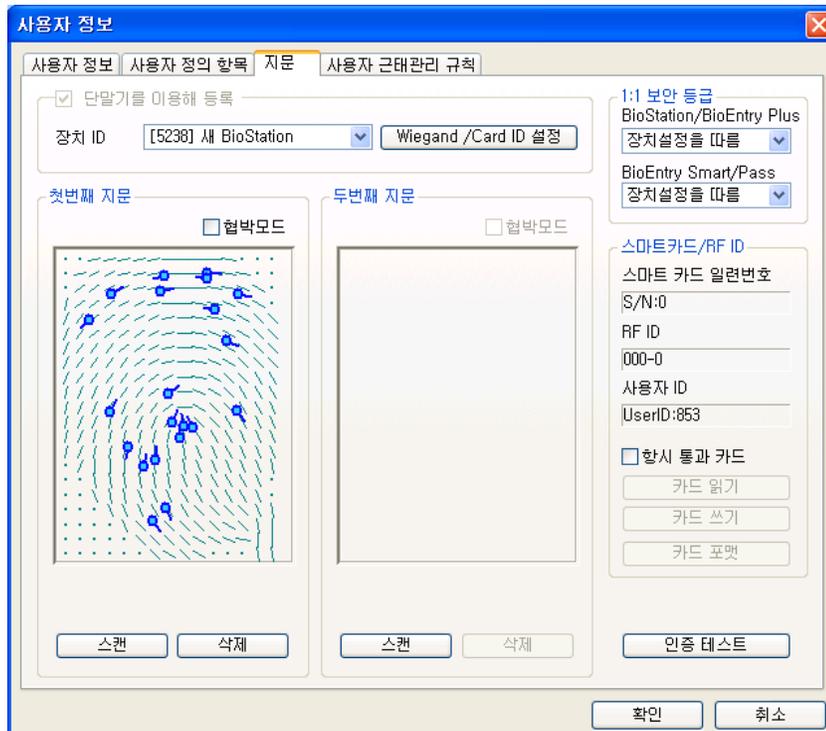
삭제

닫기

- 사용자 지문인식정보를 등록하기 위해 **지문** 탭을 클릭합니다.

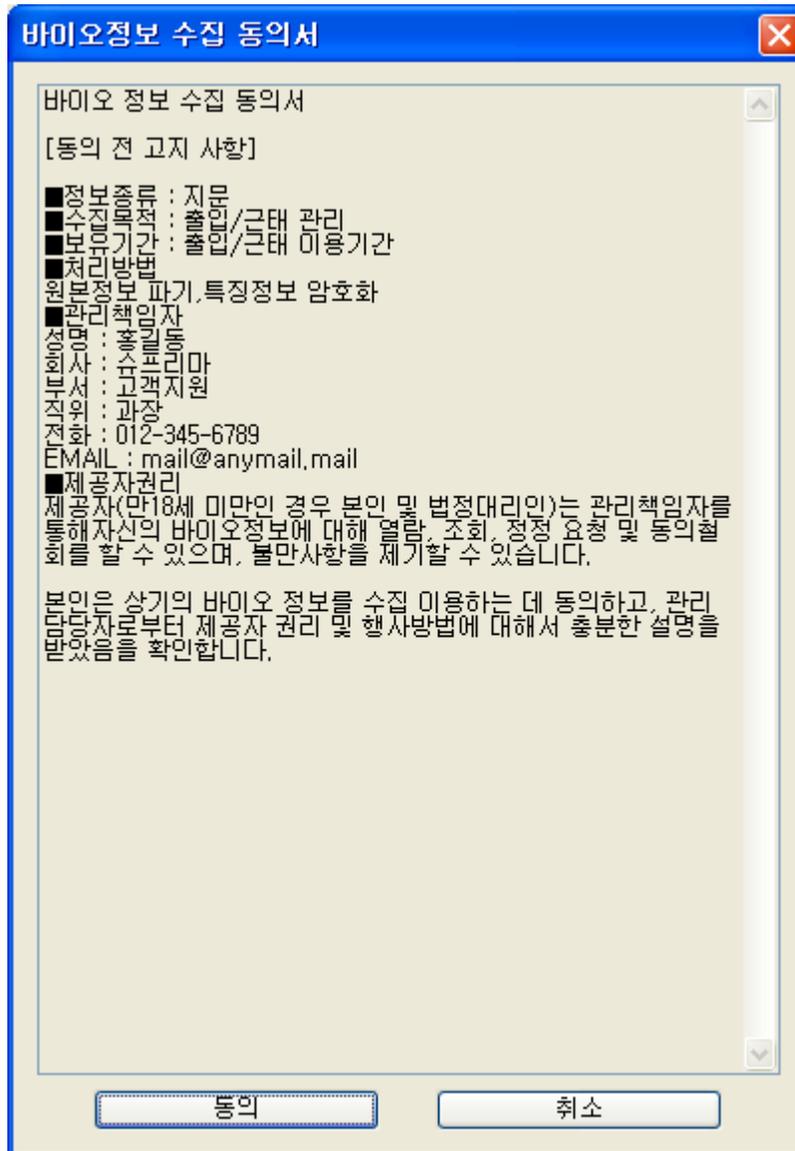


- 스캔 버튼을 누르고 USB 지문 스캐너에 손가락을 두 번 대어 첫 번째 지문 정보를 입력합니다.

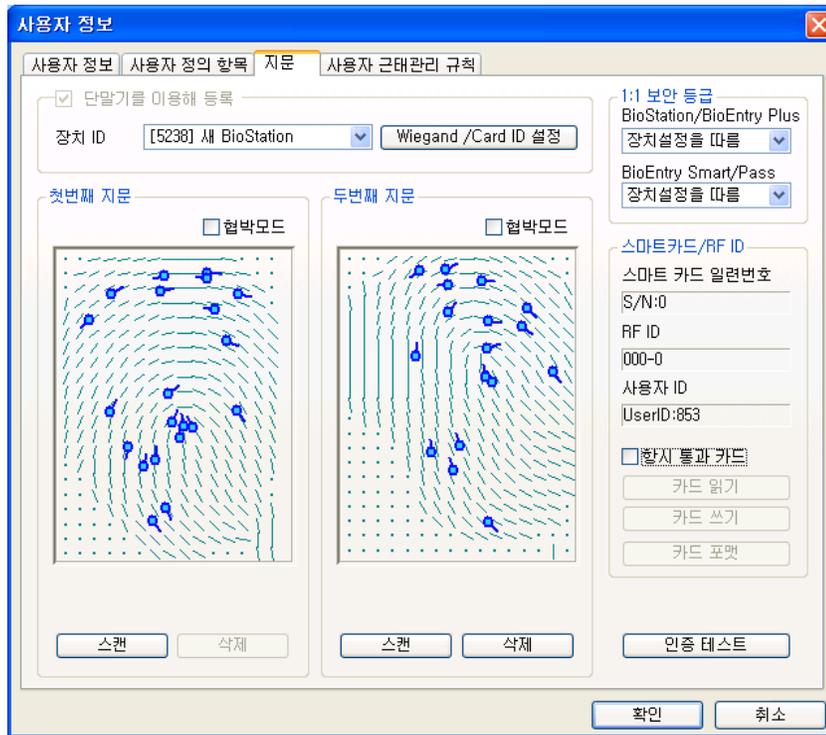


- 이 때, 바이오 정보보호 가이드가 활성화 되어 있다면 바이오 정보 수집 동의

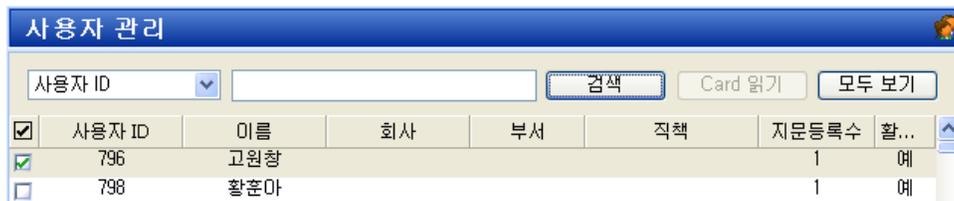
서가 나타나며, 동의하지 않는 경우 지문을 입력 받지 않습니다. 이 동의서는 새로운 사용자 정보 다이얼로그를 볼 때마다 나타납니다.



- 첫 번째 지문인식정보를 입력하는 과정과 같이 두 번째 지문인식정보를 입력합니다.



- 등록 과정을 종료하려면 **확인** 버튼을 클릭합니다. 그러면 사용자 리스트 윈도우에서 등록된 사용자에 대한 정보를 볼 수 있습니다. 이는 사용자 정보가 호스트 PC상의 데이터베이스에 추가되었음을 의미합니다.



3.4.3. 3단계 : 사용자의 스마트카드 발급하기

- 사용자 리스트 상의 등록된 사용자를 더블 클릭합니다. 그러면 사용자 정보 윈도우가 나타나 등록된 사용자의 정보를 보여줍니다.
- 사용자 정보 윈도우에서 **지문** 탭을 클릭합니다.
- 스마트카드를 PC USB 스마트카드 장치에 놓고 **카드쓰기** 버튼을 클릭합니다.

스마트카드/RF ID

S/N:0

RF ID:0

UserID:853

할시 통과 카드

카드 읽기

카드 쓰기

카드 포맷

- 처음 시도 할 때 사이트 키 관리 윈도우가 나타납니다. 키 입력 필드가 공백이면 초기 설정 값이 사용됩니다. 알맞은 사이트 키를 입력하고 **확인** 버튼을 눌러 발급 과정을 마칩니다.

사이트키 입력

현재 사이트키

사이트키 변경

사이트키 확인

확인

취소

- 사용자 리스트 윈도우에서 사용자 데이터가 저장된 스마트카드의 일련 번호를 볼 수 있습니다.

스마트카드/RF ID

S/N:1077514292

RF ID:0

UserID:853

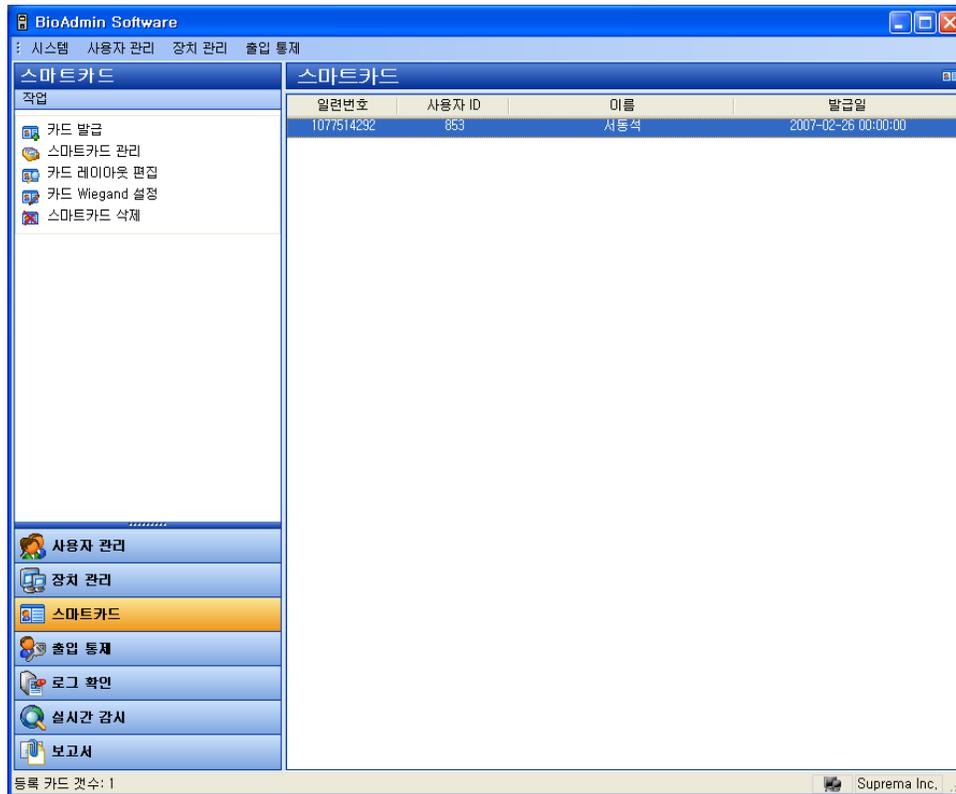
할시 통과 카드

카드 읽기

카드 쓰기

카드 포맷

- 스마트카드 메뉴를 선택하면 리스트에 추가된 스마트카드를 볼 수 있습니다.



3.4.4. 4단계 : 외부 컨트롤러에 사용자 ID 등록

사용자에 대한 Wiegand 스트링을 받아들일 때 출입을 허가하기 위해서는 발급된 사용자 ID를 컨트롤러에도 등록해 주어야만 합니다.

슈프리마의 BEACon 컨트롤러를 사용한다면 이러한 부가적인 등록과정은 필요 없습니다.

3.4.5. 5단계 : 인증 테스트

사용자의 스마트카드를 이용하여 인증을 테스트하는 과정은 다음과 같습니다.

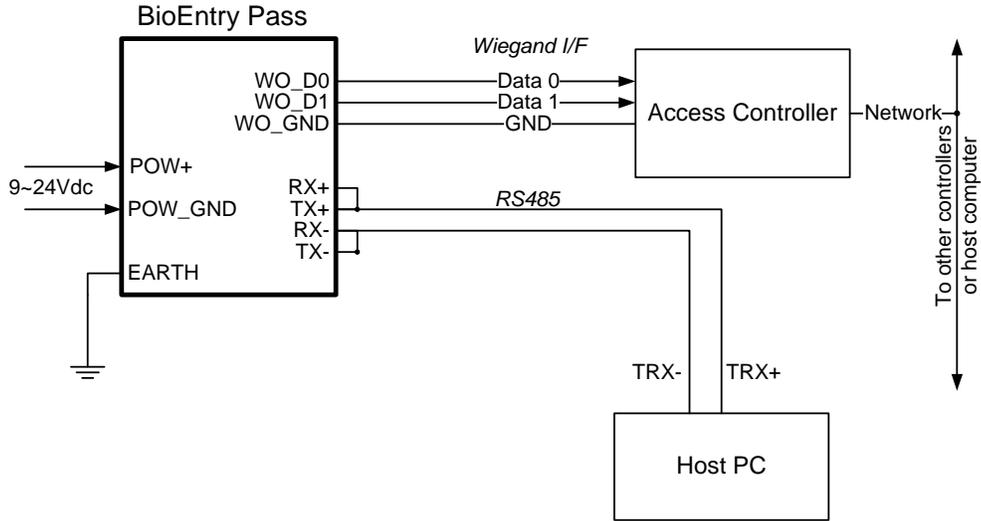
- 우선 사용자의 스마트카드를 센서아래 부분 장치의 전면에 가져다 댑니다. 그러면, 장치가 인증을 위해 손가락을 스캔 하려고 대기 중 이라는 표시로 황색 LED가 깜박입니다.
- 센서 위에 손가락을 대십시오. 사용자가 성공적으로 인증되었다면 녹색 LED가 한 번의 비프 음과 함께 나타납니다. 실패했다면 빨강 LED가 3번의 비프 음과 함께 나타납니다..
- 인증에 성공하면 Wiegand 스트링이 컨트롤러에 보내지고, 컨트롤러는 릴레이를 동작시킵니다.

3.5. BioEntry Pass와 함께 빠른 시작

이 절에서는 PC 장치가 없는 BioEntry Pass를 작동시키는 기본적인 과정에 대해 기술하고 있습니다.

3.5.1. 1단계 : 하드웨어 설치

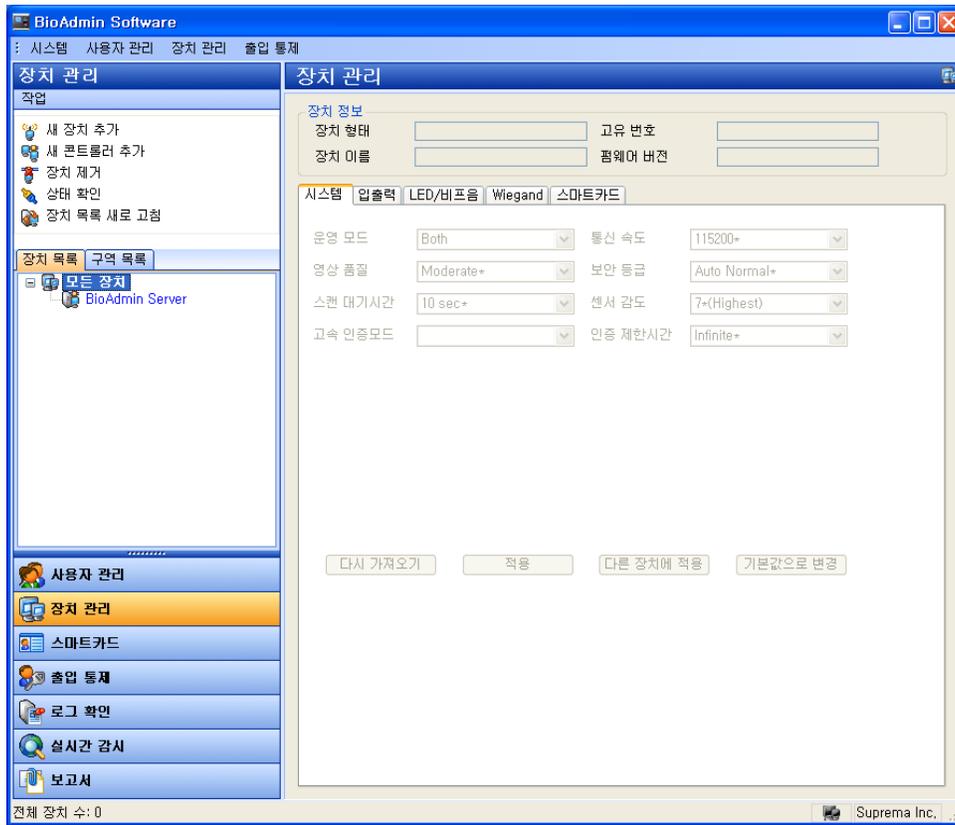
이 환경설정에서, 리더는 **Wiegand** 인터페이스를 통해 외부 컨트롤러와 연결되고 또한 **RS485** 인터페이스를 통해서 호스트 **PC**와 연결됩니다. 컨트롤러가 **BioEntry** 장치에서 기본으로 설정된 표준 26비트 **Wiegand** 포맷을 지원한다고 가정합니다.



설치에 관한 더 상세한 정보는 **BioEntry** 설치 안내서 또는 **BEACon** 사용설명서를 참조하시기 바랍니다.

3.5.2. 2단계 : 새 장치 검색

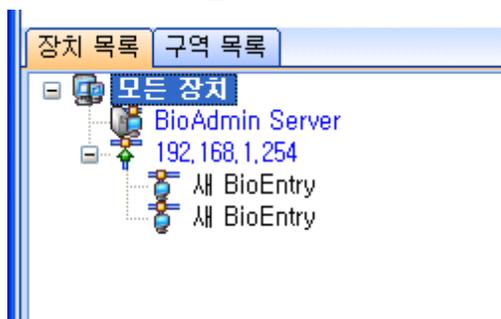
- **BioAdmin** 소프트웨어를 실행합니다.
- 로그인ID와 패스워드를 입력합니다.
- 주 메뉴상에서 **장치관리**를 선택하면 주 윈도우에 장치 관리 페이지가 나타납니다.



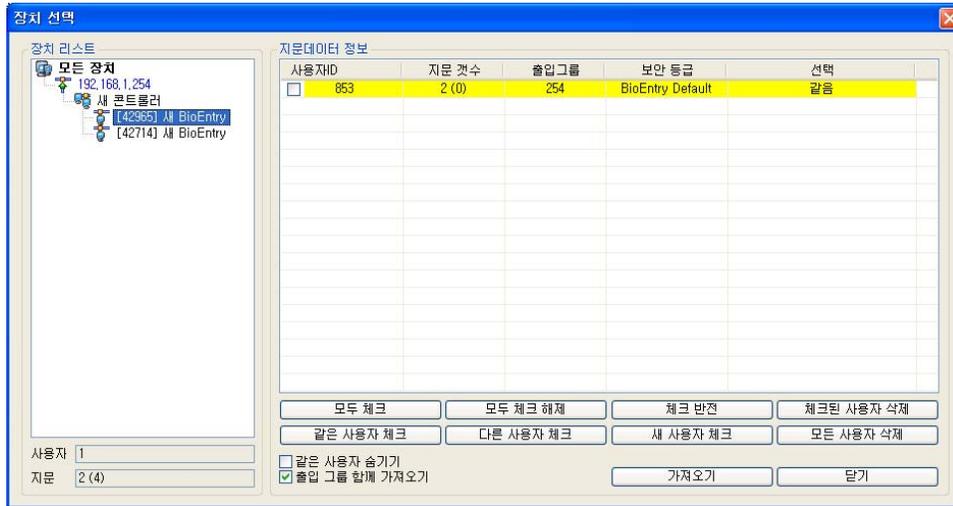
- 새 장치 검색 메뉴를 선택하고, BioEntry 검색을 클릭한 뒤 직렬포트와 TCP/IP 중 사용할 통신을 선택한 후에 검색버튼을 누릅니다. 검색결과에서 장치를 찾게 되면 몇 개의 장치를 선택했습니다 라는 결과리포트가 쓰여진 후 확인 버튼을 누르시면 장치가 선택됩니다.



- 장치와 잘 연결되었다면, 새로운 장치 ID와 장치와 연결된 통신방식까지 장치 리스트 윈도우에 나타납니다.



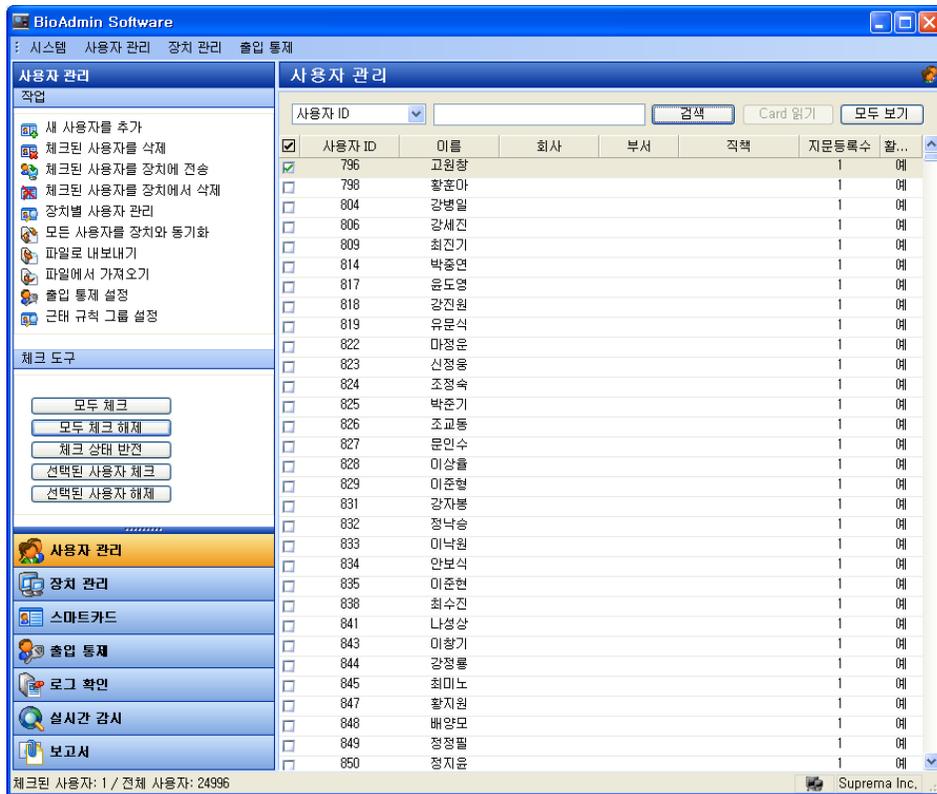
- 주 메뉴상의 사용자 관리 버튼을 선택하고 작업 윈도우상에서 장치 별 사용자 관리를 선택합니다.
- 장치를 선택하면 사용자ID, 지문 개수, 출입그룹, 보안등급, 선택 등 지문 정보가 표시됩니다.



3.5.3.

3단계 : 사용자 등록

- 사용자 관리 메뉴를 선택하면 주 윈도우에 사용자 관리 페이지가 나타납니다.

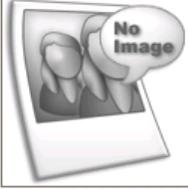


- 작업 윈도우상의 새 사용자를 추가 메뉴를 선택하면 팝업 윈도우가 나타납니다.

사용자 정보 [X]

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

개인 정보

 사용자 ID: [11] 사진 및 개인 인증화면 편집

이름: []

회사: [사용 안함] ...

부서: [사용 안함] ...

직책: [사용 안함] ...

상세정보

전화번호: []

핸드폰: []

이메일: []

성별: [남자]

생년월일: [2007-10-17]

시작일: [1970-01-01]

만료 일시: [2030-12-31] [0] 시

출입 통제

출입 상태: 활성화

그룹 1: [전체 출입]

그룹 2: [사용 안함]

그룹 3: [사용 안함]

그룹 4: [사용 안함]

인증 제한 (BioStation 전용)

제한 횟수: [0] 회

인증 간격(분): [0] 분

추가 정보

비밀번호: []

사용자 등급: [일반]

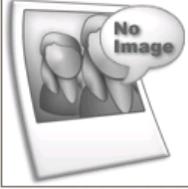
[확인] [취소]

- 사용자 정보 탭에 사용자 정보를 입력합니다.

사용자 정보

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

개인 정보


 사용자 ID: 853 사진 및 개인 인증화면 편집
 이름: 서동석
 회사: 슈프리마
 부서: R&D
 직책: 선임연구원

상세정보

전화번호:
 핸드폰:
 이메일:
 성별: 남자
 생년월일: 1970-06-14
 시작일: 1970-01-01
 만료 일시: 2030-12-31 0 시

출입 통제

출입 상태: 활성화
 그룹 1: 전체 출입
 그룹 2: 사용 안함
 그룹 3: 사용 안함
 그룹 4: 사용 안함

인증 제한 (BioStation 전용)

제한 횟수: 0 회
 인증 간격(분): 0 분

추가 정보

비밀번호: 사용자 등급: 일반

확인 취소

- 콤보 박스를 이용해 회사, 부서, 직책을 선택할 수 있습니다.
- 새로운 회사, 부서 또는 직책 정보를 추가하려면 버튼을 누르거나, 정보 입력 창에 회사, 부서, 직책 명을 입력 후 추가 버튼을 누릅니다. 추가된 정보를 저장하려면 저장 버튼을 누릅니다.

회사명 관리

회사명관리

슈프리마

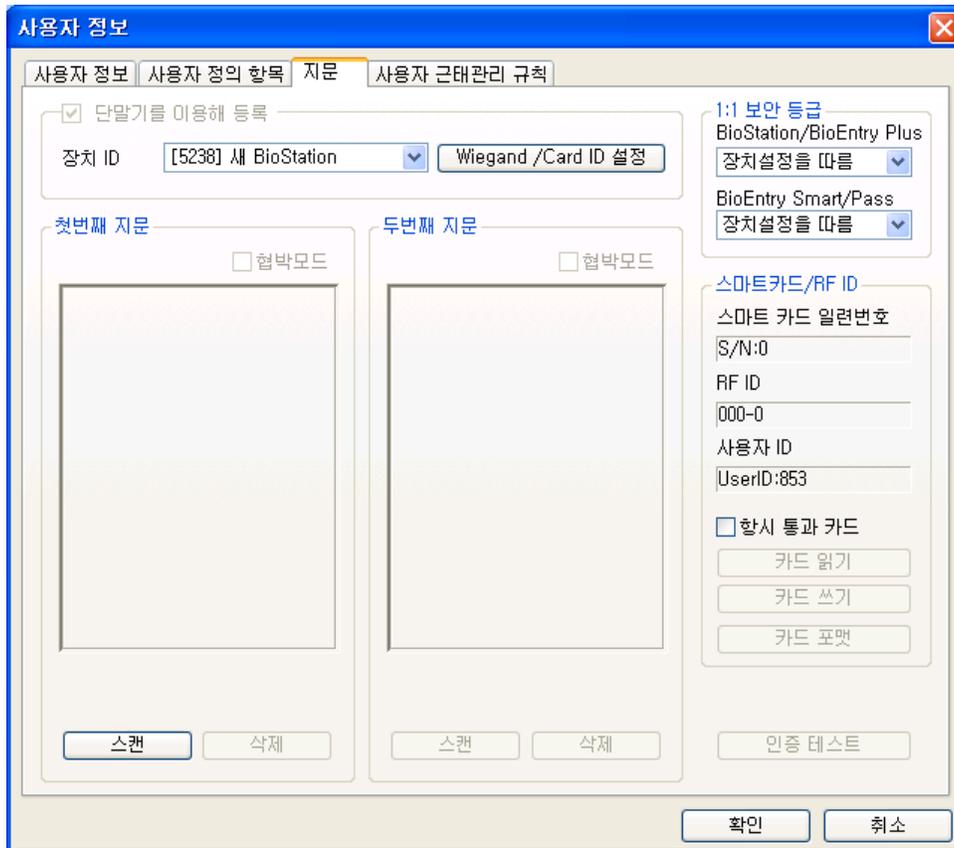
추가

수정

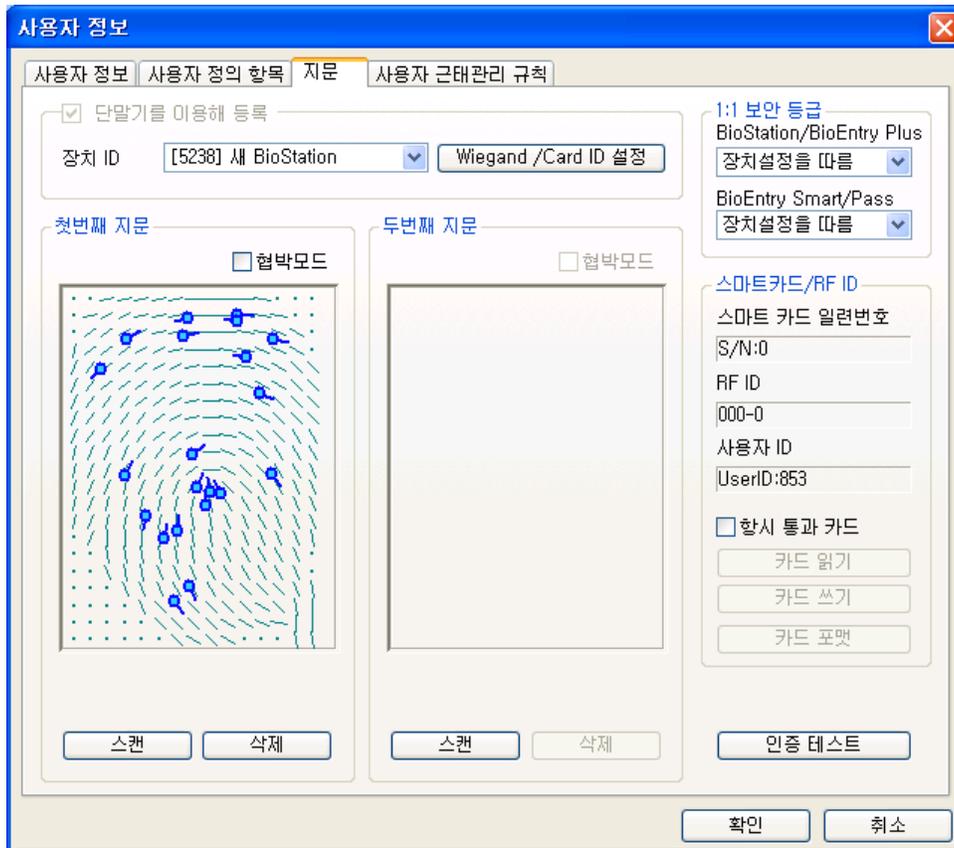
삭제

닫기

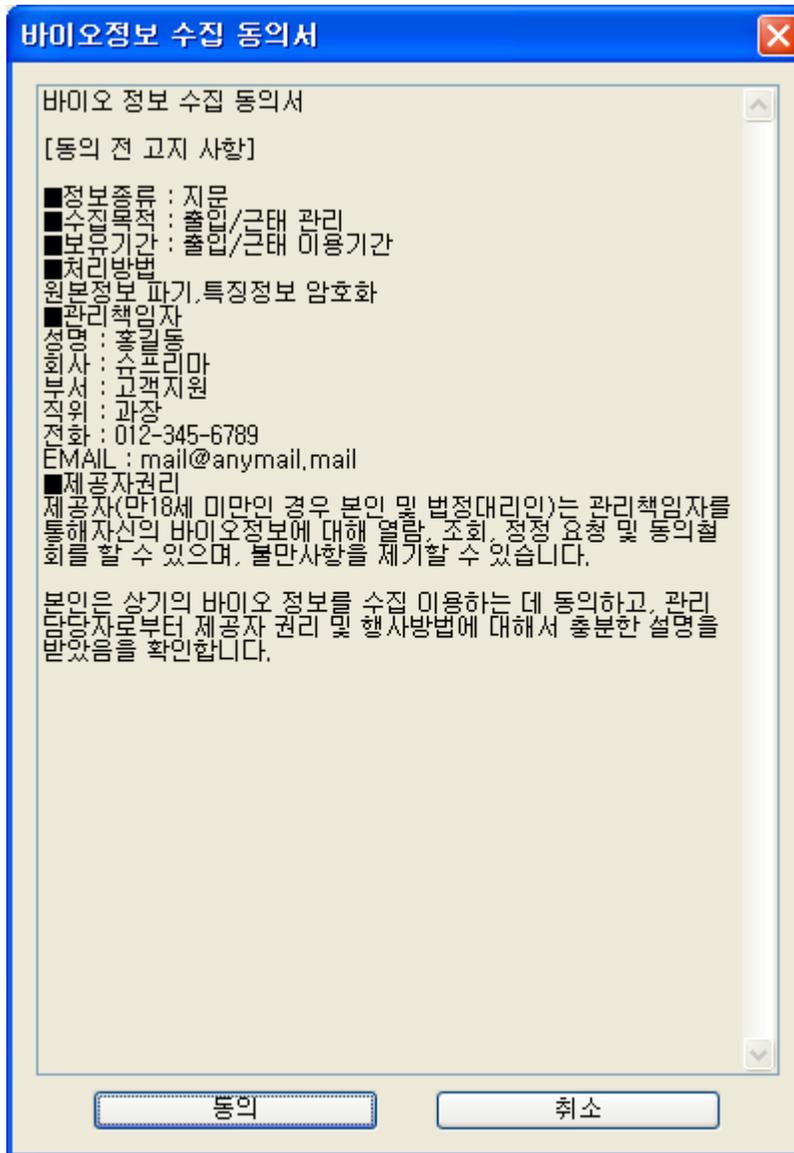
- 사용자 지문인식정보를 등록하기 위해 지문 탭을 클릭합니다.



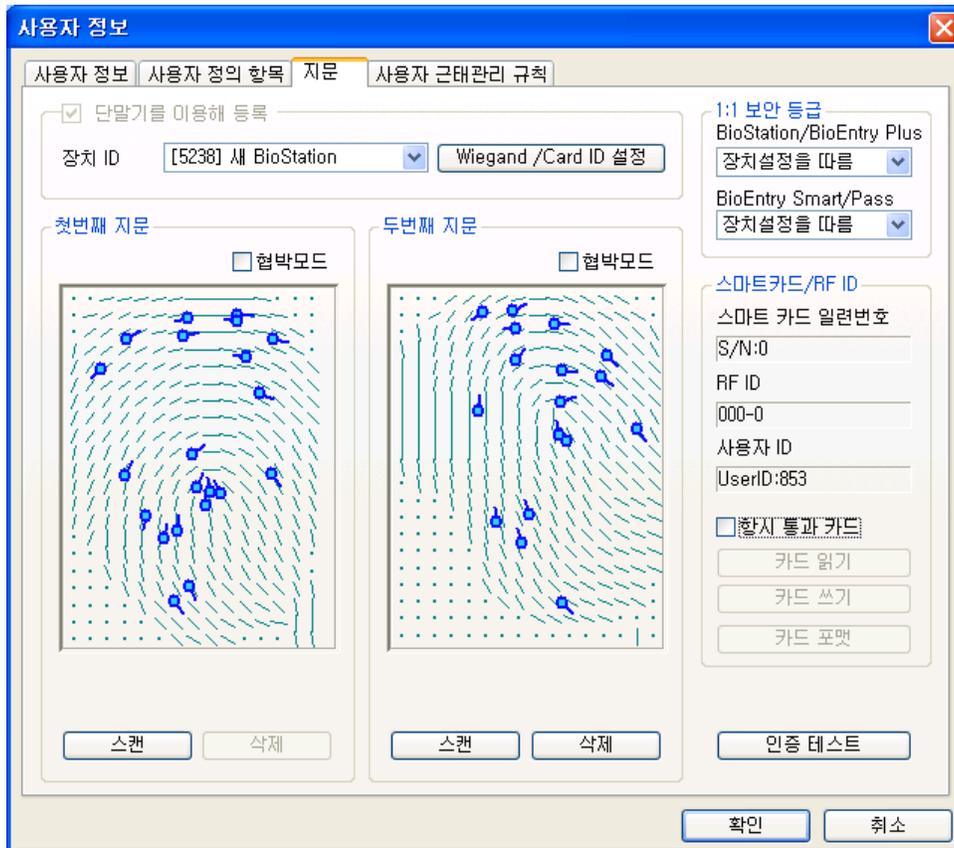
- 스캔 버튼을 누르고 USB 지문 스캐너에 손가락을 두 번 대어 첫 번째 지문 정보를 입력합니다.



- 이 때, 바이오 정보보호 가이드가 활성화 되어 있다면 바이오 정보 수집 동의서가 나타나며, 동의하지 않는 경우 지문을 입력 받지 않습니다. 이 동의서는 새로운 사용자 정보 다이얼로그를 볼 때마다 나타납니다.



- 첫 번째 지문정보를 입력하는 과정과 같이 두 번째 지문정보를 입력합니다.



- 등록 과정을 종료하려면 **확인** 버튼을 클릭합니다. 그러면 사용자 리스트 윈도우에서 등록된 사용자에 대한 정보를 볼 수 있습니다. 이는 사용자 정보가 호스트 PC상의 데이터베이스에 추가되었음을 의미합니다.

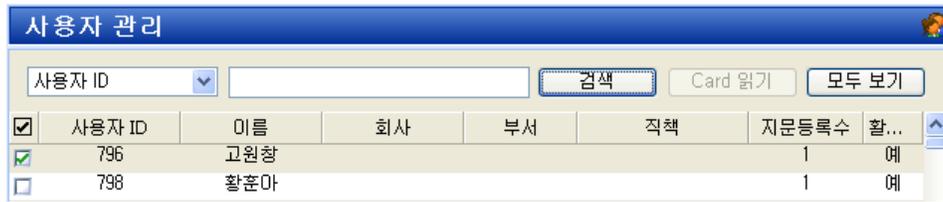
사용자 ID	이름	회사	부서	직책	지문등록수	활...
796	고원창				1	예
798	황훈마				1	예

3.5.4.

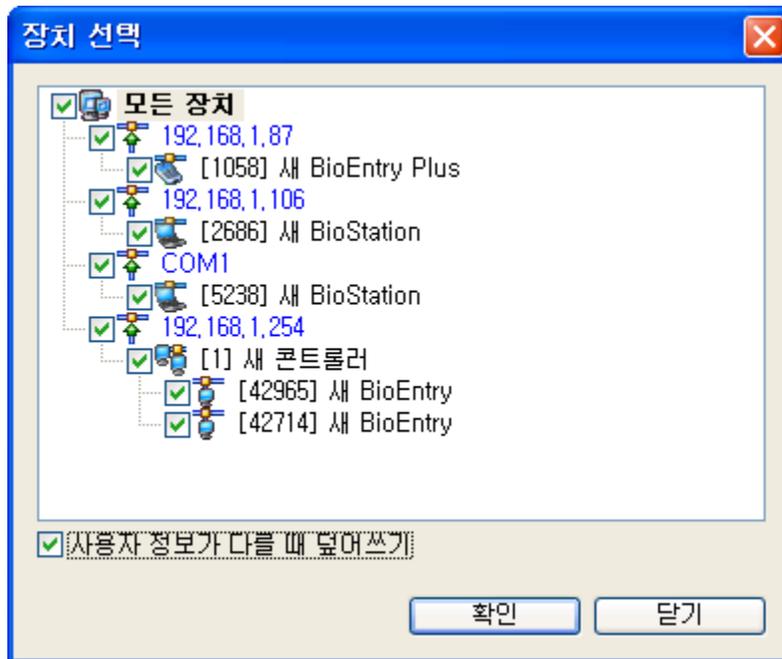
4단계 : 체크된 사용자를 장치에 전송 메뉴로 사용자 등록

체크된 사용자를 장치에 전송은 호스트 PC에서 장치로 사용자 데이터베이스를 전송하는데 사용됩니다. 사용자 ID, 지문정보, 출입 그룹과 보안 등급과 같은 사용자 정보가 이 과정을 통해 전송됩니다.

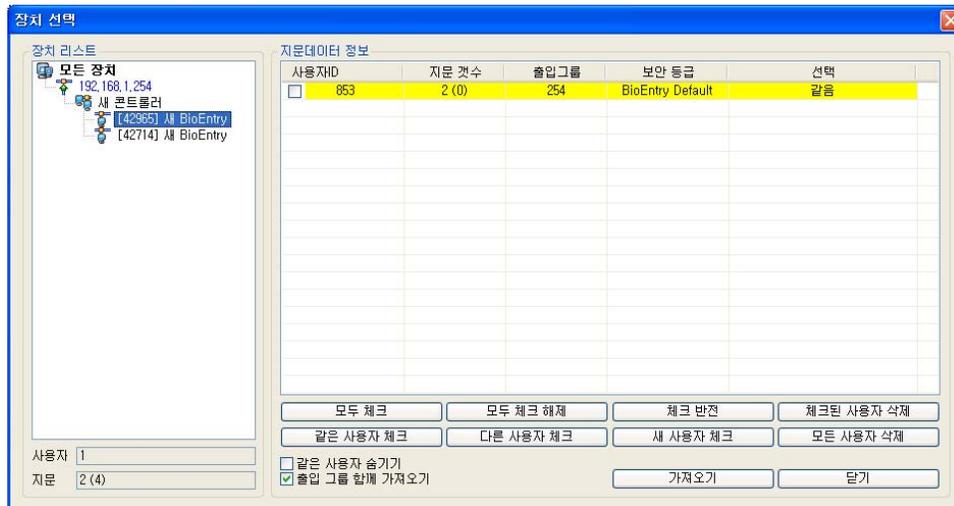
- 등록된 사용자 확인하기



- 체크된 사용자를 장치에 전송 버튼을 클릭하고 장치를 체크 한 후 선택버튼을 클릭합니다.



장치 별 사용자 관리 버튼을 눌러 장치를 클릭합니다. 지문데이터 정보 영역이 노란색으로 표시되어 있다면, 사용자 정보가 장치로 성공적으로 전송되었음을 나타냅니다.



3.5.5. 5단계 : 외부 컨트롤러에 사용자 ID 등록

사용자에 대한 Wiegand 스트링을 받아들일 때 출입을 허가하기 위해서는 발급된 사용자 ID를 컨트롤러에도 등록해 주어야만 합니다.

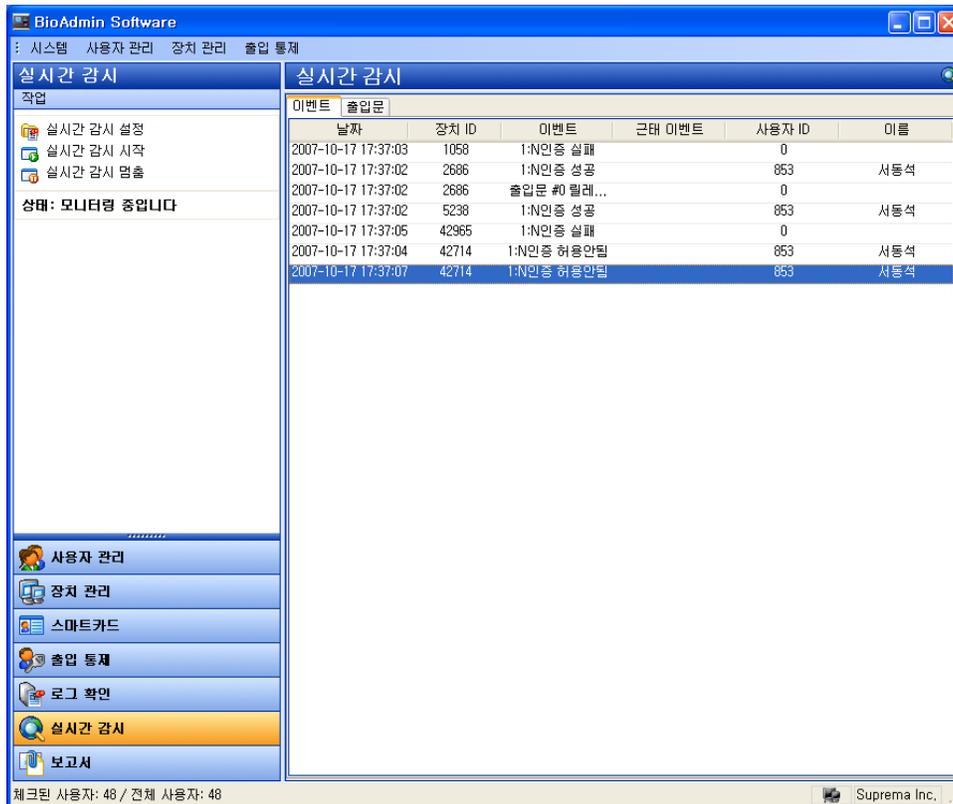
슈프리마의 BEACon 컨트롤러를 사용한다면 이러한 부가적인 등록과정은 필요 없습니다.

3.5.6. 6단계 : 인식 테스트

- 손가락을 스캔 하기 위해 대기하고 있다는 표시로 리더 황색 LED가 느리게 깜박입니다.
- 센서 위에 손가락을 대어 주십시오. 사용자가 성공적으로 인식되었다면 한번의 비프 음과 함께 녹색 LED가 나타납니다. 실패했다면, 빨간 LED가 3번의 비프 음과 함께 표시됩니다.
- 인식에 성공하면 Wiegand 스트링이 컨트롤러에 보내지고, 컨트롤러는 릴레이를 동작시킵니다.

3.5.7. 7단계 : 실시간 감시

연결된 모든 BioEntry 리더들에 대한 실시간 감시를 시작하려면 실시간 감시 시작을 선택합니다.



3.5.8. 8단계 : 로그 확인

- 로그확인 메뉴를 선택하면 로그 리스트 윈도우가 주 윈도우에 표시됩니다. 로그 가져오기 / 예약 전송 설정 버튼을 누르면 호스트 PC상의 로그 데이터베이스에 추가된 이벤트 로그 데이터를 볼 수 있습니다.

The screenshot shows the '로그 확인' (Log Check) window. The table displays the following data:

날짜	장치 ID	이벤트	근태이벤트	사용자 ID	이름	종류
2007-02-26 10:14:23	1539	시스템 시작		0		BioStation
2007-02-26 10:15:28	1539	시스템 시작		0		BioStation
2007-02-26 11:12:16	1539	1:N인증 실패		0		BioStation
2007-02-26 11:16:25	1539	1:N인증 실패		0		BioStation
2007-02-26 11:16:34	1539	1:N인증 실패		0		BioStation
2007-02-26 11:16:53	1539	등록 성공		853	서동석	BioStation
2007-02-26 11:17:00	1539	1:N인증 성공		853	서동석	BioStation
2007-02-26 11:17:00	1539	릴레이 On		0		BioStation
2007-02-26 11:17:03	1539	릴레이 Off		0		BioStation
2007-02-26 11:17:03	1539	1:N인증 성공		853	서동석	BioStation
2007-02-26 11:17:03	1539	릴레이 On		0		BioStation
2007-02-26 11:17:06	1539	릴레이 Off		0		BioStation

4. 사용자 관리

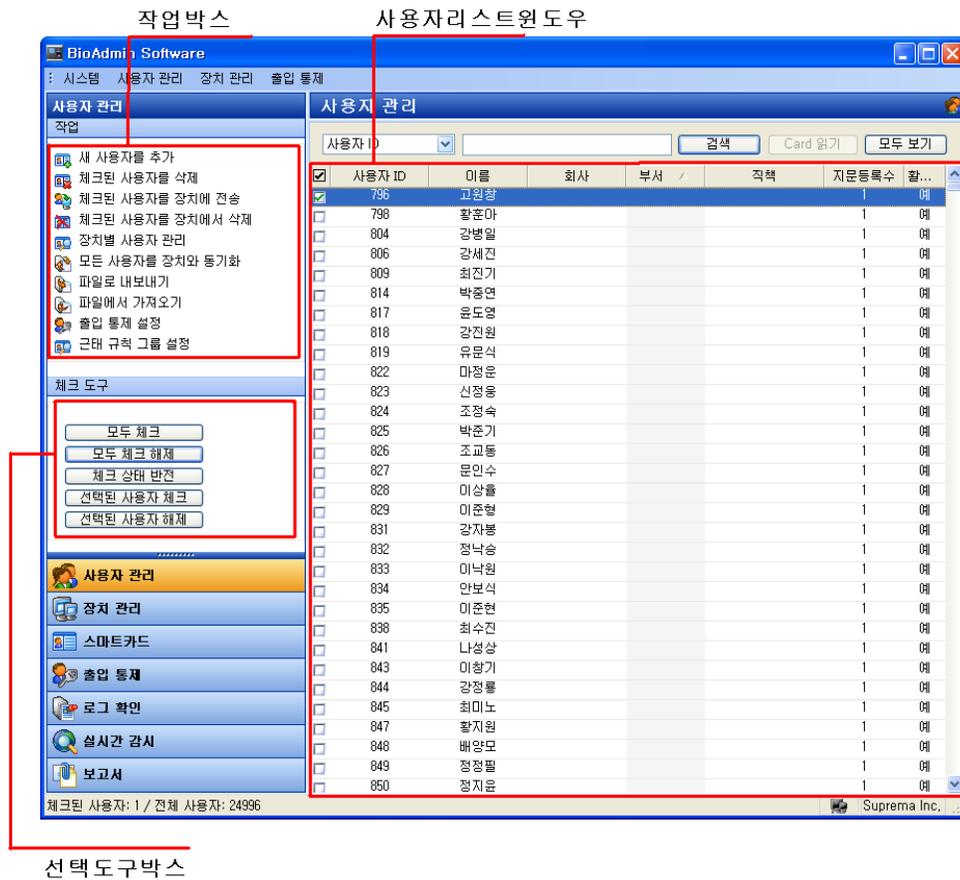
사용자 관리 메뉴는 다음과 같은 사항들을 포함합니다.:

- 새 사용자를 추가

- 체크된 사용자를 삭제
- 체크된 사용자를 장치에 전송
- 체크된 사용자를 장치에서 삭제
- 장치 별 사용자 관리
- 모든 사용자를 장치와 동기화
- 파일로 내보내기
- 파일에서 가져오기

4.1. 사용자 관리 페이지의 구성

사용자 관리 메뉴를 선택하면 사용자 관리 페이지가 주 윈도우에서 갱신됩니다.



사용자 관리 페이지는 3개의 영역으로 나누어 집니다.

- 사용자 리스트 윈도우
 - 사용자 데이터베이스는 호스트 PC에서 관리됩니다. 사용자 관리 페이지에는 사용자 데이터베이스의 구체적인 리스트와 요약 정보가 포함되어 있습니다.
- 체크 도구 박스
 - 체크 도구 박스에는 사용자를 선택하는 버튼들이 있습니다.
- 작업 박스

작업 박스에는 사용자 관리 페이지의 기본 동작들을 제어하는 버튼들이 있습니다.

4.2. 사용자 리스트 윈도우

사용자 리스트 윈도우는 사용자들에 대한 다음과 같은 정보들을 포함하고 있습니다.

- 사용자 ID, 이름, 회사, 부서, 직책 등 기본적인 내용과 지문등록 수 및 활성화 상태를 보여줍니다.
- 사용자의 ID를 마우스로 두 번 클릭하게 되면 사용자정보 윈도우 창이 띄워집니다. 사용자정보에는 사용자정보, 사용자정의항목, 지문, 사용자 근태관리규칙의 4가지 탭이 있습니다.
- 지문정보 (지문 영상은 저장되지 않음)

Note : 출입그룹 설정에서 활성화란? 호스트PC의 사용자 데이터를 장치로 전송할 때 사용되며, 사용자 리스트에서의 체크된 사용자를 장치로 전송할 때 활성화가 체크 되어 있지 않으면 사용자 데이터가 전송되지 않으며 장치내의 데이터는 삭제됩니다.

예를 들면) 과건 , 장기 휴가 등 출입그룹에서 제외되어서 비활성화된 상태로 있다가 복귀를 했을 때 활성화를 시켜서 사용자 리스트를 관리합니다.

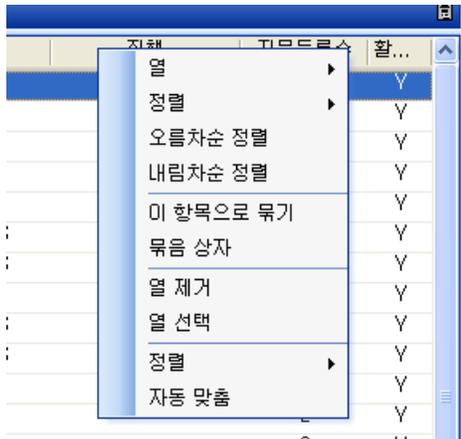
4.3. 사용자 리스트 표시 설정

사용자 리스트 표시를 설정할 수 있으며, 구체적인 동작방법은 다음과 같습니다.

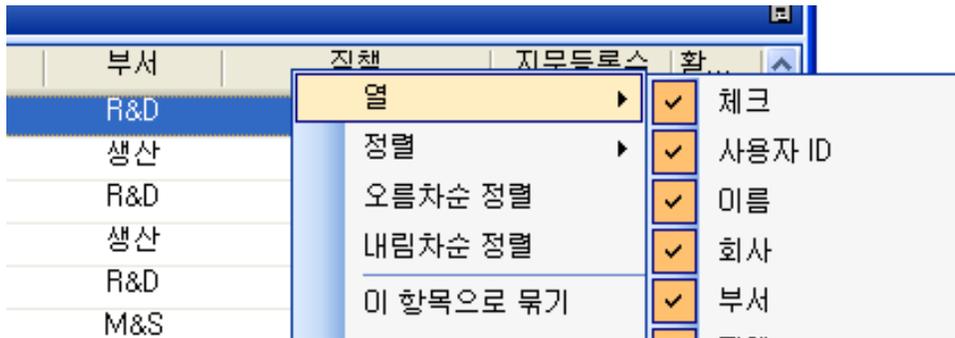
- 사용자 리스트의 행 머리 위에 마우스를 대고 오른쪽 버튼을 클릭합니다.

Note : 행 머리란? 사용자 리스트의 윈도우 창에서 사용자 ID, 이름, 회사, 부서 등 행의 위쪽에 있는 부분을 행머리라고 합니다.

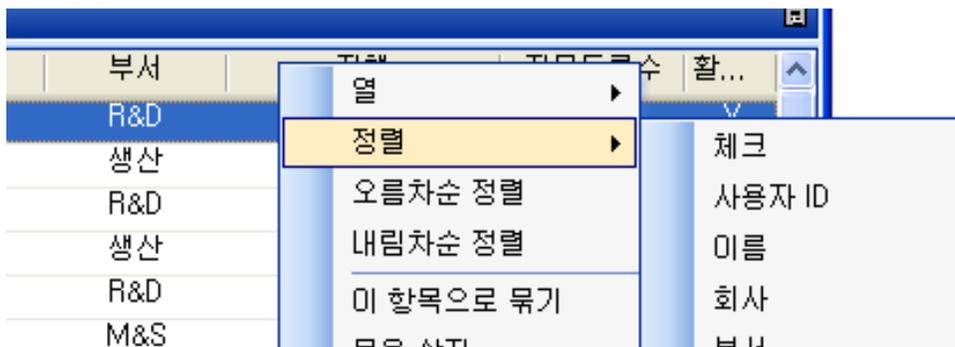
<input checked="" type="checkbox"/>	사용자 ID	이름	회사	부서	직책	지문등록수	활...
<input checked="" type="checkbox"/>	796	고원창				1	예
<input type="checkbox"/>	798	활훈마				1	예



- 열 버튼을 누르고 사용자 리스트 윈도우 창에 보이게 하려는 행들을 표시합니다.



- 정렬 버튼을 클릭하고 사용자 리스트를 정렬시키는 기준이 되는 행을 선택합니다.



- 사용자 리스트를 오름차순으로 배열하려면 **오름차순 정렬** 버튼을 클릭합니다.
- 사용자 리스트를 내림차순으로 배열하려면 **내림차순 정렬** 버튼을 클릭합니다.
- 사용자 리스트를 특정 행에 대한 그룹으로 관리하려면 행 머리에 마우스커서를 두고 마우스 오른쪽쪽을 눌러서 **이 항목으로 묶기** 버튼과 **묶음 상자** 버튼을

클릭하면 행을 헤더박스에 끌어 놓음으로써 특정 행을 그룹에 추가하며 특정 행에 대한 배열을 할 수 있습니다.

예를 들면) 부서를 헤더박스에 끌어놓으면 각각의 부서별로 사용자 리스트가 정렬이 됩니다.

부서	사용자 ID	이름	회사	부서	직책	지문등록수	활...
	1205	신군생	슈프리마	M&S	대리	2	예
	1211	강인하	슈프리마	M&S	과장	2	예
	3786	전현복	슈프리마	M&S	과장	2	예
	4582	강일환	슈프리마	M&S	대리	2	예
	4583	홍경훈	슈프리마	M&S	사원	2	예
	4594	서부자	슈프리마	M&S	사원	2	예
	4595	도오희	슈프리마	M&S	사원	2	예
	4596	이의호	슈프리마	M&S	사원	2	예
	4597	강순임	슈프리마	M&S	대리	2	예
	4598	문진기	슈프리마	M&S	과장	2	예
	4599	황동순	슈프리마	M&S	대리	2	예
	10400	강세진	슈프리마	M&S	사원	2	예
	15792	이철인	슈프리마	M&S	사원	2	예
	15798	이현식	슈프리마	M&S	사원	2	예
	16070	강영현	슈프리마	M&S	사원	2	예
	18852	문명순	슈프리마	M&S	부장	2	예
	19789	배동욱	슈프리마	M&S	부장	2	예
	33044	문보기	슈프리마	M&S	대리	2	예
	42110	오숙경	슈프리마	M&S	대리	2	예
	59644	류경철	슈프리마	M&S	대리	2	예
	64259	박형원	슈프리마	M&S	과장	2	예
	64999	이준식	슈프리마	M&S	부장	2	예
부서: 생산							
	861	이낙원	슈프리마	생산	대리	2	예
	1144	경호영	슈프리마	생산	과장	2	예
	4465	가보현	슈프리마	생산	사원	2	예
	4580	한백영	슈프리마	생산	대리	2	예
	4584	황종욱	슈프리마	생산	사원	2	예
	4585	박민형	슈프리마	생산	과장	2	예
	4586	윤호영	슈프리마	생산	부장	2	예
	4587	윤봉근	슈프리마	생산	사원	2	예

4.4. 사용자 검색

등록된 사용자가 많은 경우 사용자ID, 사용자 이름 및 등록된 카드/카드 번호를 통해서 사용자를 검색할 수 있습니다.

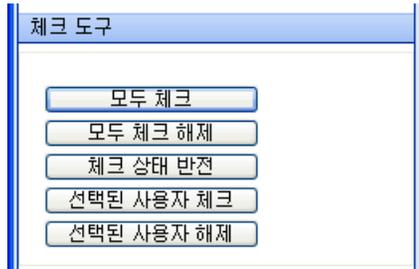
사용자 ID	<input type="text"/>	검색	Card 읽기	모두 보기				
<input checked="" type="checkbox"/> 사용...	이름	회사	부서	직책	규칙 그룹	지문등...	RF ID	활...
<input checked="" type="checkbox"/>	796	고원창				0	0	예

Card로 검색하는 경우에는 '카드로 검색'을 선택한 뒤에 Card 읽기를 클릭하여 실제 등록된 카드로 번호를 입력할 수도 있으며 직접 입력으로 검색도 가능합니다.

4.5. 사용자 선택

사용자 리스트 윈도우상의 체크 박스에 체크를 하여 사용자를 선택할 수 있습니다.

또한 체크 도구를 이용해 손쉽게 사용자를 선택할 수 있습니다.



- 모두 체크: 모든 사용자들을 체크합니다.
- 모두 체크 해제: 모든 체크된 사용자들을 해제합니다.
- 체크 상태 반전: 원래 체크된 사용자들을 제외한 모든 사용자들을 표시합니다.
- 선택된 사용자 체크: 선택된 사용자를 체크합니다.
- 선택된 사용자 해제: 선택된 사용자를 체크 해제합니다.

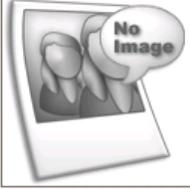
4.6. 새 사용자를 추가

새 사용자를 추가 버튼을 누르면 호스트 PC에 사용자를 등록하는 팝업 윈도우창이 활성화 됩니다..

사용자 정보

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

개인 정보


 사용자 ID: 853 사진 및 개인 인증화면 편집
 이름: 서동석
 회사: 슈프리마
 부서: M&S
 직책: 사원

상세정보

전화번호:
 핸드폰:
 이메일:
 성별: 남자
 생년월일: 1970-06-14
 시작일: 2006-04-13
 만료 일시: 2030-12-31 0 시

출입 통제

출입 상태: 활성화
 그룹 1: 전체 출입
 그룹 2: 사용 안함
 그룹 3: 사용 안함
 그룹 4: 사용 안함

인증 제한 (BioStation 전용)

제한 횟수: 0 회
 인증 간격(분): 0 분

추가 정보

비밀번호: 사용자 등급: 일반

확인 취소

4.6.1. 사용자 정보

- 사용자 정보에서 개인정보와 상세정보, 출입그룹 설정, 기타정보, BioStation 추가 정보의 내용을 입력 할 수 있습니다. 개인정보에는 사용자ID, 이름, 회사, 부서, 직책 등을 입력합니다. 상세정보에는 전화번호, 핸드폰 번호, 이 메일 , 성별 , 생년월일을 입력합니다.
- 사진 및 개인 인증 화면 편집

사진 및 인증 화면 수정

사진


 사용자 ID: 853
 이름: 서동석
 표시 횟수/기간: 제한 없음
 인증 성공 메시지:

사진 변경
 사진 지우기

저장 취소

- 인증 성공 시에 나타날 개인별 사진 및 메시지를 변경하고, 표시 조건을 설정할 수 있습니다. 이 내용은 장치의 '개인 인증 화면'을 사용하도록 해야 나타납니다.

- 출입통제

- 해당 사용자에 대한 출입 그룹 정보를 입력합니다.
- 출입그룹에서 활성화를 꼭 체크를 하셔야 장치에서 인증을 할 수 있습니다. 활성화를 체크하지 않으면 장치 내의 사용자 데이터는 비활성화 됩니다.
- 항상 통과 카드에 체크 할 경우에는 해당 사용자는 지문이나 비밀번호 입력 없이 카드만으로 출입할 수 있게 됩니다.
- 출입횟수는 해당일의 0시부터 24시까지 출입 가능한 횟수입니다. 출입횟수를 제한하지 않고자 할 경우에는 0으로 설정하면 됩니다.
- 인증간격은 사용자 인증 / 출입 후 다음 번 인증 / 출입 시까지의 최소한의 시간 간격을 말합니다. 즉, 인증간격이 5분으로 설정 되어있다면, 해당 사용자는 출입 후 5분 이내에는 다시 출입할 수 없게 됩니다.

- 추가정보

- 비밀번호를 설정하게 되면 출입할 때 장치에서 ID 입력 시 비밀번호를 사용하실 수 있습니다. 또한, 일반 사용자가 BioAdmin 에 접속하여 자신의 로그 등을 확인 하고자 할 경우에도 여기에서 지정한 비밀번호를 입력 하여야 합니다.
- BioStation 사용자 등급은 일반과 관리자 중 선택이 가능합니다.

Note: 사용자 정보에서 필수항목인 사용자ID는 꼭 작성하시고, 그 외의 항목은 필수사항이 아니므로 비워두셔도 됩니다.

4.6.2. 사용자 정의 항목

사용자 정의 항목 메뉴에서 필요한 필드들을 지정하여 사용자 관리 윈도우에 설정된 사용자 정보 항목을 추가할 수 있습니다.

- **설정** 버튼은 설정된 사용자 정보 행을 추가하는 팝업 윈도우를 활성화합니다. 필요한 항목들을 채운 후에 확인 버튼을 누릅니다.

사용자 정보

사용자 정보 | 사용자 정의 항목 | 지문 | 사용자 근태관리 규칙

취미: 닥시
 팩스번호: 031-456-7895
 할당IP: 123,123,23,1
 사무실 호수: 423
 기념일: 2006-04-13
 기혼
 차량 보유

설정

확인 취소

사용자 정의 항목 설정

문자열

문자열 1: 취미
 문자열 2: 팩스번호
 문자열 3: 할당IP
 문자열 4:
 문자열 5:
 문자열 6:
 문자열 7:
 문자열 8:

숫자

숫자 1: 사무실 호수
 숫자 2:
 숫자 3:
 숫자 4:

날짜

날짜 1: 기념일
 날짜 2:
 날짜 3:
 날짜 4:

체크박스

체크박스 1: 기혼
 체크박스 2: 차량 보유
 체크박스 3:
 체크박스 4:

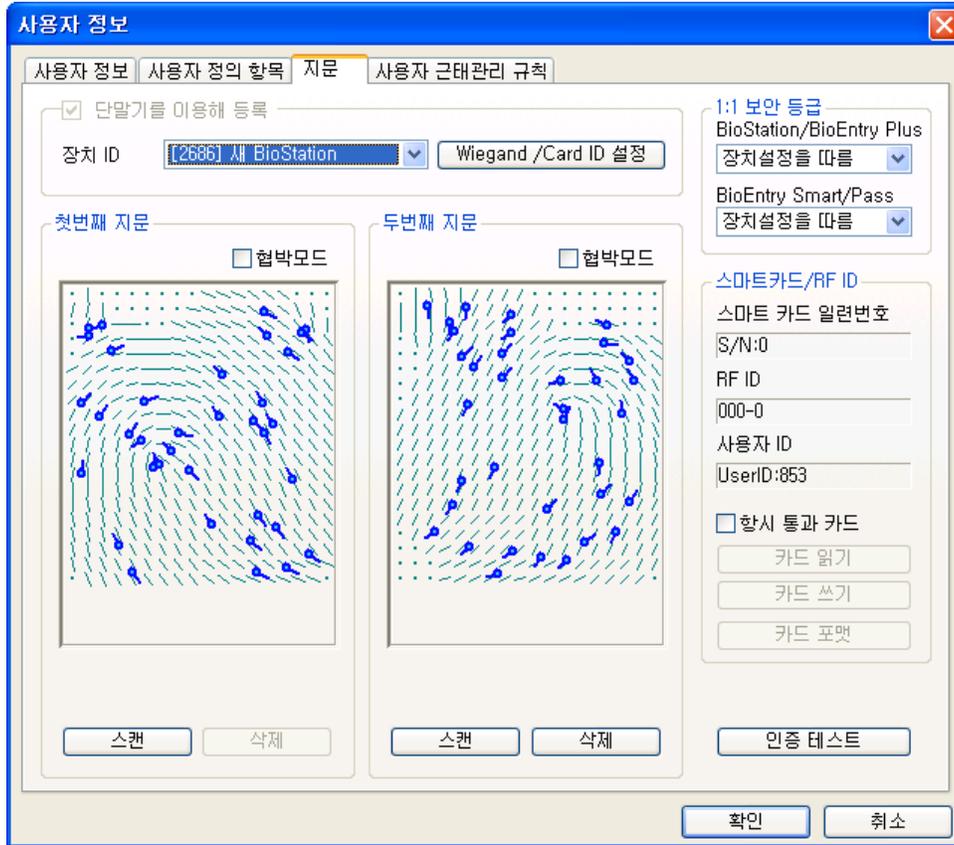
확인 취소

Note : 사용자 정의항목은 빈 화면처럼 보이나 오른쪽 하단부의 설정을 클릭하게 되면 문자열 , 숫자, 날짜 , 체크박스 등의 사용자 정의항목을 설정하는 화면이 띄워집니다. 그 항목을 체크하게 되면 빈 화면의 사용자 정의항목에

서 항목들이 생성됩니다.

4.6.3. 지문

지문메뉴에서는 호스트 PC의 데이터베이스에 사용자 지문정보를 추가합니다.



- PC USB 스캐너를 사용한 등록
- 호스트 PC와 연결된 장치를 사용한 등록
단말기를 이용해 등록 체크 박스를 활성화하고 장치 ID를 선택하여, BioEntry 및 BioStation 장치를 사용자 지문정보를 얻기 위해 사용할 수 있습니다. 사용자 데이터베이스는 2개 지문 정보까지 포함할 수 있습니다.
- 지문 입력
스캔 버튼을 누르고 동일한 손가락을 두 번 대어 주십시오. 지문정보가 성공적으로 획득되었다면, 스캔 된 지문정보가 윈도우상에 나타납니다. 다른 손가락에 대한 두 번째 지문을 등록하기 위해서는 오른쪽 영역에 있는 스캔 버튼을 클릭하십시오.
- 협박모드 손가락 등록
특정 손가락이 장치에서 감지되면 협박모드 신호를 발생시키는 협박모드 손가락을 등록할 수 있습니다. 지문인식정보를 등록한 후, 지문인식정보를 협박모드로 저장하기 위해서 협박모드 표시 박스를 활성화 합니다.

Note : 협박모드란?

협박모드 손가락은 출입문 앞에서 도둑에게 협박을 당하는 상황에서 요긴하게 사용될 수 있습니다. 협박 손가락이 입력되면 정상적으로 출입문은 열리지만 출력포트로 설정해 놓은 비상경보장치를 울리거나 비상연락전화로 발신하는 등의 구성이 가능합니다. 예를 들어 손가락을 2개를 등록할 경우 첫 번째 손가락은 정상 손가락, 두 번째 손가락은 협박 손가락으로 등록할 수 있습니다. 협박 손가락은 앞서 등록한 정상 손가락과 반드시 다른 손가락을 사용해 등록해야 합니다.

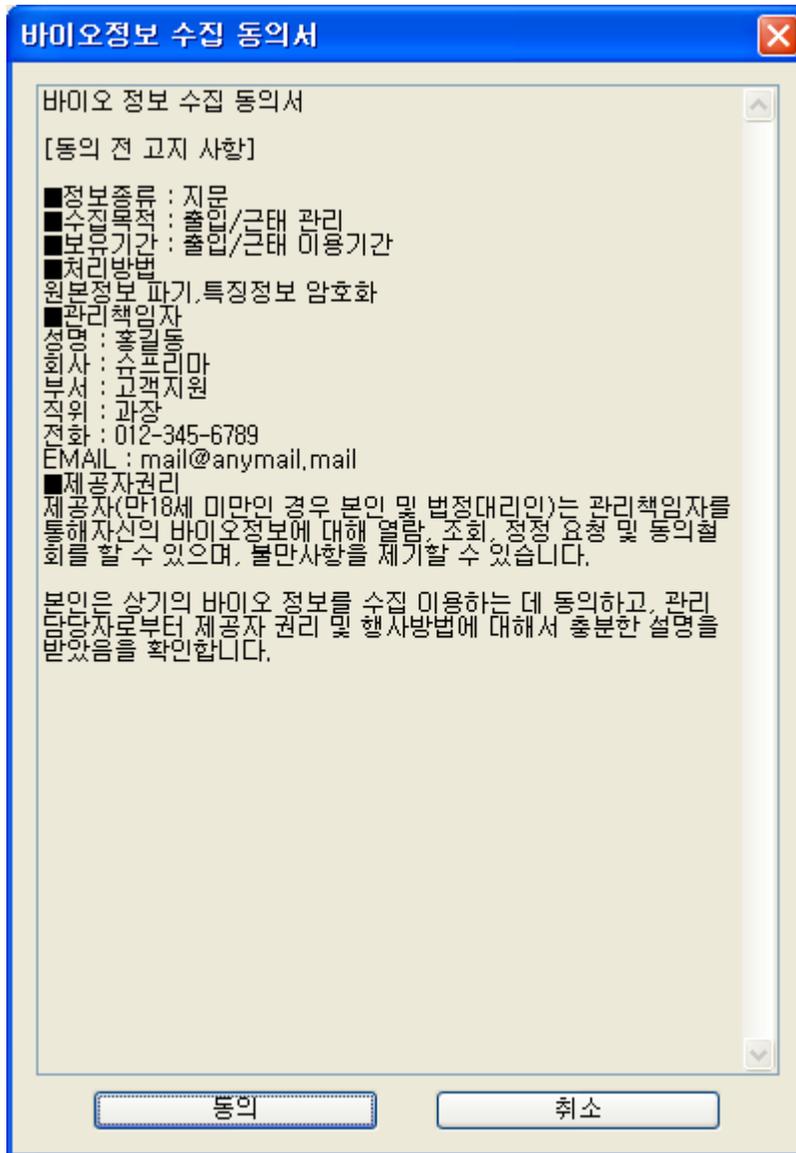
- 지문삭제

입력된 지문을 삭제할 때에는 오른쪽 두 번째 지문정보부터 삭제를 하며, 첫 번째 지문정보는 두 번째 지문정보를 삭제한 후에 삭제하실 수 있습니다.

- 인증 테스트

지문인식정보의 등록이 올바르게 끝났음을 확인하기 위해 인증 테스트를 수행할 수 있습니다. **인증 테스트** 버튼을 누르면 장치에 손가락을 대십시오 라는 메시지가 띄워집니다. 손가락을 대면 인증 결과를 보여주는 메시지가 나타납니다.

- 바이오 정보보호 가이드가 활성화 되어 있다면 지문을 입력 받기 전에 바이오 정보 수집 동의서가 나타나며, 동의하지 않는 경우 지문을 입력 받지 않습니다. 이 동의서는 새로운 사용자 정보 다이얼로그를 볼 때마다 나타납니다.



● Wiegand / Card ID 설정



BioStation RF의 RF 카드를 사용하거나 혹은 별도의 외부 Wiegand 카드리더를 BioStation 에 연결하여 사용 할 경우 사용자 별로 카드 ID를 설정

하기 위한 메뉴입니다.

- **Wiegand / 카드 ID 가져오기** 버튼을 누르면 BioStation (혹은 외부 Wiegand 카드리더) 은 카드의 입력을 기다리는 상태가 됩니다. 사용자가 카드를 BioStation (혹은 외부 Wiegand 카드리더) 에 대어 Wiegand ID를 보내주게 되면 그 카드의 ID 가 해당 사용자를 위한 카드의 ID로 입력됩니다. 즉, 카드로부터 ID를 받아들여 그 카드 ID를 해당 사용자의 사용자 ID 와 연결시키는 방법입니다.
 - **사용자 ID를 사용** 버튼을 누르면 Wiegand/카드 ID 가 사용자 ID 와 동일하게 입력됩니다. 이 기능은 기존에 카드 ID를 사용자 ID와 동일하게 설정하여 사용하고 있을 경우 손쉽게 카드 ID를 입력하는 방법입니다.
 - **Wiegand/카드 ID 직접 입력** 버튼을 누르면 Wiegand / 카드ID 영역이 활성화됩니다. 여기에 사용하고자 하는 카드 ID를 직접 입력하면 됩니다. 이 기능은 기존에 사용자에게 발급된 카드가 있을 경우 그것을 직접 입력할 때 사용됩니다.
- **1:1 보안등급**
해당 사용자가 BioEntry 또는 BioStation 에 1:1 인증을 할 경우의 보안등급을 의미합니다. 특정 사용자가 지문상대가 좋지 않아 1:1 인증 시 인증실패가 자주 나올 때에는 해당 사용자의 1:1 보안등급은 다소 낮추어 잘못된 인증 실패오류를 줄일 수 있습니다.

4.6.4. 사용자 스마트카드 발급하기

BioEntry Smart 는 기본적으로 사용자 지문인식정보를 포함하는 사용자 정보를 가지고 작동하며, Mifare Card 를 지원하는 BioStation 과 BioEntry Plus 에서도 스마트 카드를 발급하여 사용할 수 있습니다.

사용자의 스마트카드 발급은, 사용자 리스트에서 사용자를 클릭하거나 주 윈도우에서 새 사용자 추가 버튼을 더블 클릭하면 초기화 되는 사용자 관리 윈도우에서 처리됩니다.

스마트카드를 발급하는 데는 2가지 방법이 있습니다:

- PC USB 스마트카드 등록기로 발급.
- 호스트 PC와 연결된 장치로 발급.
BioStation Mifare, BioEntry Plus Mifare 또는 BioEntry Smart를 카드 발급기로 사용하기 위해서는 단말기를 이용해 등록 체크 박스를 활성화하고 장치 ID를 선택합니다. 그렇지 않으면, PC USB 장치가 카드 발급기로서 사용됩니다.

4.6.5. PC USB 스마트카드 장치로 발급

- 대상 스마트카드를 PC 스마트카드 장치에 놓습니다.
- 카드발급을 시작하기 위해 **카드쓰기** 버튼을 누릅니다.
- BioAdmin 소프트웨어가 시작된 후에 첫 번째 카드발급 시 사이트 키 관리 윈도우가 나타납니다. 또한, 사이트 키가 일치하지 않아 스마트카드를 불러오는 실패했다면 경고 윈도우가 나타날 것입니다.
- 스마트 카드를 불러오기 위해 현재 사이트 키를 입력하십시오.

- 공백으로 남겨둔다면, 관리 소프트웨어는 현재 사이트 키를 기본값 (0xFFFFFFFF)으로 사용합니다.
- 발급 시 사이트 키를 변경하고자 한다면, 사이트 키 변경 표시 박스를 활성화하고 새로운 사이트 키를 입력합니다. 그러면, 스마트카드에서 새로운 사이트 키가 갱신됩니다. 새로운 사이트 키는 장치상의 사이트 키와 일치해야 합니다.

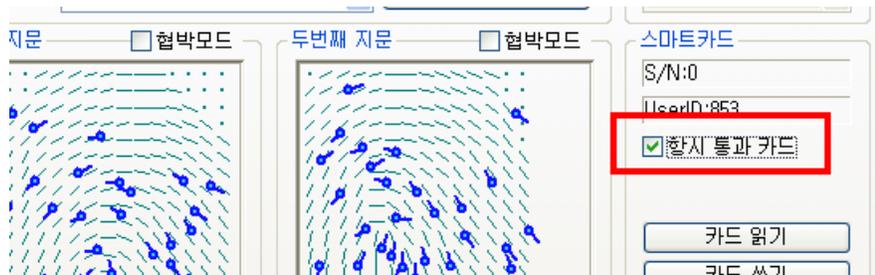
4.6.6. 단말기로 발급

- 대상 스마트카드를 선택된 장치에 놓습니다.
- 발급과정을 진행하기 위해 **카드 쓰기** 버튼을 누릅니다. 사이트 키 관리 정보가 장치에 저장되어 있기 때문에, 발급과정은 사이트 키가 없어도 진행됩니다.

4.6.7. 사용자 보안 등급과 항시 통과카드 설정

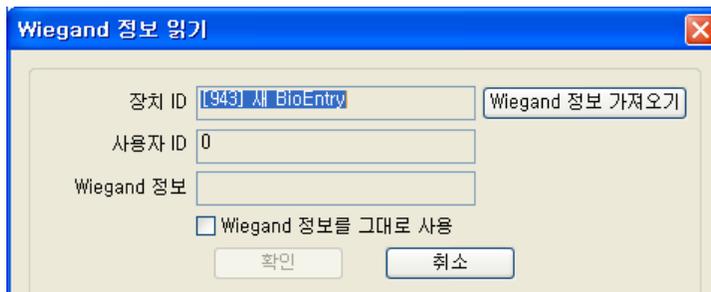
카드를 발급할 때 각 사용자에게 대해 보안 등급을 정할 수 있습니다. 드롭다운 리스트에서 보안 등급을 1/1,000에서 1/100,000,000까지 지정할 수 있습니다. 한편, 항시 통과카드를 발급하기 위해 **항시 통과 카드** 라는 옵션이 있습니다.

Note : 항시 통과카드란? 사용자가 지문을 입력할 필요 없이 카드만으로 장치가 승인하는 것을 말합니다.



4.6.8. ID 카드 이용하여 Wiegand 스트링 설정

스마트 카드를 발급할 때 고객의 ID 카드의 특정 Wiegand 스트링을 스마트카드에 전송할 수 있습니다. 전송을 위해 RF Wiegand 장치가 선택된 BioEntry 장치의 Wiegand 입력 포트에 연결되어야 합니다.



구체적인 동작과정은 다음과 같습니다.

- **Wiegand 정보설정** 버튼을 누릅니다.

- **Wiegand정보 가져오기** 버튼을 누르고 Wiegand 장치에서 Wiegand 정보를 가진 ID 카드를 접촉시킵니다.
- 장치로부터 가져온 Wiegand 정보가 사용자 관리 윈도우에 나타납니다.
- 사용자 ID대신에 Wiegand 정보를 사용하기 위해 Wiegand 정보를 그대로 사용 표시 박스를 체크하시면 됩니다.
- 사용자의 스마트카드를 발급하려면 확인 버튼을 누릅니다. 그러면, 전송된 Wiegand 정보는 스마트카드에 저장됩니다. 만약 표시 박스가 비활성화되었다면, 사용자 ID로부터 변환된 Wiegand 정보가 스마트카드에 기록됩니다.

4.6.9. 발급된 스마트카드 정보 읽기

사용자 정보 윈도우상의 **카드 읽기** 버튼을 이용해 발급된 스마트카드에 저장된 정보를 검색할 수 있습니다.

PC USB 스마트 카드 등록기가 사용될 때, 사이트 키가 불일치하면 사이트 키 관리 윈도우가 나타납니다.

4.6.10. 카드 포맷

포맷은 스마트카드에 저장된 정보를 삭제하는 과정입니다. 사용자 관리 윈도우에 **카드 포맷** 버튼은 스마트카드를 포맷하는 과정을 초기화합니다.

일정시간까지 스마트카드를 대지 않으면 스마트카드 포맷 실패라는 윈도우 창이 띄워집니다.

4.6.11. 카드 발급 시 중요한 주의사항

- 새로운 스마트 카드를 발급하기 전에, 먼저 새로운 스마트카드를 포맷해야 합니다. 즉, 새로운 카드로 사용자 카드를 발급하고자 할 경우 **카드 포맷** 버튼을 눌러 카드를 포맷하고, **카드 쓰기** 버튼을 눌러 사용자 카드를 발급하여야 합니다.

시스템의 보안을 강화하기 위해서는 사이트 키를 장치관리 소프트웨어에 저장하지 마십시오.

Note : 관리자가 적절한 시스템 관리를 위해 고객 사이트 키를 기억하고 비밀로 유지할 것이 요구됩니다. 또한 스마트카드의 사이트 키는 장치의 사이트 키와 일치하여야 사용이 가능하므로 사이트 키를 변경할 때는 많은 주의를 해 주십시오.

- 발급 과정에서 스마트카드를 작성하는 도중에 뜻하지 않게 중단될 경우에는, 스마트카드가 손상되어 복구 불가능 할 수 있습니다. 스마트카드에 쓸 때 뜻하지 않는 중단이 일어나지 않도록 주의하시기 바랍니다.

4.6.12. 사용자 근태관리 규칙

근태관리를 위한 사용자 근태관리 규칙을 설정하는 메뉴입니다. 구체적 설정방법에 대해서는 12장 보고서 상의 내용을 참조하십시오.

4.7. 체크된 사용자를 삭제

4.7.1. BioAdmin 소프트웨어에서 체크된 사용자 삭제

사용자 리스트 윈도우 창에서 체크 된 사용자의 정보를 삭제합니다.

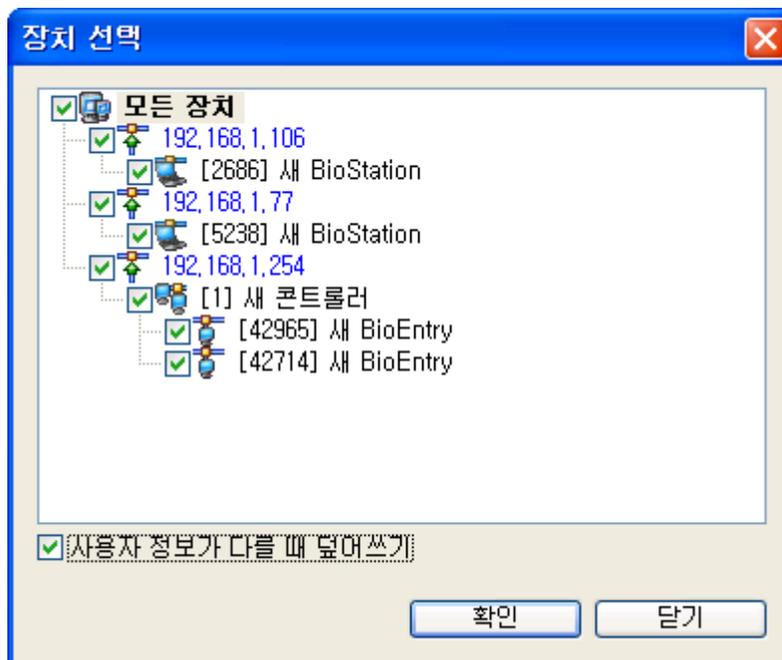
사용자를 체크하고 작업 박스에서 체크된 사용자를 삭제를 클릭하면 선택된 사용자를 제거하시겠습니까? 라는 메시지가 나옵니다.

확인버튼을 누르면 체크된 사용자가 호스트 PC의 BioAdmin 에서 삭제됩니다.

4.7.2. 삭제된 사용자 정보를 장치와 동기화

특정 사용자를 삭제한 후 남아 있는 사용자 정보를 장치에 전송하면 장치에서도 삭제된 사용자의 정보를 삭제할 수 있습니다.

4.8. 체크된 사용자를 장치에 전송



체크된 사용자를 장치에 전송은 호스트PC의 사용자 데이터베이스를 장치로 전송하는 것입니다. 장치를 작동시키기 위해서는 지문정보를 포함한 사용자 데이터가 사용자 등록 후에 장치로 전송되어야 합니다.

사용자 ID, 지문인식정보, 출입 그룹과 보안 등급과 같은 사용자 정보는 이 과정을 통해 전송됩니다. 전송과정은 선택된 장치, 선택된 그룹 또는 네트워크상의 연결된 모든 장치에서 처리됩니다. 사용자 선택 방법에서 사용자 정보의 선택적인 전송을 할 수 있습니다.

구체적인 동작과정은 다음과 같습니다.

- 전송하려는 사용자를 체크합니다.
- 체크된 사용자를 장치에 전송 버튼을 누릅니다.

- 장치선택 창에서 장치를 선택합니다..
- 사용자 ID는 같으나, 사용자정보가 다를 경우 덮어쓰기를 체크하게 되면 호스트PC의 데이터가 장치의 동일한 사용자의 다른 정보를 덮어쓰게 됩니다.
- 장치에서 선택된 사용자를 찾을 수 없다면, 새로운 사용자 데이터가 호스트 PC 데이터베이스에서 장치로 전송됩니다.

4.9. 체크된 사용자를 장치에서 삭제

사용자 리스트 윈도우에서 체크된 사용자를 장치에서 삭제 버튼으로 등록된 사용자를 제거할 수 있습니다.

구체적인 동작과정은 다음과 같습니다.

- 제거하려는 사용자를 선택합니다.
- 작업 창에서 체크된 사용자를 장치에서 삭제 버튼을 누릅니다.
- 장치선택 화면에서 해당 장치를 선택합니다.
- 선택된 사용자는 호스트PC의 사용자 리스트에서는 삭제되지 않습니다. 호스트PC의 사용자 리스트에서도 삭제하시려면 “체크된 사용자를 삭제”버튼을 누르면 됩니다.

Note : 선택한 장치에서 사용자 정보를 삭제를 하는 작업이므로 네트워크로 구성되어 있는 경우, 장치를 선택하실 때 신중하여야 합니다.

4.10. 체크된 사용자의 출입그룹 설정

사용자 리스트 윈도우에서 체크된 사용자들의 출입통제 정보를 일괄적용 합니다. 리스트에서 마우스 오른쪽 버튼을 클릭하면 팝업 메뉴가 나타납니다.

변경할 정보를 체크하여 설정값을 변경할 수 있습니다.

- 출입상태 : 출입상태를 활성화 할 것인지의 여부를 변경하기 위해서는 체크되어야 합니다.
 - 활성화 : 활성화에 체크가 되어야 출입이 가능한 상태가 됩니다.
- 출입방법 : RF 카드를 사용할것인지를 변경 하기 위해서 체크합니다.
 - 향시통과카드 : RF 카드를 사용하여 출입을 하기 위해서는 체크 되어야 합니다.
- 출입그룹 : 출입통제 메뉴의 출입시간에서 미리 정한 출입그룹을 선택하여 부여할 수 있으며, 기본값으로는 전체출입이 설정 되어 있습니다.
- 제한횟수 : 하루에 인증을 허용하는 최대 횟수를 지정합니다.
- 인증제한 : 인증 후, 설정된 시간 동안은 인증을 허용하지 않도록 제한합니다.

4.11. 체크된 사용자의 근태 규칙 그룹 설정

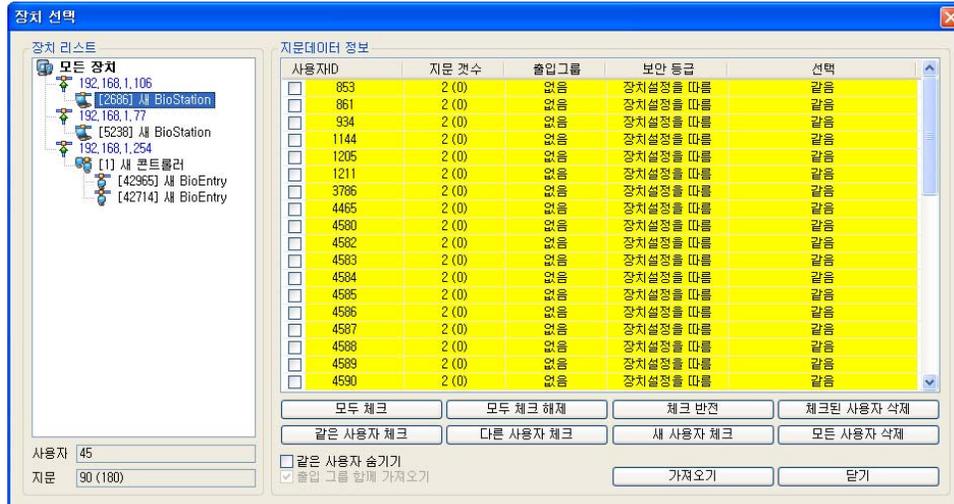
사용자 리스트 윈도우에서 체크된 사용자들의 근태관리규칙을 설정합니다. 리스트에서 마우스 오른쪽 버튼을 클릭하면 팝업 메뉴가 나타납니다.

보고서 메뉴에서 미리 설정된 근태관리규칙을 선택하여 적용합니다.

4.12. 장치 별 사용자 관리

장치 별 사용자 관리 버튼은 사용자 정보를 장치에서 호스트 PC의 데이터베이스로 업로드 하는 것을 말합니다. 사용자 ID, 지문정보, 출입 그룹의 번호,보안 등급과 같은 사용자 정보가 이 과정에 의해서 업로드 됩니다.

이 메뉴에서는 네트워크 상에서 선택된 장치로부터 사용자 데이터베이스를 선택적으로 가져오는 것이 가능합니다.



구체적인 동작과정은 다음과 같습니다.

- 장치 별 사용자 관리 버튼을 누릅니다.
- 장치 리스트 윈도우에서 해당 장치를 선택합니다.
- 장치 리스트 윈도우 아래서, 선택된 장치에 등록된 사용자와 지문정보의 수를 알 수 있습니다.
- 사용자 구분
 - 같은 사용자: 장치에서 가져온 사용자 정보와 BioAdmin 소프트웨어의 사용자 정보가 일치하는 사용자
 - 다른 사용자: 장치에서 가져온 사용자 정보와 BioAdmin 소프트웨어의 사용자 정보가 일치하지 않는 사용자
 - 새 사용자: 장치에서 가져온 사용자의 정보가 BioAdmin 소프트웨어의 없는 경우이며, 장치에서의 잉여사용자라 볼 수 있습니다.
- 색상구분
 - 같은 사용자: 노란색으로 표시 됩니다.
 - 다른 사용자: 빨간색으로 표시 됩니다.
 - 새 사용자: 녹색으로 표시 됩니다.
- 선택의 구분
 - 모두 선택: 사용자 정보를 모두 선택
 - 모두 해제: 사용자 정보를 모두 선택을 한 뒤 해제하고자 할 때
 - 선택 반전: 선택된 사용자를 해제하거나, 해제상태의 사용자를 선택할 때
 - 선택 삭제: 선택된 사용자를 삭제
 - 같은 사용자 선택: 장치에서 가져온 사용자 정보와 BioAdmin 소프트웨어의 사용자 정보가 일치하는 사용자를 선택합니다.
 - 다른 사용자 선택: 장치에서 가져온 사용자 정보와 BioAdmin 소프트웨어

의 사용자 정보가 일치하지 않는 사용자를 선택합니다.

- 새 사용자 선택: 장치에서만 등록되어 있고 BioAdmin 소프트웨어에 없는 사용자를 선택합니다.
- 모두 삭제: 선택된 사용자와 그 외의 사용자 모두 삭제

- 같은 사용자 숨기기

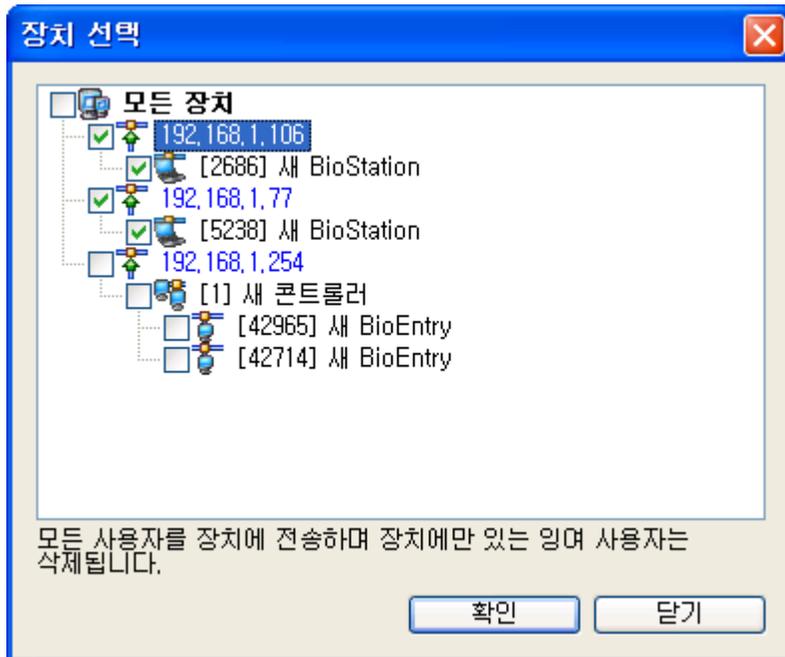
같은 사용자 선택을 누르면 장치와 호스트PC의 데이터가 같은 사용자의 체크박스에 체크를 합니다.. 같은 사용자 숨기기를 표시하면 이러한 사용자들을 지문인식정보 윈도우에서 숨길 수 있습니다.

- 출입 그룹 함께 가져오기

출입 그룹 함께 가져오기를 체크박스에 체크를 한 후 가져오기를 실행하면 사용자 출입 그룹 정보도 업로드 할 수 있습니다.

4.13. 모든 사용자를 장치와 동기화

모든 사용자를 장치와 동기화 버튼은 호스트PC에 있는 모든 사용자 데이터베이스를 장치로 전송하며, 장치에만 있는 잉여 사용자는 삭제됩니다. 사용자 ID, 지문정보, 출입 그룹의 번호와 보안 등급과 같은 사용자 정보가 이 과정에 의해서 업로드 됩니다.



구체적인 동작과정은 다음과 같습니다.

- 모든 사용자를 장치와 동기화 버튼을 누릅니다.
- 장치 리스트 윈도우에서 해당 장치를 선택합니다.
- 선택 버튼을 누르면 장치에 있는 사용자 정보 데이터베이스를 호스트PC에서 장치로 전송하게 됩니다.

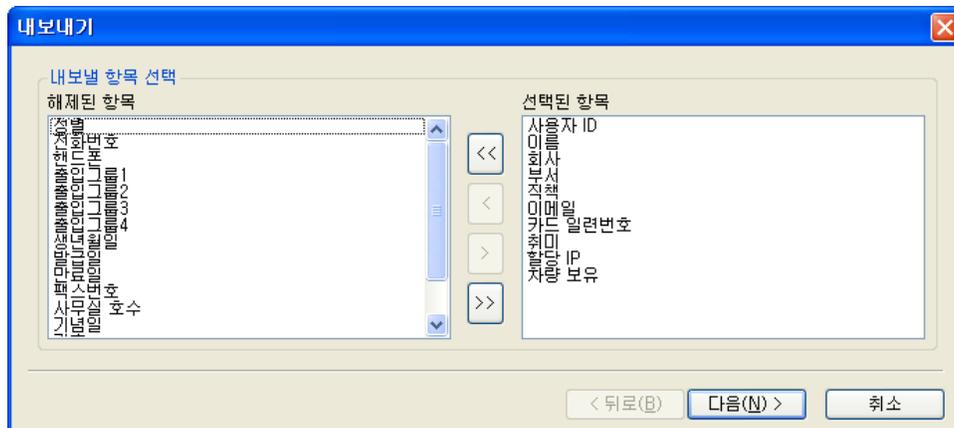
Note: 모든 사용자를 장치에 전송하며 장치에만 있는 잉여사용자는 모두 삭제 됩니다.

4.14. 파일로 내보내기

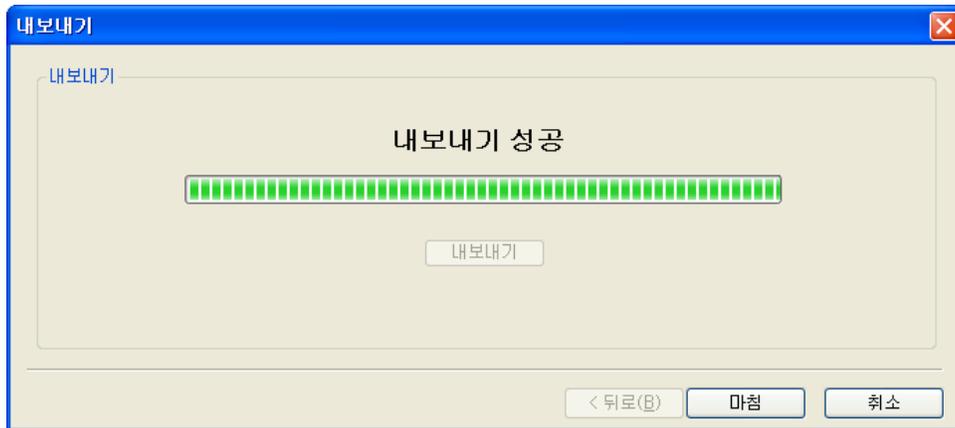
파일로 내보내기 버튼은 내보낼 항목 선택에서 해제된 항목의 목록에서 선택된 사용자의 정보를 **CSV** 포맷으로 저장하려는 과정을 초기화합니다. 단, 사용자의 지문정보는 내보내는 항목에 포함되지 않습니다. **Microsoft Office Excel**이나 보통의 텍스트 편집기를 이용하여 전송된 **CSV** 파일을 편집할 수 있습니다.

구체적인 동작과정은 다음과 같습니다.

- 파일로 내보내려는 사용자들을 선택합니다.
- **파일로 내보내기** 버튼을 누릅니다.



- 대상 항목을 해제된 항목에서 선택된 항목으로 옮기면, 내보내려는 항목들이 선택됩니다.
- 항목들을 선택하고 **다음** 버튼을 누릅니다.
- 내보내려는 파일을 선택합니다.
- 파일을 선택하고 **다음** 버튼을 누릅니다.
- **내보내기** 버튼을 누릅니다.
- 내보내기 성공 이라는 메시지가 띄워집니다.

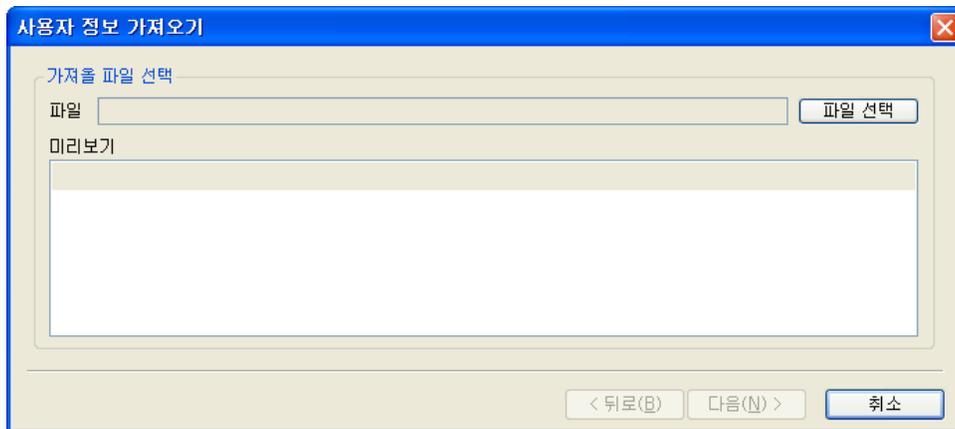


4.15. 파일에서 가져오기

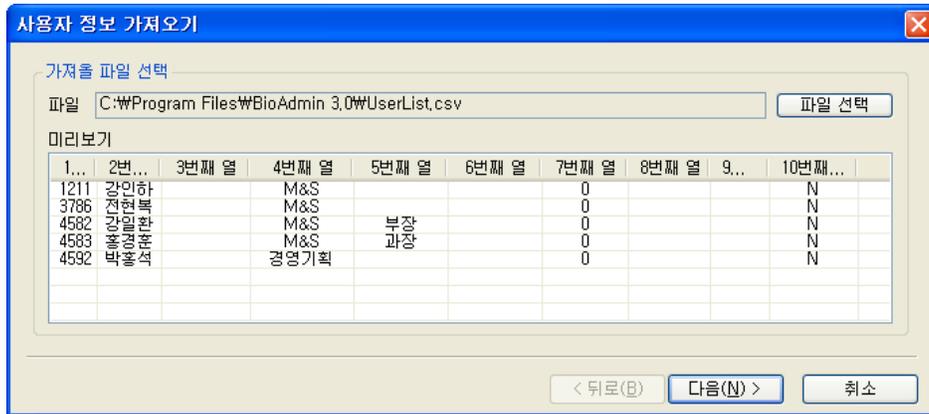
파일에서 가져오기 버튼은 사용자 데이터베이스를 외부 데이터베이스로부터 BioAdmin 소프트웨어 사용자 데이터베이스로 가져오는데 사용됩니다. CSV(Comma Separated Values) 포맷으로 저장된 사용자 리스트는 사용자 데이터베이스로 리스트로 가져올 수 있습니다.

구체적인 동작과정은 다음과 같습니다.

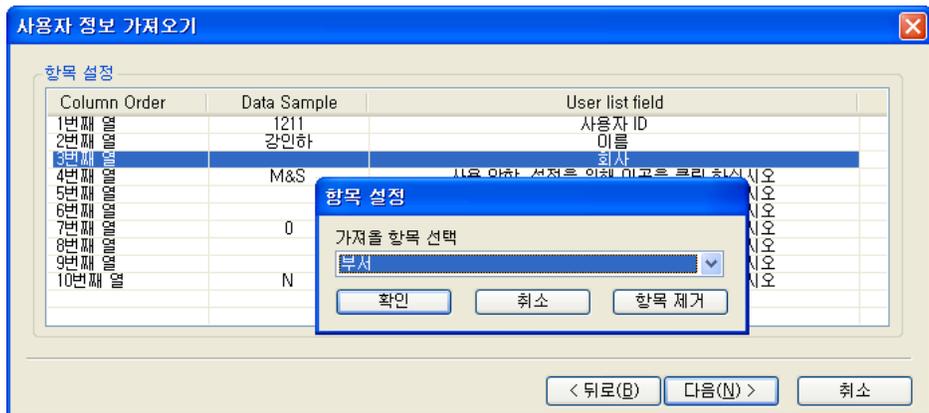
- 파일로 가져오기 버튼을 누릅니다.



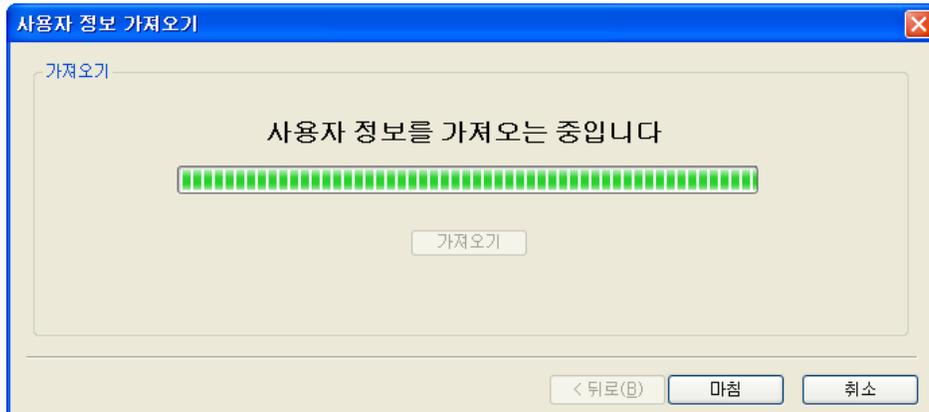
- 불러올 파일을 선택합니다.
- 파일을 선택하면 미리 보기 윈도우에서 사용자의 정보를 볼 수 있습니다. 선택된 파일이 데이터베이스를 가져올 파일로 확인되는 미리 보기 윈도우를 표시합니다.



- 파일이 맞으면 다음 버튼을 누릅니다.
- 가져올 항목을 선택 후 확인을 누르면 항목설정이 되며 다음 버튼을 클릭합니다.



- 가져오기 버튼을 누릅니다.
“사용자 정보를 내보내는 중입니다.” 라는 메시지가 띄워집니다.



5. 장치 관리

장치 관리 메뉴에서는 장치 별 설정 값들을 확인하고 이를 변경할 수 있습니다.



장치관리 화면은 3개 영역으로 나눌 수 있습니다.

- **장치 환경 설정**
환경 설정 윈도우는 연결된 장치의 현재 설정 상태를 보여줍니다. 이 창에서 설정 값을 변경시킬 수도 있습니다.
- **작업 박스**
작업 박스는 장치 관리 페이지의 기본 동작들을 관리하는 버튼들을 포함하고 있습니다.
- **목록창**
목록창은 '장치목록'과 '구역목록' 으로 나뉘어 있습니다. '장치'목록'에서는 연결된 장치의 목록이 나타나며, 장치를 선택하면 해당 장치의 설정값을 변경할 수 있고, '구역목록'에서는 연결된 장치들의 설정된 구역이 나타나게 됩니다. 자세한 설명은 '4.4 목록창' 을 참조하시기 바랍니다. 여기서서는 우선 작업 박스에 있는 각종 메뉴의 기능을 설명한 후, 각 장치 별 환경설정에 대한 내용을 설명합니다.

5.1. 새 장치 추가

새로운 BioStation이나 BioEntry 또는 BioEntry Plus, BioLite Net 장치를 검색하여 추가하기 위해서는 작업 박스의 새 장치 추가 메뉴를 클릭해야 합니다. 새 장치 추가라는 윈도우 창이 띄워지면 먼저 검색할 장치를 BioEntry 나 BioStation 또는 BioEntry Plus, BioLite Net 중에 선택합니다. 그리고, 장치와 호스트 PC 사이의 인터페이스 방법에 따라 직렬포트(시리얼 통신), TCP/IP(이더넷), USB, UDP 장치 중 하나를 선택합니다. 이 중에서 USB 연결은 BioStation만 가능하며 BioEntry Plus 는 UDP 를 선택합니다. BioLite Net 역시 UDP 검색을 지원하며, TCP/IP(이더넷) 연결과 RS485 를 통한 직렬포트(시리얼 통신) 연결이 가능합니다.

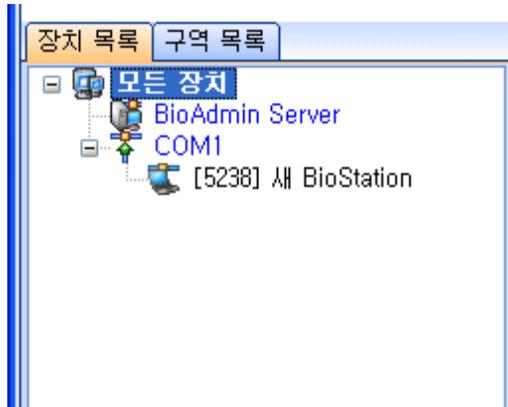
5.1.1. 직렬 포트

장치와 호스트 PC가 시리얼 통신으로 연결된 경우, 호스트PC의 해당 COM단자를 설정하고 통신속도(Baudrate)를 선택합니다. BioStation, BioEntry, BEACon, BioLite Net 은 모두 초기 설정 통신속도가 115,200 bps로 설정되어 있습니다.

The screenshot shows a dialog box titled "새 장치 추가" (Add New Device). At the top, there are four radio buttons for device selection: "BioEntry 검색" (unselected), "BioStation 검색" (selected), "BioEntry Plus 검색" (unselected), and "BioLite Net 검색" (unselected). Below this, there are four main options, each with a radio button: "직렬포트" (selected), "TCP/IP", "USB 장치 (BioStation)", and "USB 가상 BioStation". The "직렬포트" section has a "COM" dropdown menu set to "COM1" and a "통신속도" (Baud Rate) dropdown menu set to "115200". The "TCP/IP" section has an "IP 주소" (IP Address) field and a "포트" (Port) field set to "1470". The "USB 가상 BioStation" section has a drive letter dropdown menu set to "A:". The "UDP (BioEntry Plus / BioLite Net)" option is also present but unselected. At the bottom of the dialog, there is a "검색" (Search) button, and below that, "확인" (OK) and "취소" (Cancel) buttons. A large empty text area is located above the "확인" and "취소" buttons.

검색버튼을 누르면 검색 결과를 메시지로 표시합니다. 확인 버튼을 누르면 검색된 장치가 장치리스트에 나타나게 됩니다. 검색된 장치의 이름 앞에 각괄호 [] 사

이의 숫자는 해당 장치의 ID 입니다. 장치의 이름을 바꾸고 싶을 경우 장치리스트의 해당장치에 커서를 대고 마우스의 오른쪽 버튼을 누르면 메뉴가 나타나는데 여기서 “이름 변경”을 선택하면 새 이름을 입력할 수 있는 입력 창이 뜹니다.

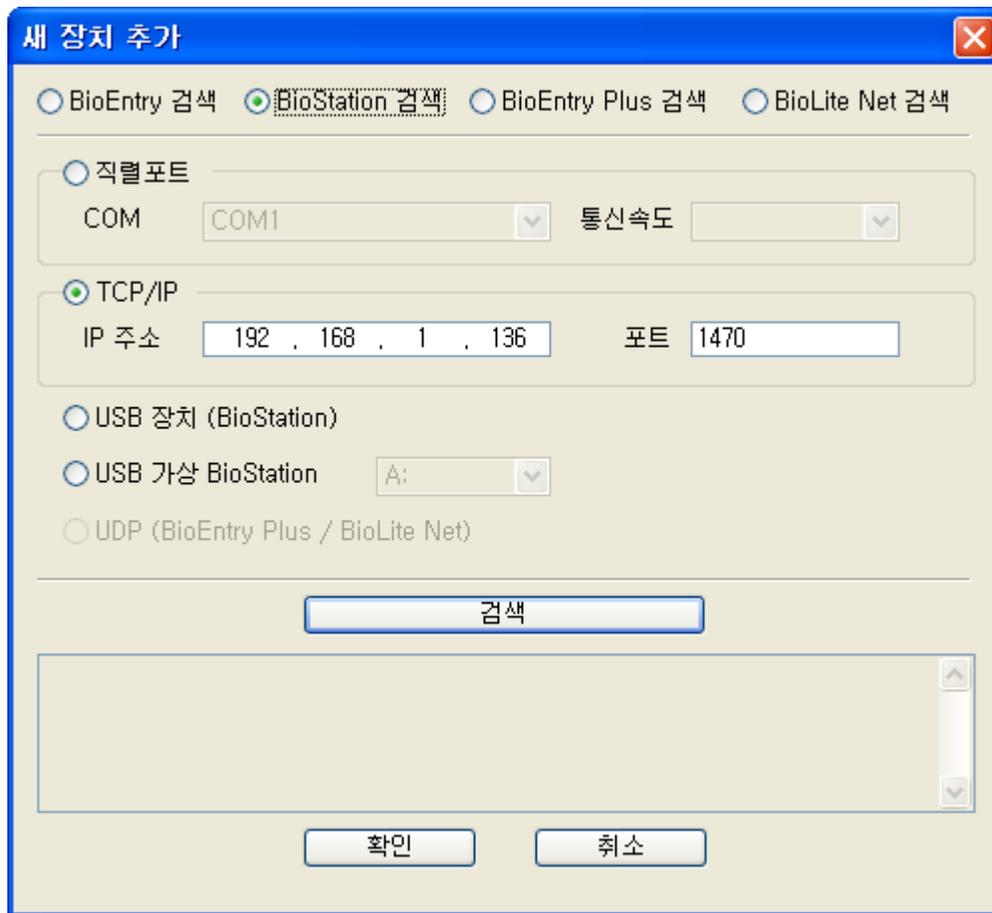


5.1.2. 이더넷

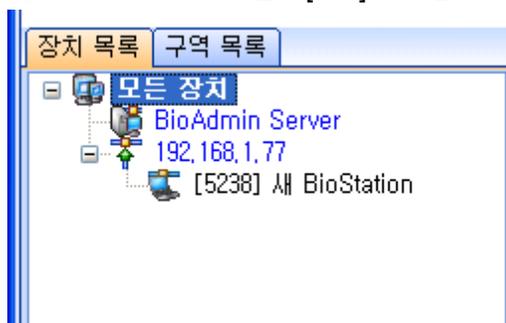
장치와 호스트 PC가 이더넷으로 연결된 경우, 새 장치 추가창의 TCP/IP에서 IP 주소와 포트를 입력합니다.

BioStation 과 BEACon, BioLite Net 의 경우, IP 주소를 장치에서 확인할 수 있습니다. 자세한 방법은 각 장치의 사용설명서를 참조하시기 바랍니다. BioEntry의 경우, 이더넷 인터페이스가 지원되지 않지만 호스트 PC에서 Ethernet to Serial 컨버터를 이용하여 이더넷으로 연결할 수 있습니다. 이 때에는 장착된 Ethernet to Serial 컨버터의 IP 주소를 입력하면 됩니다.

포트는 모두 1470으로 입력하여야 합니다.

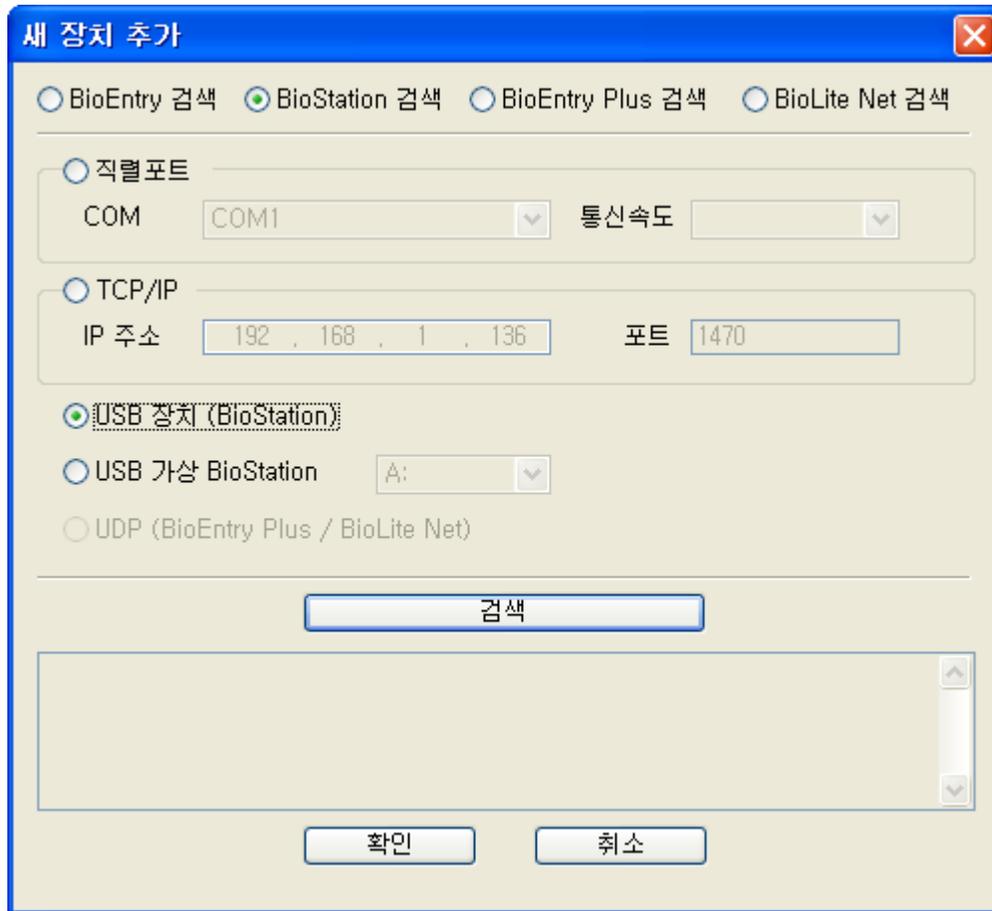


장치가 네트워크와 올바르게 연결되었다면, 검색된 장치 ID가 장치 트리 윈도우 상의 포트아래 각괄호[****] 와 함께 나타날 것입니다.



5.1.3. USB 장치

BioStation을 호스트 PC와 USB로 연결한 경우, USB 장치를 선택하고 검색하면 됩니다.



5.1.4. USB 가상 BioStation

BioAdmin에서는 USB 메모리를 사용하여 특정 BioStation을 가상 장치로 사용할 수 있습니다. BioStation에 USB 메모리를 연결하여 BioStation의 사용자, 로그 및 설정상태를 저장한 뒤 PC에 연결하면 BioAdmin에서 마치 해당 BioStation이 연결되어 있는 것처럼 대부분의 기능을 사용할 수 있습니다.

Note: USB 가상 BioStation을 사용하기 위해서는 PC 운영 체제에서 USB 메모리를 올바른 USB 드라이브로 인식해야만 사용이 가능합니다. 따라서, 사용자 임의로 드라이브 내의 파일을 변경하는 경우 오작동의 원인이 될 수 있

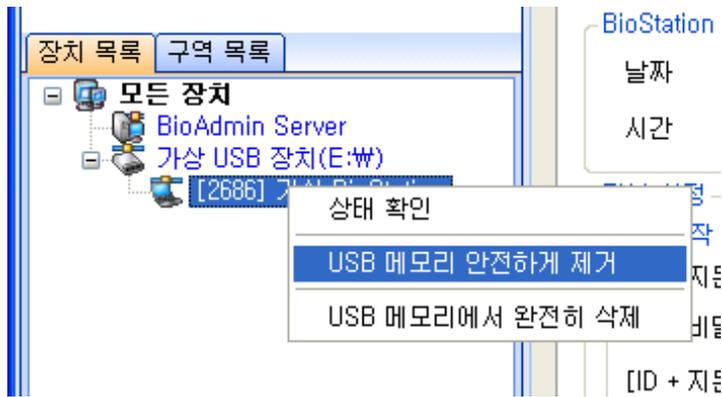
습니다.

아래와 같은 방법으로 USB 가상 BioStation을 네트워크에 추가합니다.

- USB 가상 BioStation을 사용하기 위해서는 우선 사용자 정보 및 설정을 변경하고자 하는 BioStation으로부터 USB 가상 장치를 생성해야만 합니다. USB 가상 BioStation 생성방법에 대해서는 BioStation 사용자 설명서를 참조하시기 바랍니다.
- 생성된 USB 가상 BioStation을 PC에 연결하여 USB 드라이브로 인식하도록 한 후 '내 컴퓨터'에 해당 드라이브가 추가된 것을 확인합니다.
- BioAdmin의 새 장치 추가 메뉴에서 **USB 가상 BioStation** 을 선택합니다.
- 해당 USB 가상 BioStation 의 드라이브를 선택한 후 **검색** 버튼을 누릅니다.
- **확인** 버튼을 눌러 USB 가상 BioStation 을 장치로 등록 합니다.

The screenshot shows a dialog box titled "새 장치 추가" (Add New Device). It has four radio buttons at the top: "BioEntry 검색", "BioStation 검색" (which is selected), "BioEntry Plus 검색", and "BioLite Net 검색". Below these are three sections: "직렬 포트" (Serial Port) with "COM" set to "COM1" and "통신속도" (Baud Rate) empty; "TCP/IP" with "IP 주소" (IP Address) set to "192.168.1.136" and "포트" (Port) set to "1470"; and "USB 장치 (BioStation)" with "USB 가상 BioStation" selected and the drive set to "A:". At the bottom, there is a "검색" (Search) button, and "확인" (OK) and "취소" (Cancel) buttons.

이제 PC에서 원하는 사용자를 저장하거나, 장치의 설정을 변경한 뒤에 적용하여 USB 메모리에 기록한 뒤 'USB 가상장치 안전하게 제거' 메뉴를 통해서 USB 메모리를 PC에서 분리합니다.



5.1.5. UDP (BioEntry Plus / BioLite Net)

BioEntry Plus와 BioLite Net은 BioStation 과 달리 UDP 를 이용하여 장치를 추가합니다.

동일 네트워크 내에 새로 설치된 BioEntry Plus 및 BioLite Net 을 검색하여 발견된 장치를 선택하여 각각의 네트워크 설정을 하여야 합니다.

BioEntry Plus 및 BioLite Net 은 DHCP 를 지원하는 네트워크인 경우 자동으로 IP 를 할당 받게 됩니다. 검색된 장치를 선택하고 서버 IP의 주소를 입력하여 설정을 합니다.

이때, DHCP 를 지원하지 않는 네트워크에 설치된 경우, BioEntry Plus 는 임의로 부여된 IP로 검색됩니다. 해당 장치를 선택하여 네트워크 관리자가 지정한 IP로 변경하여야 하며, 이때는 1대의 장치만이 리스트에 보여지기 때문에 각각 검색과 설정을 하여야 합니다.

Note: BioEntry Plus 는 장치에서 IP를 입력할 수 없기 때문에 먼저 BioAdmin 을 사용하여 설정해야 합니다. DHCP 를 사용하지 않는 네트워크에서는 장치가 임의의 지정된 IP로 검색이 되지만, 두 대 이상의 장치가 동시에 설치되었을 경우에는 새 장치간 IP 가 동일하게 판단되어, 충돌을 피하기 위해 각각 1대씩 검색이 됩니다.

새 장치 추가

BioEntry 검색
 BioStation 검색
 BioEntry Plus 검색
 BioLite Net 검색

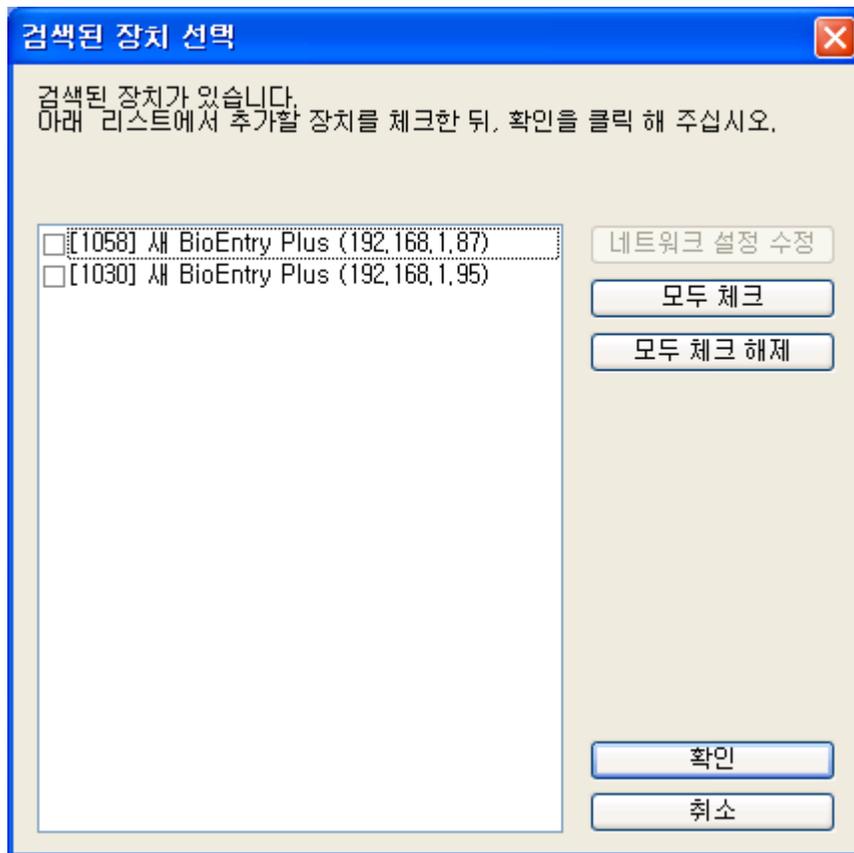
직렬포트
 COM 통신속도

TCP/IP
 IP 주소 포트

USB 장치 (BioStation)
 USB 가상 BioStation

UDP (BioEntry Plus / BioLite Net)

‘새 장치 추가’ 창에서 **UDP** 를 선택 후, 검색을 클릭하면 동일 네트워크에 연결되어 있는 **BioEntry Plus** 가 모두 검색 됩니다. 단, 회선의 문제로 일정 시간 응답이 없는 장치는 검색이 되지 않을 수도 있습니다.



- 확인을 클릭하면 검색된 장치 선택 창이 뜨며, 리스트에서 설치하고자 하는 장치의 ID 를 찾아 체크한 후, 네트워크 설정 수정을 클릭하여 설정 정보를 변경합니다. 이미 정상적으로 설치가 완료된 장치는 리스트에서 보이지 않습니다.
- 네트워크 환경에 따라 DHCP 를 선택하고, 서버를 사용하는 경우 체크를 하여 서버 주소를 입력할 수 있습니다.
- BioEntry Plus 는 기본적으로 1471 Port 를 사용하며, 변경이 가능합니다.
- 설정이 끝난 후, 확인을 클릭하면 장치목록에 추가된 새 장치가 나타나며, 이후 리스트 내의 장치명에서 오른쪽 마우스를 클릭하면 설정변경이 가능합니다.

Note: BioEntry Plus 의 네트워크 설정에서 '서버 사용'으로 체크하는 경우에는 BioAdmin 이 설치된 PC의 IP를 입력하고, 서버 설정에서 입력한 TCP/IP 포트를 입력해야 합니다. (초기 기본값은 1480으로 사용합니다.)
장치가 설치 되었으나 1-2초 후 바로 연결이 끊어지는 경우에 발생하는 가장 빈번한 문제이므로 주의하시기 바랍니다.

- BioLite Net의 UDP를 통한 검색은 BioEntry Plus와 동일한 방법으로 진행하시면 됩니다.

5.2. BEACon 컨트롤러 추가

BEACon 컨트롤러를 검색하여 추가하는 과정입니다.

BEACon 검색

직렬 포트

포트번호 전송속도

TCP/IP

IP 주소 포트

BEACon

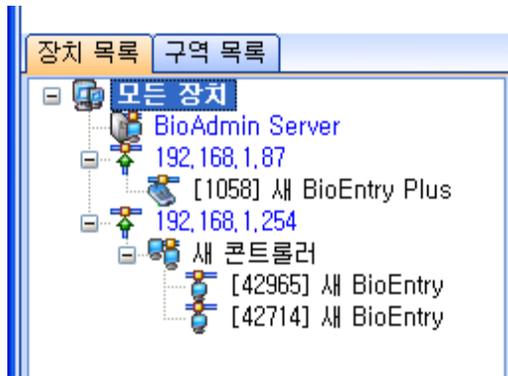
BEACon ID

이름

BioEntry #1

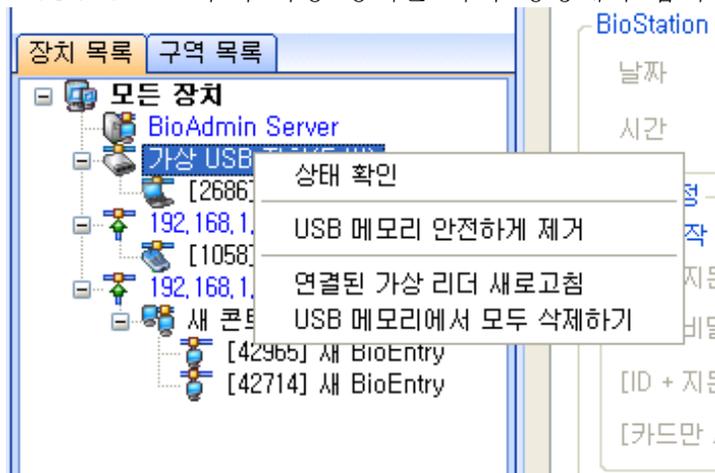
BioEntry #2

- 작업박스에서 새 컨트롤러 추가 버튼을 누릅니다.
- 시리얼과 TCP/IP 중에서 통신 방법을 선택합니다.
- 시리얼의 경우 COM 포트와 통신속도를 설정하고, TCP/IP의 경우 추가하고자 하는 BEACon의 IP 주소를 입력합니다. BEACon에서 IP 주소를 확인하는 방법은 BEACon의 사용설명서를 참조하시기 바랍니다.
- **BEACon ID** 난에 추가하고자 하는 BEACon의 ID를 입력합니다. BEACon에서 ID를 확인하는 방법에 대해서는 BEACon의 사용설명서를 참조하시기 바랍니다.
- **Name** 난에 BEACon의 이름을 적절히 정하여 입력합니다.
- **장치 검색** 버튼을 누르면 해당 BEACon과 거기에 연결된 BioEntry 장치를 검색합니다.
검색 결과로 BioEntry #1, BioEntry #2 난에 연결된 BioEntry의 ID가 표시됩니다. 만약 IP 주소나 ID 입력이 잘못 되어 BEACon를 검색하지 못한 경우 여기에 None로 표시됩니다.
- 확인 버튼을 누르면 장치리스트에 검색한 BEACon과 거기에 연결된 BioEntry를 확인할 수 있습니다.



5.3. 장치제거

- 장치리스트에서 장치를 선택하고 작업박스의 장치제거를 클릭하면 선택한 장치를 제거하게 됩니다. 장치리스트의 장치를 선택하고 오른쪽 마우스를 클릭하여 제거를 선택하여도 됩니다.
- USB 가상 BioStation은 장치리스트의 해당 드라이브 또는 장치에서 오른쪽 마우스를 클릭할 경우 아래의 방법으로 삭제 할 수 있습니다.
 - USB 메모리 안전하게 제거: USB 메모리내의 모든 가상 BioStation에 데이터를 저장한 뒤에 PC로부터 분리하기 전에 사용합니다. 만약 저장이 완료되기 전이나, USB 메모리의 데이터를 사용하는 중에 분리하면 데이터의 일부를 잃어버릴 수 있다.
 - USB 메모리에서 모두 삭제하기: 연결된 USB 메모리 내에 생성된 모든 가상 BioStation의 데이터를 삭제합니다. 다시 사용하기 위해서는 BioStation으로부터 가상 장치를 다시 생성해야 합니다.



- USB 메모리에서 완전히 삭제: 선택한 USB 가상 BioStation을 USB 메모리에서 완전히 삭제합니다.

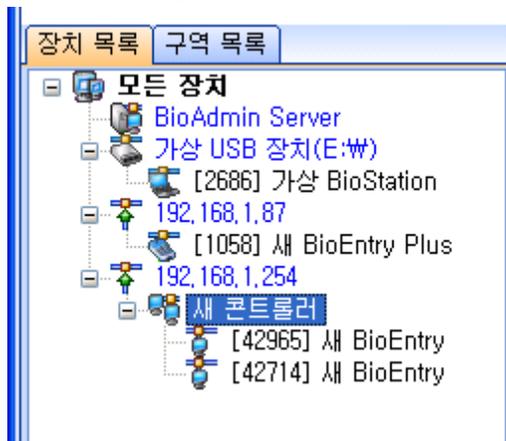


5.4. 목록창

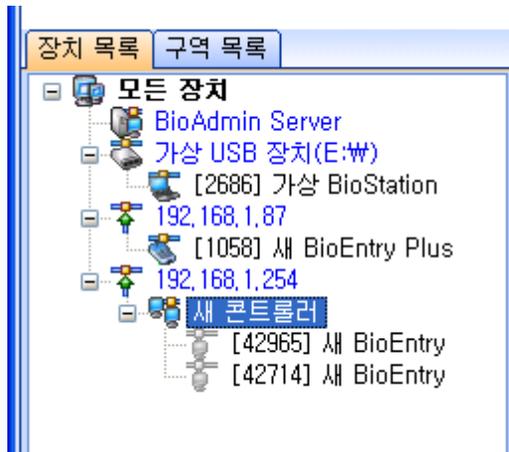
목록창은 장치 목록과 구역 목록을 나타내며, 장치 목록에서는 장치의 현재 상태를 아이콘 형태로 표시하고, 구역목록에서는 장치간 설정된 구역에 대한 리스트를 표시합니다.

5.4.1. 장치목록

- [장치목록] 장치가 연결되어 있다면 아이콘은 활성화됩니다.



- [장치목록] 장치가 연결되어 있지 않다면 아이콘은 비활성화됩니다.



각 장치의 상태는 다음 경우에 갱신됩니다.

- 소프트웨어가 시작될 때
- 장치가 새로이 선택될 때
- 상태 확인 메뉴를 클릭할 때
- '장치 목록 새로 고침' 을 클릭할 때

5.4.2. 구역목록

구역목록은 연결된 각 장치들을 관리나 통제를 위해 그룹으로 묶을 수 있도록 설정하고, 리스트를 보여줍니다.

목록창에서 구역목록을 클릭하면, 현재 서로 연결된 장치들끼리 각각의 구역으로 보여지며, 구역 설정이 되지 않은 장치들은 '구역없음'에 하위 장치로 표시 됩니다.

- 하위구역 추가
 - 구역을 설정하고자 하는 마스터장치를 마우스 오른쪽 버튼으로 클릭하게 되면 나타나는 메뉴 중에 '새 구역 생성' 을 클릭 합니다..
 - 구역설정창이 나타나면 구역 이름을 입력하고 구역에서 마스터 역할을 할 장치를 선택합니다.
 - 마스터 장치와 같은 구역으로 설정할 구성장치를 선택하여 체크하고 다음을 클릭 합니다.
 - 구역 내 장치들 간 원하는 동기화에 체크를 하고 다음을 클릭합니다.
 - 하위 구역을 어떤 용도로 사용할 것인지 설정합니다. 동일 구역 내 장치들 간 동기화만 목적으로 한다면 '하위 구역 설정 안함' 을 선택해야 합니다.
 - 새로운 **Anti-passback** 구역 생성은 동일 구역 내 연결된 장치를 입실용 장치와 퇴실용 장치로 구분하여, 입실용 장치에 지문인증을 성공하여 들어온 사용자만 퇴실용 장치에서 인증이 되도록 설정할 수 있습니다. 보안을 강조하는 은행 금고, 연구소 등에서 출입자를 관리하기 위해 사용할 수 있습니다.
 - 새로운 인증제한구역 생성은 동일 구역 내 단말기들의 동기화된 인증 로 그를 토대로 인증 제한 기능을 일괄적으로 적용할 수 있도록 설정할 수

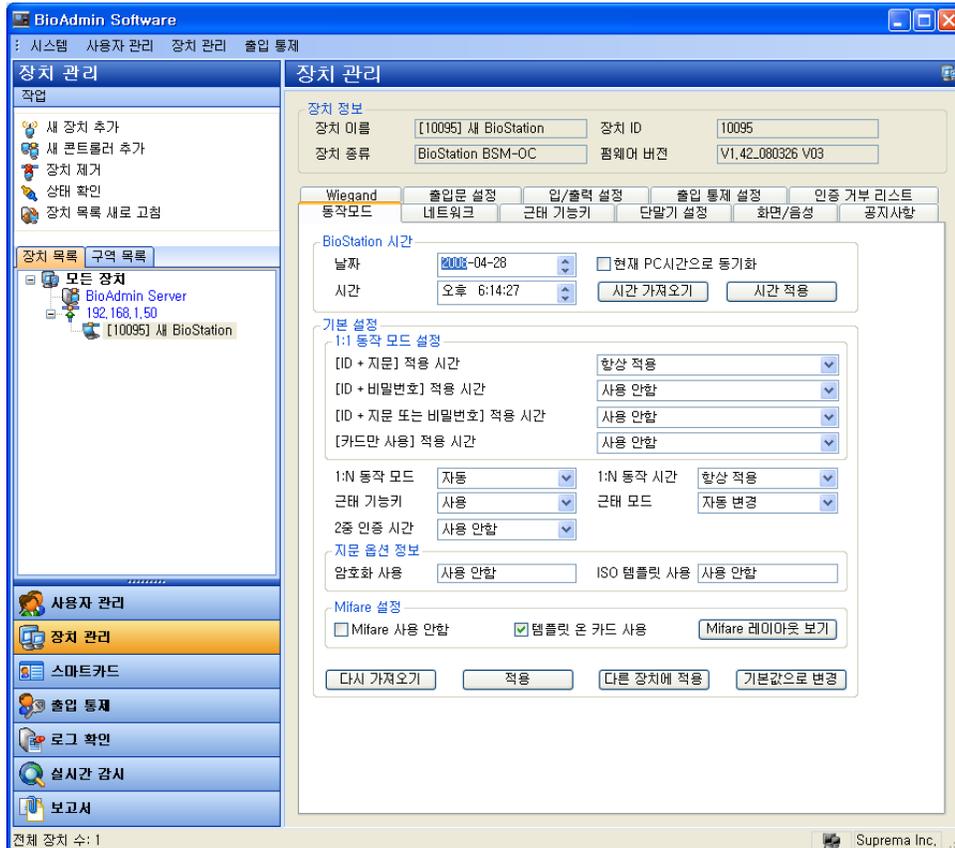
있습니다. 일정 시간 내 반복 인증을 받지 못하게 설정을 해 두면 동일 구역 내 장치간에는 어떤 장치에서 인증을 받더라도 나머지 장치들도 설정 값에 따라 반복 인증을 거부 합니다.

- 구역 구성 장치에서 장치를 선택한 후, 다음을 누르면 인증 허용 시간과 최대인증허용횟수를 설정할 수 있으며, 반복 인증을 허용하는 최소 시간값을 입력하여 적용할 수 있습니다.

Note: 같은 구역으로 연결된 각각의 장치는 설정에 따라 사용자 정보, 로그 정보, 시간 정보 등을 자동으로 동기화 할 수 있으며, 하나의 구역을 **Anti-Pass Back Zone**으로 설정하여 출입을 통제할 수 있습니다. 또한 같은 구역 내 단말기 간 동기화 된 로그를 이용하여 여러 대의 단말기에서 동시에 인증 횟수 제한 등을 설정할 수 있도록 하여 식수 관리 등에 활용할 수 있습니다.

5.5. BioStation 장치 관리

장치 리스트에서 **BioStation**을 선택하면, 선택된 **BioStation** 의 장치 설정 윈도우가 주 윈도우에서 갱신됩니다.



장치 설정 윈도우는 2개 영역으로 나누어 집니다.

- 장치 정보

장치 정보는 선택된 장치의 종류, 이름, 일련 번호, 펌웨어 버전을 표시합니다.

- 환경설정 윈도우

환경설정 윈도우는 장치리스트에서 선택된 **BioStation** 장치의 환경설정 값을 보여주고 이를 수정할 수 있게 합니다. 환경설정 메뉴들은 동작모드, 네트워크, 근태 기능키, 설정, 화면/음성, 공지사항 등을 나타내는 분리된 탭들로 구성되어 있습니다.

환경설정 윈도우 아래쪽에는 **다시 가져오기, 적용, 다른 장치에 적용, 기본값으로 변경** 네 가지 버튼이 있습니다.

- **다시 가져오기:** 장치의 설정 값을 다시 불러옵니다.
- **적용:** 현재 윈도우에 수정한 설정 값을 장치에 적용합니다.
- **다른 장치에 적용:** 현재 윈도우에 수정한 설정 값을 다른 장치에도 적용합니다. 장치 선택 윈도우에서 장치를 선택할 수 있습니다.
- **기본값으로 변경:** 설정 값을 기본 설정 값으로 변경합니다. 이 값을 실제로 장치에 적용하려면 반드시 적용 버튼을 눌러야 합니다.

5.5.1. 장치정보

선택한 **BioStation**의 장치 이름, 장치 종류 및 단말기 ID와 펌웨어 버전을 확인할 수 있습니다. 단말기 ID 번호와 펌웨어 버전 등은 설치 후 기술 지원 등에서 제품을 확인하기 위해 필요한 정보입니다.

5.5.2. 동작모드

- 시간 설정

처음에 보이는 날짜와 시간이 **BioStation**에서 읽어온 값입니다. **시간확인** 버튼을 클릭하면 **BioStation**으로부터 날짜와 시간을 다시 읽어옵니다.

BioStation의 시간 변경 방법은 직접 입력 방법과 현재 **PC** 시간으로 동기화의 두 가지 방법으로 나뉩니다.

- **직접 입력:** 날짜와 시간 창에서 숫자를 직접 입력하거나 숫자에 커서를 두고 위아래 화살표를 클릭하여 입력합니다. 입력 후 **시간적용** 버튼을 누르면 입력된 날짜와 시간이 선택된 **BioStation**으로 전송됩니다.
- **PC 시간으로 동기화:** 현재 **PC시간으로 동기화**를 체크하고, **시간적용** 버튼을 누르시면 선택된 **BioStation** 의 시간이 현재 **PC**의 시간으로 맞춰집니다.

BioStation 시간

날짜	2006-07-29	<input type="checkbox"/> 현재 PC시간으로 동기화
시간	오후 7:19:02	<input type="button" value="시간 확인"/> <input type="button" value="시간 적용"/>

● 기본설정

- 1:1 동작모드설정: **BioStation**에서 1:1 인증을 하려면 사용자는 자신의 ID를 입력한 후 지문이나 비밀번호를 통해 본인임을 인증하여야 합니다. 인증 방식에 대한 설정을 각 시간대별로 지정할 수 있으며, 초기값으로 항상 적용과 사용 안 함이 있습니다. 세부적인 시간을 적용하고자 하는 경우에는 메인 메뉴의 '출입통제' 에서 설정한 출입시간 중에 하나를 선택하여 적용할 수 있습니다.
단, 설정된 출입시간은 모든 장치에 전송이 되어 있어야 합니다.

1:1 동작 모드 설정

[ID + 지문] 적용 시간	사용 안함
[ID + 비밀번호] 적용 시간	사용 안함
[ID + 지문 또는 비밀번호] 적용 시간	항상 적용
[카드만 사용] 적용 시간	사용 안함

- 1:N 동작모드 : 1:N 인식 모드에서는 사용자 ID 입력 없이 지문 만으로 본인 인증을 하게 됩니다. 이 때 지문입력을 어떻게 시작할 것인지에 대하여 자동 , OK 버튼 또는 근태기능키 , 사용 안 함의 3가지 모드를 선택할 수 있습니다. 자동 모드에서는 **BioStation**의 센서가 항상 입력 대기 상태여서 손가락을 대면 바로 인식을 합니다. OK 버튼 또는 근태기능키를 선택 시에는 OK 버튼 또는 근태기능키를 눌러야만 지문의 입력이 가능합니다. 1:N 인식 기능을 사용하지 않고 1:1 인증으로만 사용 할 경우 사용 안 함 모드를 선택하면 됩니다. 근태 기능키: 근태 기능키는 출근, 퇴근, 외근, 복귀 등과 같이 근태관리 용도로 지문입력 전에 근태이벤트를 입력하기 위한 키를 의미합니다. **BioStation**에서는 보통 F1부터 F4까지의 기능키를 이러한 용도로 사용하며, 필요할 경우 16개까지 기능키를 확장할 수 있습니다. 근태 기능키 모드는 사용과 사용 안 함 두 가지 중에 선택하게 되어 있습니다. **BioStation**을 출입통제 전용으로 사용할 경우에는 사용 안 함을 선택하고, 근태관리 용으로 이용할 경우 사용함을 선택하면 됩니다. 이 때에는 **BioStation**에서 근태 기능키를 먼저 누르고 지문 입력을 하면 해당 근태이벤트가 로그에 기록되게 됩니다. 향후 근태관리 소프트웨어에서 이 로그정보를 이용하여 각종 근태 및 급여 관리 데이터로 사용할 수 있습니다.

1:N 동작 모드	자동	1:N 동작 시간	항상 적용
근태 기능키	사용	근태 모드	사용 안함
2중 인증 시간	사용 안함		

- 1:N 동작시간 : 위에서 설정한 1:N 동작모드에 대해 설정된 시간에만 적용 되도록 시간을 선택할 수 있습니다. 이 때도 출입통제에서 미리 정해 놓은 출입시간을 적용할 수 있으며, 설정해 놓은 각 출입시간은 장치 내에 전송이 되어 있어야 합니다.
- 근태모드 : 장치의 기능키를 자동으로 지정 또는 변경 되도록 설정이 가능합니다. 자동변경, 수동변경, 고정 중에 하나를 선택 후, 근태기능키 탭에서 세부적인 설정을 합니다.
 - 자동변경 : 설정된 시간에 따라 자동으로 장치의 근태 입력모드가 변경됩니다. 자동변경을 선택 후, 근태기능키 탭을 클릭하면 '자동모드적용시간' 이 활성화 됩니다. 출입통제에서 미리 정한 출입시간을 선택하면 해당 시간에 설정된 근태 기능키 입력 모드로 자동 변경 됩니다
 - 수동변경 : 사용자가 근태기능키를 누르고 인증하는 경우, 해당 근태기능키가 계속 유지 되어 다음 사용자가 기능키를 누르지 않고 인증할 때 자동으로 이전 사용자가 누른 기능키를 적용합니다.고정 : 장치에 특정 근태 기능키로 고정할 수 있습니다. 고정을 선택 후, 근태기능키 탭을 클릭하면 고정이라는 체크상자가 활성화 되어 있으며, 특정 근태 기능키에서 고정을 선택 시, 장치는 해당 기능키로 고정되어 키 입력 없이 지문 인증만 하여도 해당 근태기능키가 자동 입력 됩니다
- 2중인증시간 : 이중인증시간은 두 개의 지문이 인증에 성공해야, 외부로 릴레이를 전달하여, 문을 개방하거나 경광등을 작동 시키는 등의 동작을 수행할 수 있도록 합니다. 인증이나 로그 기록은 동일하게 동작합니다. 항상 사용하거나 사용하지 않을 수 있으며, 출입통제에서 설정한 출입시간을 선택하여 적용할 수 있습니다.

Note: 이중인증은 보안성을 강조하는 장소의 출입 통제를 위해 설정할 수 있으며, 2인 1조가 되어 인증하는 경우에만 출입을 허용되도록 구성합니다.

각종 모드 등 설정 값을 변경할 경우 적용 버튼을 눌러야 실제로 장치에 적용 됩니다. 윈도우 하단 버튼에 대한 보다 자세한 설명은 앞 페이지의 설명을 참조하기 바랍니다.

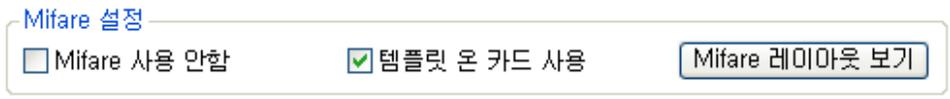
● 지문 옵션 정보

지문 옵션 정보

암호화 사용	사용 안함	ISO 템플릿 사용	사용 안함
--------	-------	------------	-------

- 암호화 사용: 바이오 정보 보호가이드를 적용 선택한 경우에 사용함으로 표시되고 그 외에는 사용 안 함으로 표시됩니다.
- ISO 표준 템플릿 사용: ISO 표준 템플릿 사용 유무를 나타냅니다.

● Mifare 설정



- Mifare 사용 안 함: 체크하면 Mifare 기능을 사용하지 않습니다.
- 템플릿 온 카드 사용: Mifare 카드에 사용자 정보를 저장할 것인지를 결정합니다. 체크하면 사용자 정보를 카드에 저장합니다.
- Mifare 레이아웃 보기: 현재 BioStation™에 저장된 Mifare의 레이아웃을 보여줍니다. BioStation™의 Mifare 레이아웃 정보는 6.5.7. Mifare 카드 레이아웃 설정 (BioStation / BioEntry Plus) 절을 참조 하십시오.

5.5.3. 네트워크

장치의 각종 네트워크 설정 창입니다. 인터페이스 방법에 따라 LAN, 시리얼통신, USB 세 가지로 나누어져 있습니다.

● LAN

윈도우 상단 네트워크 설정 리스트박스에서 LAN을 사용할 것인지, 사용할 경우 유선 LAN을 사용할 것인지 무선 LAN을 사용할 것인지를 설정합니다. 포트는 1470을 지정하여야 합니다.



● 무선 LAN 설정

BioStation은 무선 네트워크를 통해서도 통신이 가능합니다. 이 무선 네트워크를 사용하기 위해서는 아래와 같은 준비사항이 필요합니다.

먼저 무선 연결이 가능한 Access Point가 필요합니다. Access Point는 각각의 고유한 SSID를 가지고 있으며, 몇 가지 암호화 방식을 통해서 데이터를 암호화 하는 기능을 사용하기도 합니다. BioStation은 WPA_PSK, WEP 방식의 암호화를 지원합니다. Access Point의 사용 설명서를 참고하여 현재 사용 중인 암호화 방식이 있는 지와 어떤 방식인지를 파악해야 합니다.

BioStation의 경우 4가지의 프리셋을 정의할 수 있으며, 미리 정의된 이 프리셋을 선택 함으로써 무선랜 기능이 활성화 됩니다. 물론 이때는 유선랜은 사용할 수 없습니다.

네트워크	무선 LAN 사용	포트	1470
무선랜 설정			
프리셋	프리셋 1번	설정 변경	
프리셋이름	WPA	ESSID	biostation_wpa
네트워크 인증	WPA_PSK	암호화방식	TKIP/AES
TCP/IP	<input checked="" type="radio"/> DHCP 사용 <input type="radio"/> DHCP 사용 안함		
IP 주소	0 . 0 . 0 . 0	게이트웨이	0 . 0 . 0 . 0
서브넷	0 . 0 . 0 . 0	연결 허용	1

- 프리셋 설정하기: BioStation이 4가지 프리셋을 가질 수 있습니다.

BioStation 무선랜 설정

프리셋 이름: WPA

네트워크이름(SSID): biostation_wpa

무선 네트워크 키

네트워크 인증: WPA_PSK

데이터 암호화: TKIP/AES

네트워크 키:

네트워크 키 확인:

확인 취소

- 프리셋 이름: BioStation에서 프리셋을 보여주는 이름입니다.
- SSID: Access Point의 고유 ID입니다. 이 ID를 잘못 사용하면 무선랜 기능을 사용할 수 없습니다. 현재 사용 중인 Access Point의 SSID를 확인하려면 네트워크 관리자 혹은 해당 기기의 사용자 설명서를 참고하시기 바랍니다.

- 네트워크 인증: 네트워크 인증은 개방 모드, 공유 모드, WPA-PSK 방식이 있으며, 이 인증 방식에 따라 사용할 수 있는 암호화 방식에 차이가 있습니다.
- 암호화 방식: 암호화 방식은 크게 사용 안 함, WEP, WPA-TKIP/AES 방식을 지원하며, WEP 및 WPA-TKIP/AES의 경우 사용자가 정의한 암호화 키에 의해서 통신하는 데이터를 암호화 합니다. (이 키는 사용자 지문 데이터를 암호화 하는데 사용하는 암호화 키와는 다른 것입니다.)

무선랜을 사용함에 있어서, Access Point와의 거리가 너무 멀거나, 장애물이 많은 경우에는 통신에 장애가 발생할 가능성이 있습니다. 또한 각 Access Point마다의 특성 차이로 연결이 안되거나 통신 상태가 매우 불량할 가능성이 있으므로 무선랜을 통한 통신 이외에 별도의 통신 가능한 방법을 마련해 둘 것을 권장합니다.

● 서버 IP

서버 IP: 서버 IP는 BioAdmin Server가 설치된 PC의 IP를 입력하는 것으로 일일이 BioStation의 IP를 확인하지 않아도 자동으로 BioAdmin Server에 장치를 등록할 수 있게 해줍니다. 다만, BioAdmin Server를 사용하는 PC가 방화벽을 사용하여 보호되고 있거나, BioStation과는 서로 다른 공유기를 사용하는 등 네트워크 연결에 따라서 접속이 불가능한 경우도 있습니다. 이때는 해당 네트워크를 구성한 관리자에게 문의하여 도움을 받도록 하십시오.

서버 설정	<input checked="" type="radio"/> 사용 <input type="radio"/> 사용 안함	<input type="checkbox"/> 서버와 자동으로 시간 동기화
서버 IP 주소	192 . 168 . 1 . 24	서버 포트 1480

● IP 설정

BioStation의 설정 값 중에서 IP 주소를 자동으로 받을 것인지, 수동으로 설정할 것인지를 선택합니다. DHCP로 BioStation에 IP 주소가 자동으로 부여될 경우 자동으로 IP 주소 받기를 체크합니다. DHCP를 사용하지 않을 경우에는 수동으로 IP 주소 설정을 체크하고 IP 주소, 게이트 웨이, 서브 넷 마스크, DNS 등을 설정합니다.

이와 같이 LAN 설정 값을 바꾸는 것은 Serial이나 USB로 연결된 BioStation을 LAN으로 연결하기 위하여 IP 값 등을 설정하거나, 이미 LAN으로 연결된 BioStation의 IP 주소를 다른 주소로 바꾸는 경우 등에 필요합니다.

연결허용은 BioStation 이 서버가 아닌 일반 TCP/IP로 연결되어 있을 경우 동일한 BioStation 에 연결될 수 있는 PC 의 개수를 말합니다. 만약 연결허용을 4로 설정한다면 최대 4대의 PC에서 BioAdmin을 통해 동일한 BioStation을 찾을 수 있습니다. 물론, 서버에 연결되어 있을 경우에는 연결허용의 제약 없이 모든 서버 및 클라이언트 PC 에서 동 BioStation을 찾을 수 있습니다.

● 서버 설정

해당 BioStation이 서버에 연결되어 있는지를 보여줍니다.

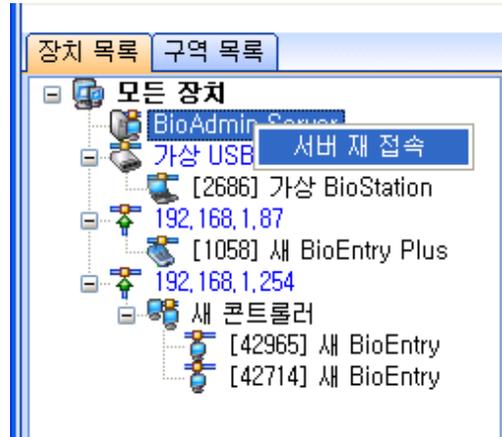
서버가 아닌 일반 TCP/IP로 연결된 BioStation을 서버에 연결시키고자 할 경우에는 사용에 체크한 후 서버 IP 주소와 서버 포트를 설정하면 됩니다.

이처럼 서버에 연결하는 경우에는 해당 BioStation은 원래 연결되어 TCP/IP에서 연결이 즉시 해제되며, 다시 서버에 연결되기까지는 네트워크 환경에 따

라 다소 시간이 걸릴 수 있습니다.

서버와 자동으로 시간 동기화에 체크하면 해당 BioStation의 시간이 서버의 시간에 자동으로 맞추어 집니다. 이 작업은 1시간을 주기로 시행 됩니다.

서버에 연결된 BioStation의 통신상태가 좋지 않을 때에는 장치리스트에 있는 BioAdmin Server 서버에서 마우스 오른쪽 버튼을 클릭한 후 서버 재 접속을 시도하십시오.



- 시리얼 통신-RS232

BioStation의 RS232 포트의 통신속도를 설정합니다. 기본 설정 값은 115,200 bps 입니다. 시리얼 통신에서 통신선의 상태 등에 문제가 발생할 경우 통신속도를 좀 더 낮은 값으로 바꾸는 것이 해결책이 되는 경우도 있습니다.

- 시리얼 통신-RS485

BioStation의 RS485 포트로 통신을 사용하는 경우에 대해 설정합니다.

RS485모드에서는 서로 연결된 장치가 호스트(Host)와 슬레이브(Slave) 역할을 나누어 하게 되며 해당 장치를 Host 로 할지 Slave 로 할지를 결정 합니다.

BioStation, BioEntry Plus 및 Secure I/O 로 구성되는 통합 시스템은 Host 장치 1대, Slave 장치 1대와 함께 4대의 Secure I/O 가 최대로 연결되며, Host 장치는 총 10개의 릴레이와 20개의 입력을 관리합니다.

- 시스템의 장치 구성에 따라 다음과 같이 설정 합니다.
- BioStation 을 출입문 바깥쪽에 설치하고 BioEntry Plus 를 안쪽에 설치하는 경우.

일반적으로 보안을 위해 안쪽에 설치된 장치에서 출입문 오픈 릴레이를 내 보내게 되므로 안쪽에 설치되는 BioEntry Plus 를 'Host'로 설정합니다. BioStation는 'Slave'로써 하위장치가 되며 RS485로 BioEntry Plus 에 연결합니다. 설정 방법으로는 BioEntry Plus의 장치관리 메뉴 내 네트워크 탭에서 'Host' 선택 후 하위장치인 BioStation의 ID를 입력하고, 'Slave' 장치가 되는 BioStation에서는 장치관리 메뉴의 네트워크 탭에서 'Slave' 로 지정해 두어야 합니다.

- BioStation 을 출입문 바깥쪽에 설치하고 보안성 강화를 위해 Secure I/O 를 설치하는 경우

BioStation이 'Host' 가 되어 Secure I/O 의 입출력을 제어하며, 인증에 성공하면 BioStation 은 Secure I/O 를 통해 출입문을 열게됩니다. 설정 방법으로는 BioStation 을 'Host' 로 설정 후, 제어하고자 하는 SIO 를 Check 합니다. 총 4대

까지 연결이 가능하며, **Secure I/O** 뒷면의 딥스위치를 조정하여 부여된 번호를 선택합니다. **Secure I/O** 의 기본 입출력 설정을 통해 출입문이나 비상 경광등 등을 제어할 수 있습니다.

- **Secure I/O** 에 대한 자세한 설명은 **Secure I/O** 매뉴얼을 참조하시기 바랍니다.**USB 연결**

BioStation의 **USB** 포트를 통한 호스트 **PC**와의 연결을 허용할 것인지를 선택합니다. **USB** 포트는 외부로 노출되는 포트이므로 보안상의 이유로 연결을 허용하지 않는 경우도 있습니다.

5.5.4. 근태 기능 키

근태 기능키는 출근, 퇴근, 외근, 복귀 등과 같이 근태관리 용도로 지문 입력 전에 근태이벤트를 입력하기 위한 키를 의미합니다. **BioStation**에서는 보통 **F1**부터 **F4**까지의 기능키를 이러한 용도로 사용하며, 필요할 경우 **16**개까지 기능키를 확장할 수 있습니다. **BioStation**에서 근태 기능키를 먼저 누르고 지문 입력을 하면 해당 근태이벤트가 로그에 기록되게 되며, 향후 근태관리 소프트웨어에서 이 로그정보를 이용하여 각종 근태 및 급여 관리 데이터로 사용할 수 있습니다.

BioAdmin 소프트웨어에서 근태 기능키와 관련하여, 장치관리 메뉴에서의 내용과 보고서 메뉴에서 근태관리 규칙에서의 내용을 모두 참조해야 합니다.

여기서 설명하는 장치관리 메뉴에서의 근태 기능키 설정은 **BioStation**의 화면에서 보이는 근태 이벤트의 메시지를 설정하는 것이고, 보고서 메뉴의 근태관리 규칙에서의 근태 기능키 설정은 근태 보고서 생성시 적용할 근태 이벤트 메시지를 설정하는 것입니다. **BioStation**의 로그에서는 실제 근태이벤트 메시지가 기록되지 않고 눌러진 근태 기능키의 번호가 기록됩니다. **BioAdmin**에서는 이 값을 읽어 미리 정의된 기능키와 근태이벤트 간의 테이블을 참조하여 그에 맞는 근태 보고서를 작성하는 것입니다. 따라서, 이 장에서 설정하는 근태 기능 키의 이벤트는 실제 **BioAdmin**의 보고서나 로그확인 시에는 나타나지 않습니다.

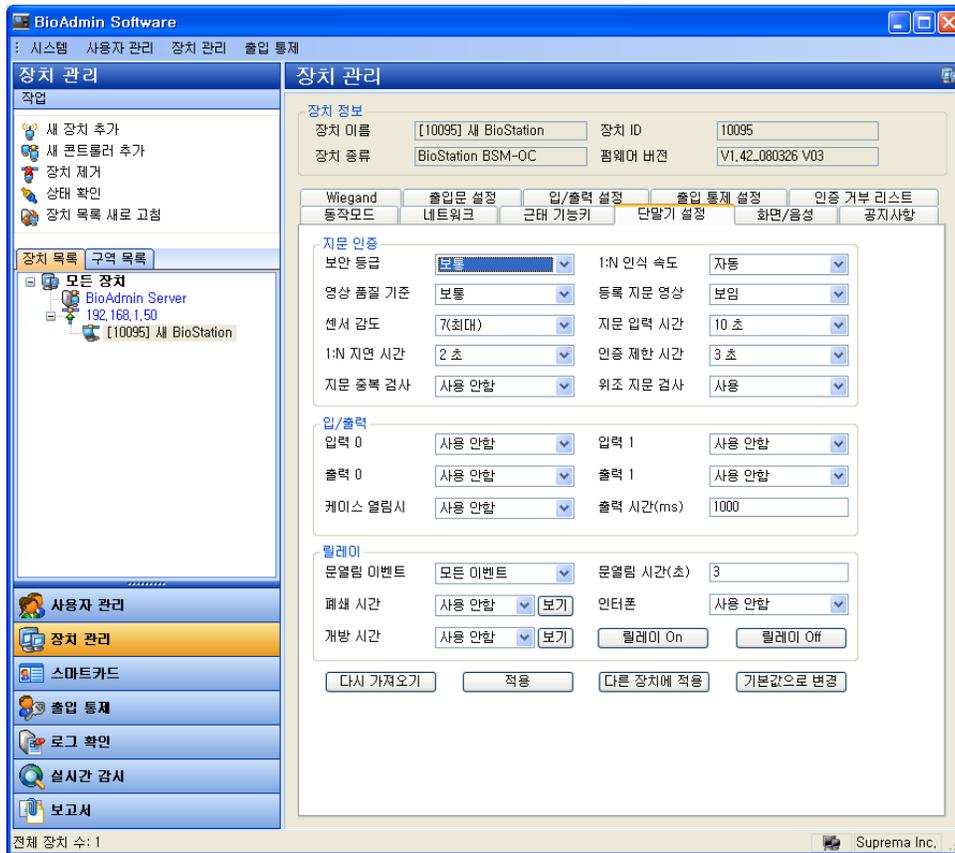


장치에서의 16개 키의 설정을 하며, 근태기능 키에서 16개 키 중에서 하나를 선택하여 BioStation LCD 창에 표시될 기능키 이벤트의 메시지와, 이 기능키의 사용여부 체크, 마지막으로 릴레이 사용여부 체크를 합니다.

- 설정할 기능키를 선택합니다.
- 기능키 이벤트 난에 이벤트 명을 직접 입력합니다.
- 선택된 기능키의 사용유무를 위해 이 기능키 사용 체크를 결정합니다.
- 선택된 기능키의 릴레이 사용유무를 위해 릴레이 사용하기의 체크를 결정합니다. 릴레이는 보통 출입문의 락 제어장치와 연결되어 문을 개폐하는데 사용됩니다.
- 동작모드 탭에서 근태모드를 고정으로 선택한 경우, 근태 기능키 옆에 고정을 할 것인지는 묻는 체크박스가 활성화 되며, 특정 근태기능키에서 고정을 체크하는 경우 장치는 해당 근태기능 상태만 입력을 받습니다. 예를 들어 출 퇴근용 입력 장치를 각각 사용하는 경우, 적용할 수 있습니다.
- 동작모드 탭에서 근태모드를 자동변경으로 선택한 경우, 자동모드적용시간이 활성화 됩니다. 출입통제에서 미리 설정한 출입시간을 선택하여 각 기능키에 자동으로 근태를 적용할 수 있도록 설정할 수 있습니다.

5.5.5. 단말기 설정

BioStation의 각종 설정 값을 확인, 변경하는 화면입니다.



- 보안 등급

보안 등급은 **보통, 안전, 가장 안전** 중에 선택할 수 있습니다. 내부적으로 보안 등급은 FAR(타인 수락 율, False Acceptance Ratio)을 조정합니다. FAR과 FRR(본인 거부 율, False Rejection Ratio)은 서로 반비례 관계이기 때문에 보안등급을 높이면 보안성은 높아지지만 FRR이 증가하여 거부 율이 올라갈 수 있습니다. 초기 설정 값은 보통입니다.

- 영상 품질 기준

입력되는 지문의 영상 품질이 일정 수준 이상인지를 판별하는 기준을 결정합니다. 선택은 **낮음, 보통, 높음** 중에서 할 수 있습니다. 초기 설정 값은 보통입니다.

- 센서 감도

센서 감도는 손가락을 감지하는 센서의 감도를 정하게 됩니다. 높은 감도에서는 손가락 입력을 좀 더 쉽게 받아들여지게 됩니다. 반면, 감도를 낮추면 지문을 일정 영역 이상 입력을 해야 캡처가 되므로 입력 지문 영상이 보다 안정적이 됩니다. 광학식 모델의 경우에는 감도 설정 값을 낮게 함으로서 햇빛에 대한 감도를 완화시킬 수 있습니다. 기본 설정 값은 7(최대) 입니다.

- 1:N 인식 속도

수백 개 이상의 지문이 장치에 저장되어 있을 경우, 1:N 인식시간이 길어질 수 있습니다. 매칭 속도를 **빠름**이나 **가장 빠름**으로 설정하면 인증 성능이 다

소 떨어지는 대신 1:N 인식 시간을 단축시킬 수 있습니다. 기본 설정 값은 보통입니다.

- 등록 지문 영상
지문을 입력할 때 입력한 지문의 영상을 BioStation의 LCD화면에서 보임과 보이지 않음으로 선택할 수 있습니다. 기본 설정 값은 보임입니다.
- 지문 입력 시간
지문 입력 시 대기시간을 말합니다. 이 시간 내에 사용자가 지문을 입력하지 않으면 입력 실패로 판단합니다. 기본 설정 값은 10초입니다.
- 1:N 지연 시간
인증 후 다음 인증에 대한 입력을 받는 시간 간격을 말합니다. 기본 설정 값은 2초입니다.
- 인증 제한 시간
지문 입력 후, 인증 결과를 나타내기까지의 최대 시간을 지정할 수 있으며, 설정된 시간이 경과되면 인증 결과가 나오지 않더라도 지문 검색을 중단 합니다. 이 기능은 입력된 지문의 정보가 너무 적어 검색 시간이 길어질 때 일정 시간이 지나면 검색을 중단하여 전체 사용자의 원활한 사용을 유도하기 위해 사용됩니다.
- 지문 중복 검사
사용자 지문을 등록할 때 이미 등록되어 있는 지문이 있는지의 여부를 미리 검사합니다.
동일한 지문이 두 아이디로 등록되는 것을 방지하며, 간혹 일정 수준 이상의 유사한 지문이 있는 경우 등록이 되지 않을 수 있습니다.
- 위조 지문 검사
인증을 시도할 때 입력 받은 지문의 위조 지문 여부를 검사합니다. 위조 지문 일 경우 인증을 거부하도록 되며, 이 옵션을 사용하면 정상적인 지문도 인증을 거부할 가능성이 있기 때문에 인증률이 떨어지는 것 처럼 느껴질 수 있습니다.
- 입/출력 설정
BioStation은 외부 장치와 접속할 수 있는 각각 두 개씩의 프로그램 가능한 입력과 출력을 제공합니다. 입출력 메뉴에서는 입출력 포트를 설정합니다.

입/출력

입력 0	<input type="text" value="사용 안함"/>	입력 1	<input type="text" value="사용 안함"/>
출력 0	<input type="text" value="사용 안함"/>	출력 1	<input type="text" value="사용 안함"/>
케이스 열림시	<input type="text" value="사용 안함"/>	출력 시간(ms)	<input type="text" value="100"/>

- **입력 포트의 환경설정:** 입력 포트의 환경설정은 입력 0 과 입력 1의 두 개의 포트이며, 문 열림 버튼의 입력과 사용 안 함, Wiegand의 세 가지 중 선택 가능합니다. Wiegand의 경우 입력 0번과 입력 1번을 모두 Wiegand로 사용해야 설정이 가능합니다.
- **출력 포트 환경설정:** 출력 포트의 환경설정은 출력 0 과 출력 1의 두 개의 포트이며, 협박손가락, 케이스 열림, 인증성공, 인증실패, 사용 안 함,

Wiegand의 6가지 중 선택 가능합니다. 출력포트의 신호 출력시간을 msec 단위로 설정할 수 있습니다. 입력 포트와 마찬가지로 출력 포트의 Wiegand도 출력 0번과 출력 1번으로 모두 Wiegand로 사용해야 설정이 가능합니다.

- **케이스 열림 시:** BioStation의 케이스가 열릴 경우 보안을 위하여 시스템 잠금 모드로 들어갈지 여부를 선택합니다.
- **BioStation 릴레이 설정:** BioStation 내부의 릴레이 설정을 변경할 수 있습니다. 모든 이벤트, 선택된 근태 이벤트, 인증성공, 근태 이벤트, 사용 안함 의 5가지 값 중에 선택 가능합니다. 선택된 이벤트의 발생 시 문 열림 시간을 설정 하실 수 있습니다.
- **개방시간/폐쇄 시간:** 문 개방 시간 및 폐쇄 시간을 요일 별 / 휴일 군에 따라 별도로 설정하실 수 있습니다. 출입통제 메뉴의 출입시간 설정에서 미리 설정되어 있어야 합니다.
- **문 열림 시간(초):** 설정된 이벤트에 따라 릴레이가 작동되는 시간을 의미 합니다. 일단 출입문이 해제되면, 지정된 문 열림 시간이 지난 후에 출입 문은 다시 잠길 수 있습니다.

Note: 전체적으로 시스템의 문 열림 시간은 도어 락 문 열림 시간과 장치의 문 열림 시간이 합쳐서 계산됩니다.

- **인터폰:** BioStation과 인터폰을 연결하는 경우에 이 옵션을 **활성**으로 선택 해주시고, 이외의 경우에는 **비활성**으로 선택합니다.
- **릴레이 On / 릴레이 Off:** BioStation 의 릴레이를 BioAdmin 에서 제어하여 원격에서 문을 열 수 있습니다.

5.5.6. 화면 / 음성

BioStation의 배경화면, 효과음, 및 기타 화면 / 음성 설정을 위한 메뉴입니다. 원하는 배경화면, 공지사항, 로고 이미지 등을 설정할 수 있으며, 효과음 또한 사용자의 취향에 맞도록 수정이 가능합니다.



- 배경화면 변경

이 메뉴에서는 BioStation의 배경화면에 대한 이미지를 변경할 수 있습니다. BioStation의 배경화면은 로고 이미지, 공지사항 배경, 슬라이드 쇼 3가지 중에서 선택할 수 있습니다. 배경화면에 올릴 수 있는 그림 파일의 포맷은 JPG, GIF, BMP, PNG 등으로 다양하나 크기는 320*240 픽셀로 고정되어 있습니다. 만약, 업로드 하고자 하는 이미지 파일의 크기가 다를 경우 그래픽 툴 등을 이용하여 그림의 크기를 맞춰주셔야 합니다.

배경화면에서 로고이미지와 공지사항의 배경화면은 이미지 파일을 하나 선택하여 올릴 수 있으며, 슬라이드 쇼는 최대 16장까지의 이미지 파일을 업로드 하면 슬라이드 쇼 형태로 일정한 주기로 이미지를 차례로 바꿔가며 보여줍니다.

- 효과음 변경

이 메뉴에서는 장치의 효과음을 변경하거나 현재의 효과음을 확인 하실 수 있습니다. 장치의 효과음은 장치의 전원이 투입 됐을 때의 시작 음, 버튼을 누를 때 버튼 음, 지문인증이 성공했을 때 인증 성공 음, ESC버튼을 누를 때 경고 음, 지문인증이 실패했을 때 인증 실패 음, 지문센서에 손가락을 올릴 때 지문 인식 음 이렇게 총 6개의 효과음으로 구성되어 있습니다.

Note: 사운드 파일의 크기가 512KB를 넘지 않아야 하며, 파일 형식에 따라 효과음 변경이 안될 수도 있습니다.

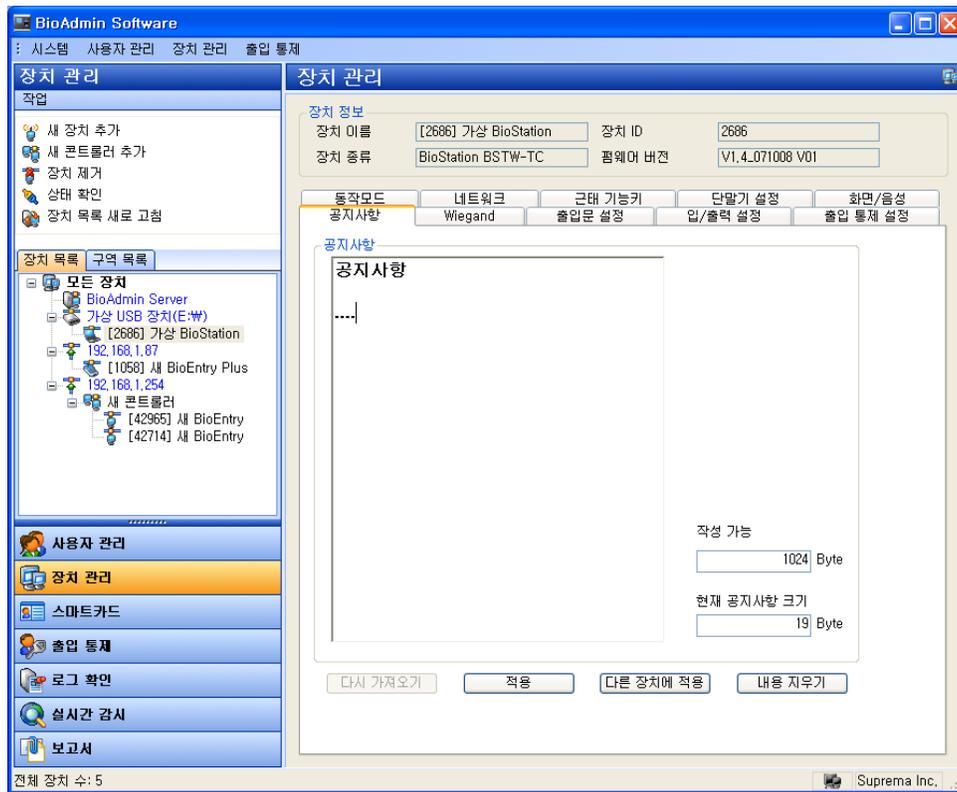
- 화면/음성 설정

- **언어:** BioStation의 LCD 창에서의 메뉴 및 각종 메시지에 사용되는 언어를 선택합니다. 언어는 **한글, 영어, 사용자정의** 중 선택 가능합니다.
- **하단정보:** BioStation의 배경화면의 아래 부분에 표시되는 내용을 설정하는 것으로 **공지사항, 시간, 사용 안 함** 중 선택 가능합니다. 공지사항의 경우 내용이 화면 오른쪽에서 왼쪽으로 스크롤 되어 지나갑니다. 기본 설정 값은 **시간**입니다.
- **메뉴 타임아웃:** 특정 메뉴에서 일정시간 동안 입력이 없으면 초기화면으로 돌아갑니다. **무제한, 10초, 20초, 30초** 중에서 선택 가능하며 기본 설정 값은 **20초**입니다.
- **개인인증화면 :** 사용자 등록 시에 설정한 개인인증 화면을 사용할 것인지를 결정합니다. 개인인증화면은 인증시 BioStation 의 LCD 창에 저장된 사진과 개인 메시지를 출력할 수 있는 기능입니다.
- **구성 파일:** **영어, 한국어, 사용자정의, 변경 안 함** 네 가지 중에 선택 가능합니다. 변경하고자 하는 언어를 선택하고 찾아보기를 클릭하여 해당 구성 파일(*.rc)을 선택합니다. 구성 파일을 바꾼 후에는 BioStation을 재 시작하여야 적용되며, 언어 선택 메뉴에서 해당 언어를 선택해야 볼 수 있습니다.
- **배경화면:** BioStation LCD 창의 배경화면으로 **로고이미지, 공지사항, 슬라이드 쇼** 중 선택 가능합니다.
- **음량:** BioStation의 스피커 음량을 조절할 수 있습니다. 음량은 **0-100%**까지 있으며, 일상적으로 사용하실 때에는 **20-50%** 정도 설정하고 사용하시는 게 좋습니다. 기본 설정 값은 **20%**입니다.
- **메시지 타임아웃:** BioStation에서 인증 시 인증 성공 및 인증 실패 메시지를 보여주는 시간을 조절할 수 있습니다. 기본 설정 값은 **2초**입니다.

5.5.7. 공지사항

회사의 공지사항 등이 있을 때 BioStation의 LCD 화면에 출력할 수 있습니다. 공지사항은 최대 **1,024 Byte**까지 입력이 가능하며 언어에 따라 글자수는 달라집니다.

공지사항 작성 후 적용 버튼을 눌러서 장치에 전송한 후, 화면/음성 메뉴에서 배경화면을 공지사항으로 선택하고 적용하여야 BioStation의 LCD 창에서 공지사항을 확인할 수 있습니다.



5.5.8. Wiegand 설정

Wiegand 탭은 장치의 Wiegand 출력/입력 포맷을 관리하기 위해 사용됩니다. 이 메뉴를 선택하면 Wiegand 설정 페이지가 주 윈도우에 갱신됩니다.



- Wiegand 포맷

Wiegand 설정 마법사를 이용하여 새로운 Wiegand 포맷을 설정할 수 있습니다. 포맷 변경 버튼을 누르면 Wiegand 설정 마법사가 나타납니다.

첫 번째 페이지에서 지원되는 3개의 포맷 중 하나를 선택해야 합니다.



- 26 비트 표준 Wiegand 포맷

26 bit standard 형식은 가장 광범위하게 쓰이며 8비트 FC 코드와 16비트 ID로 구성됩니다. 26 bit standard 형식에서 비트 정의와 패리티 비트는 변경할 수 없습니다.

- 패스 스루 Wiegand 포맷

패스 스루 포맷은 ID 필드의 형식을 알고 있을 때만 사용됩니다. Wiegand 입력 문자열이 감지되면, 장치는 ID 비트들을 찾아내고 그 ID로 인증을 시작합니다. 인증이 성공하면 장치는 Wiegand 입력 문자열을 바꾸지 않고 출력합니다. 패리티

체크와 고급 옵션들은 이 형식에서는 무시됩니다. 정의에 따르면 패스 스루 포맷은 사용 모드가 1:1인 경우에만 유용하다고 합니다. 사용 모드가 1:N일 때는 ID 필드 이외에 비트 오더가 0으로 설정되어야 합니다.

가령 32비트 Pass Through format이 다음과 같다고 가정합니다.:

XIIIIIIII IIIIIIX XXXIIIIII IIIIIIX

(가장 왼쪽 비트가 0번째 비트, BIT0) I: Id field, X: Unknown field

이 형식을 다음과 같은 순서로 설정할 수 있습니다.



Total Bits 필드에 32를 입력합니다.

정의에 따라 ID 비트를 선택합니다.

Next 버튼을 누릅니다. 패스 스루 모드에서는 패리티 비트를 특정할 수 없습니다.

▪ 사용자 설정 Wiegand 포맷

사용자가 Wiegand 형식에 대한 모든 정보를 갖고 있다면, 맞춤 포맷을 정의할 수 있습니다. Wiegand 입력 문자열이 감지되면, 장치는 우선 패리티 비트를 확인합니다. 모든 패리티 비트가 정확하면 장치는 ID 비트를 추출하고 그 ID로 인증을 시작합니다. 사용자는 또한 각 필드를 대체 값으로 설정할 수 있고 Fail ID와 같은 고급 옵션을 설정할 수 있습니다. 인증에 성공하면 장치는 Wiegand 문자열을 출력합니다. 출력 문자열은 대체 값과 고급 옵션에 따라 입력 문자열과 다를 수 있습니다.

가령, 44비트 맞춤 포맷이 다음과 같이 구성되었다고 가정합니다:

EAAAAAAAA IIIIIIIII IIIIIIIII BBBBBI IIIIIII IIII

(가장 왼쪽 비트가 0번째 비트, BIT0)

E: Even parity for BIT1 ~ BIT22

O: Odd parity for BIT23 ~ BIT42

I: ID bits(Field1 and Field 3), A: Field 0, B: Field 2

이 형식을 다음과 같은 순서로 설정할 수 있습니다.



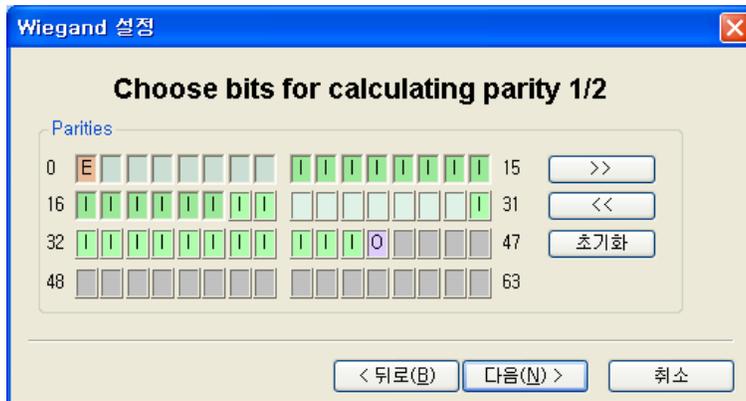
Total Bits 필드에 44를 입력합니다..

Even Parity를 선택합니다.

even parity bit를 누릅니다. 이 예제에서는 BIT0을 말합니다.

정의에 따라 **Odd Parity**와 **User ID**에 대해서 (2)와 (3)을 반복합니다.

Next 버튼을 누릅니다.



첫 번째 패리티 비트를 계산하는데 쓰이는 비트들을 누릅니다. 이 예제에서는 BIT1 ~ BIT22 입니다.

>> 버튼을 누릅니다.

두 번째 패리티 비트를 계산하는데 쓰이는 비트들을 누릅니다. 이 예제에서는 BIT23~ BIT42 입니다.

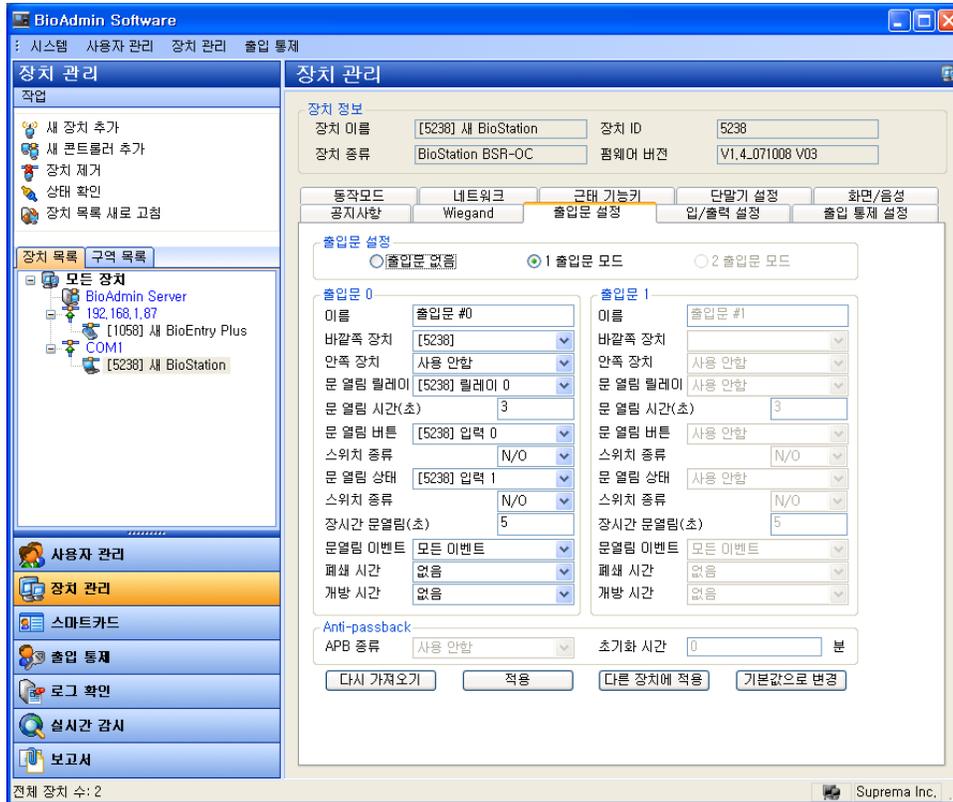
Next 버튼을 누릅니다.

- 대체 값

26 비트 표준에서 다른 FC code를 특정할 수 있습니다. 맞춤 포맷에서는 non-ID 필드에서 대체 값을 특정할 수 있습니다. 대체 값이 설정되면 장치는 출력을 보내기 전에 해당 필드들을 이 대체 값으로 바꿉니다.



5.5.9. 출입문 설정



- 각 출입문을 제어하는 장치에 대해 입출력을 설정합니다.
- 바깥쪽 장치, 안쪽장치 - 1개의 출입문에 설치되어 동작하게 되는 2개의 장치를 위치에 따라 설정하여야 합니다.
- 문 열림 릴레이 - 연결된 장치들 중, 어떤 장치를 이용하여 출입문을 제어할지에 대한 출력 장치를 설정하거나 사용안함을 선택할 수 있습니다.
- 문 열림 시간(초) - 문 열림 릴레이에서 선택한 출력 단자가 동작하는 시간을 입력합니다.
- 문 열림 버튼 - 출입문을 여는데 버튼용 입력 단자를 사용할 것인지에 따라

사용을 원하면 원하는 장치의 입력을 선택합니다. 스위치의 종류는 입력 되는 신호에 따라 스위치가 평소에 오픈 상태로 유지할 경우엔 N/O 를, 평소에 닫힌 상태로 유지될 경우엔 N/C 를 선택합니다.

- 문 열림 상태 - 출입문의 상태를 파악하는데 사용할 센서를 사용할 것인지에 따라, 사용을 원하면 원하는 장치의 입력을 선택합니다.. 스위치의 종류는 입력 되는 신호에 따라 스위치가 평소에 오픈 상태로 유지할 경우엔 N/O 를, 평소에 닫힌 상태로 유지될 경우엔 N/C 를 선택합니다.
- 장시간 문열림(초) - 문이 오래 열려 있는 것을 판단하는 시간을 정합니다.
- 폐쇄 시간 - 출입 통제 항목에서 설정한 출입 시간에 연동되는 항목으로 항상 잠겨 있는 시간을 설정할 수 있습니다.
- 개방 시간 - 출입 통제 항목에서 설정한 출입 시간에 연동되는 항목으로 항상 열려 있는 시간을 설정할 수 있습니다.
- Anti-passback: 바깥쪽 장치와 안쪽 장치간의 Anti-pass back을 적용할지 여부를 설정할 수 있습니다.

Soft : 인증시 APB 위반이더라도 기록만 남기고 출입을 허용합니다.

Hard : 인증시 APB 위반일 경우 기록과 함께 출입도 제한합니다.

초기화시간 : APB 로 인해 출입이 통제 되더라도 지정된 시간이 지나면 출입을 허용하는 설정입니다.

5.5.10. 입/출력 설정



- 입/출력 설정을 통해 각 입력 신호에 대한 작동과 출력의 설정이 가능합니다.

● 입력

입력

장치 종류	[2686]	포트	입력 0
기능	사용 안함	스위치 종류	N/O
동작 시간	항상 적용	입력 시간(ms)	254
Tamper	사용 안함		

1. 장치 종류 - 현재 설정 가능한 장치가 표시되며, 선택할 수 있습니다.
2. 포트 - 선택한 장치로 들어올 두 개의 입력 포트 중 하나를 선택합니다.
3. 기능 - 선택한 포트에 입력 신호가 오는 경우 동작할 기능을 선택합니다.
기본값은 사용안함으로 설정되어 있으며, 일반입력/비상문열림/모든경보해제/장치재시작/장치잠금 중에 하나를 선택할 수 있습니다..
4. 동작 시간 - **항상적용**/사용안함 또는 출입 통제에서 설정한 시간에 대해서만 해당 기능이 동작하도록 출입시간을 선택하여 설정이 가능합니다.
5. 입력 시간(ms) - 해당 시간 이상 입력되어야 동작하도록 합니다.
6. Tamper - Tamper의 기능을 선택하여 부여할 수 있습니다.

● 출력

출력

장치 종류	[2686]	포트	릴레이 0
-------	--------	----	-------

알람 동작 개시 이벤트

지연(ms)	0
켜짐(ms)	0
꺼짐(ms)	0
반복 횟수	0
우선 순위	0

알람 멈출 이벤트

우선 순위	0
-------	---

추가 편집 삭제 모두 삭제

추가 편집 삭제 모두 삭제

1. 장치 종류 - 현재 설정 가능한 장치가 표시되며, 선택할 수 있습니다.
2. 포트 - 선택한 장치에서 설정 가능한 출력 단자를 선택합니다.
3. 알람 동작 개시 이벤트 - 나열된 이벤트가 발생을 하면 현재 선택된 장치의 해당 포트에서 출력이 발생하도록 설정할 수 있습니다.
 - ◆ 이벤트 추가

이벤트 추가 [X]

[2686] 릴레이 0

이벤트

이벤트 인증 성공

장치 모든 장치 무선 순위 1

신호 파형

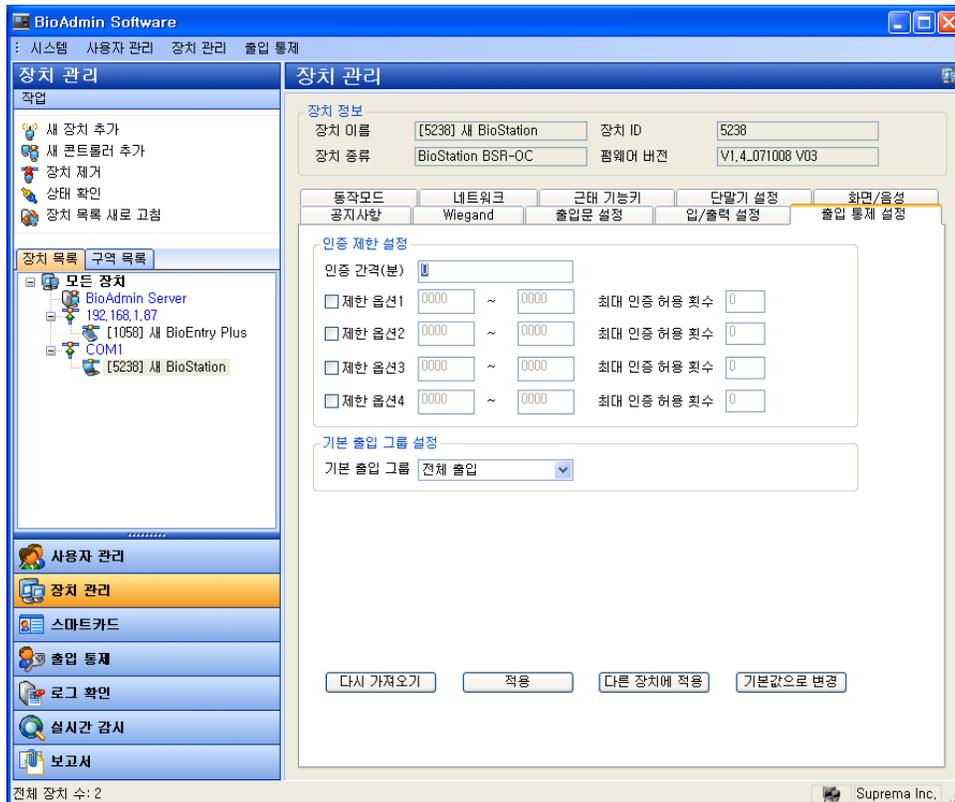
지연(ms) 0 반복 횟수 1

켜짐(ms) 0 꺼짐(ms) 0

확인 취소

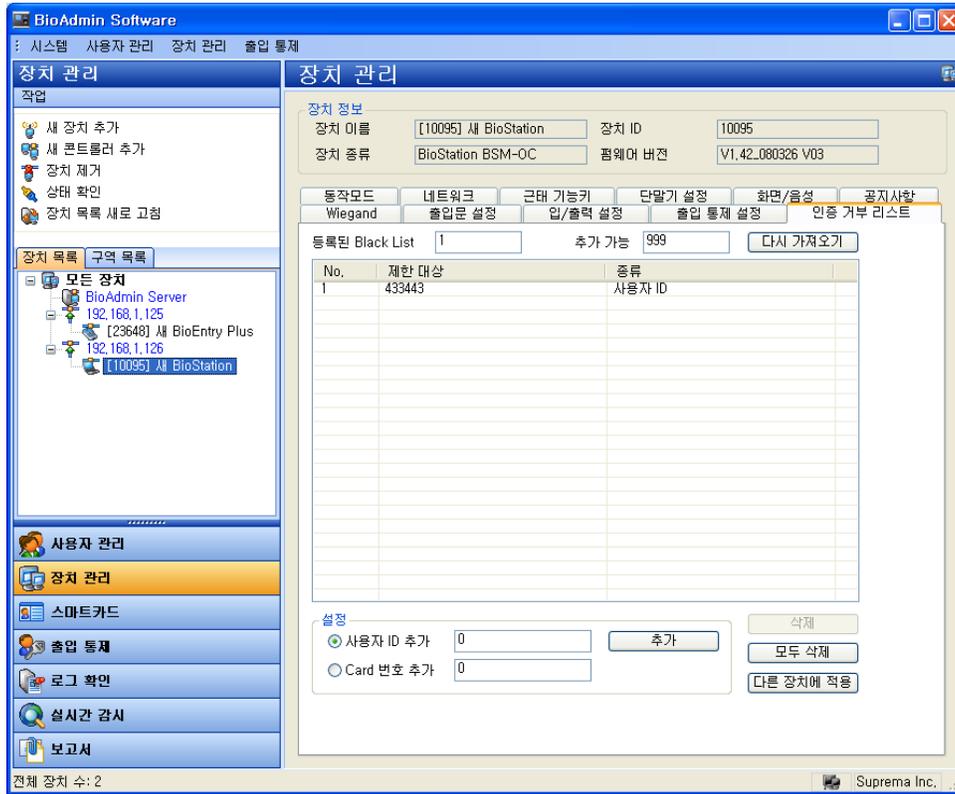
- 이벤트: 선택된 이벤트가 발생을 하면 앞에서 선택한 장치의 포트 출력이 나가도록 설정됩니다.
 - 장치: 이벤트가 발생할 장치를 선택합니다.
 - 우선 순위: 해당 기능에 대해서 우선순위를 부여하여 낮은 우선 순위를 가진 기능이 보다 중요한 우선 순위의 이벤트를 가리거나 끄는 것을 방지합니다.
 - 신호 파형
 - 지연: 출력이 나가도록 하기 전의 지연 시간
 - 켜짐: 출력이 발생할 시간
 - 꺼짐: 출력이 발생하지 않을 시간
 - 반복 횟수: 켜짐~꺼짐의 구간을 반복할 횟수
 - BioEntry의 입/출력 부분 참고
4. 알람 멈춤 이벤트 - 나열된 이벤트가 발생을 하면 선택된 장치의 해당 포트에 설정된 우선순위와 같거나 낮은 출력을 해제할 수 있습니다.

5.5.11. 출입 통제 설정



- 출입 통제 설정에서는 반복 인증을 제한하거나, 특정 시간 동안 반복 출입을 막는 등의 설정이 가능합니다. 이 기능은 특정 시간 사이에 한번만 인증 되도록 하는 식수 관리 등에 활용이 가능합니다.
- 인증 제한 설정
 1. 인증 간격 - 입력된 시간(분) 이내에 재 인증이 이루어지면 인증을 제한합니다.
 2. 제한옵션 1~4 - 각각의 옵션별 시작시간~끝시간을 입력하고 해당 시간에 대해서 최대 출입 허용 횟수를 적어주면, 지정된 시간 동안에는 지정된 횟수만큼만 인증을 허용합니다.
- 기본 출입 그룹 설정
아무런 출입 그룹 정보가 없는 사용자의 경우 여기서 설정된 출입 그룹이 적용 되도록 기본 내용을 설정할 수 있다. 기본값으로 전체출입이 설정 되어 있으며, 출입그룹이 정해지지 않은 사용자에게 대해 모두 출입을 허용 합니다.

5.5.12. 인증 거부 리스트



인증을 거부할 리스트(Black list)를 따로 관리할 수 있습니다. 이 리스트에 등록된 카드번호나 사용자 ID에 대한 인증 요청이 들어오면 단말기는 인증을 거부하고 실패 로그를 남기게 됩니다. 모두 1000개의 리스트를 등록할 수 있습니다.

- 등록된 **Black List**: 현재 등록된 list의 수입니다.
- 추가 가능: 추가로 등록 가능한 list 수입니다.
- 다시 가져오기: 리스트를 장치로부터 다시 읽어옵니다.
- 추가 : 사용자 ID 혹은 카드 번호를 체크하여 어떤 항목을 차단할 것인지 결정한 뒤, 번호를 입력하고 '추가'를 클릭합니다. 이미 등록되어 있거나, 1000개를 초과하는 항목을 추가하려고 할 경우에는 등록할 수 없습니다.
- 삭제 : 리스트에서 삭제하려는 항목을 클릭한 뒤에 '삭제'버튼을 클릭합니다.
- 모두 삭제 : 현재 등록된 모든 Black list가 삭제됩니다.
- 다른 장치에 적용 : 현재 Black list를 다른 장치에 적용합니다.

5.6. USB 가상 BioStation 장치 관리

USB 가상 BioStation은 BioStation의 장치관리와 동일한 방법으로 설정할 수 있습니다. 단, 아래의 기능들은 별도의 설정이 필요합니다.

- 시간 설정: USB 가상 BioStation이 아닌 BioStation에 직접 설정해야만 합니다.
- 모든 장치 잠금 / 모든 장치 잠금 해제: USB 가상 BioStation이 아닌 BioStation에 직접 설정해야만 합니다.
- 펌웨어 업그레이드: BioStation에 적용코자 하는 펌웨어 파일을 USB Memory에

저장한 후 BioStation에 연결하여 펌웨어를 업그레이드 합니다.

각종 설정 값이 저장된 USB 가상 BioStation을 BioStation에 연결한 후 아래와 같은 BioStation상의 메뉴를 이용하여 사용이 가능합니다. 구체적인 사용방법에 대해서는 BioStation 사용자 설명서를 참조하시기 바랍니다.

- 동기화: 현재 USB 가상 BioStation에 저장된 상태로 BioStation의 설정 및 사용자 데이터를 수정합니다.
- 가상 단말기 내보내기: 현재 USB에 저장된 내용을 버리고 다시 가상 BioStation을 생성합니다. 따라서 현재 BioStation의 상태가 USB에 저장됩니다.
- 가상 단말기 불러오기: 동일한 설정을 여러 대의 BioStation에 전파하는 경우에 사용됩니다. 현재 USB메모리에 저장된 USB 가상 BioStation들의 설정 중 한가지를 선택하여 적용할 수 있다. 이때는 사용자 데이터도 모두 선택한 USB 가상 BioStation에 저장된 내용으로 변경됩니다.
- 펌웨어 업그레이드: 가상 BioStation으로 사용중인 USB 메모리에 BioStation의 펌웨어 파일을 복사하여 BioStation의 펌웨어 업그레이드가 가능합니다.
- 메모리 초기화: 연결된 USB 메모리의 모든 BioStation을 삭제합니다.
- 새로 고침: USB 메모리의 상태를 다시 확인하여 사용 가능한 것인지 판단하고, 메뉴를 활성화 시킵니다.

5.7. BioEntry Plus 장치 관리

5.7.1. 장치 정보

- 선택한 BioEntry Plus의 장치 이름, 장치 종류 및 단말기 ID와 펌웨어 버전을 확인할 수 있습니다. 단말기 ID번호와 펌웨어 버전 등은 설치 후 기술 지원 등에서 제품을 확인하기 위해 필요한 정보입니다.

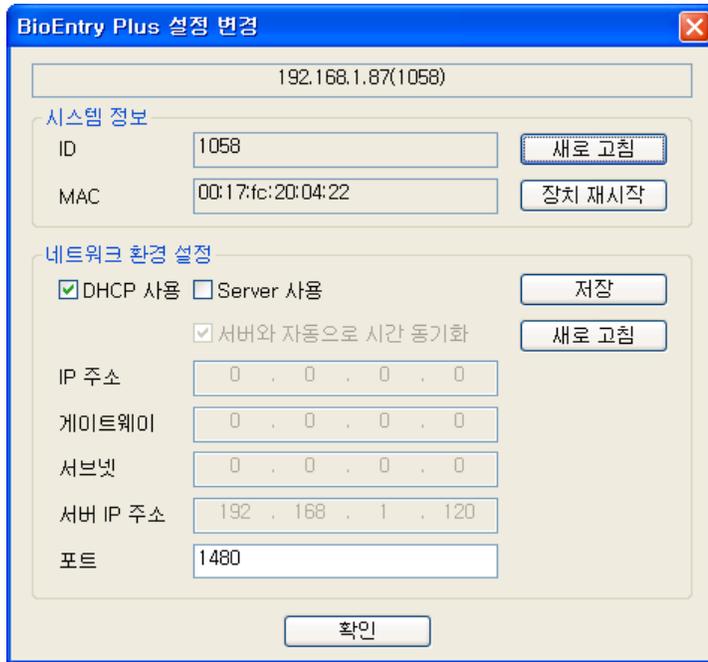


5.7.2. UDP로 환경 설정하기

- BioEntry Plus 아이콘이나 이름 위에서 마우스 오른쪽 버튼 클릭으로 '설정 변경' 메뉴를 선택할 수 있습니다.

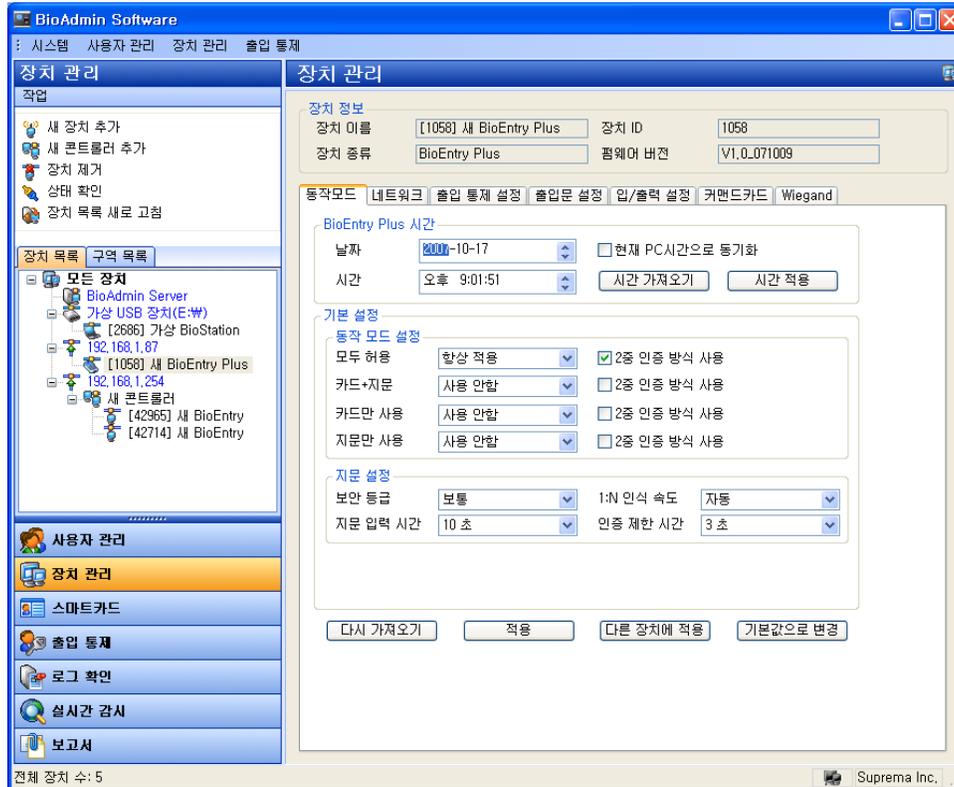


- 시스템 정보 – 현재 BioEntry Plus에 부여된 ID 및 MAC 어드레스를 확인 할 수 있으며, 새로그침 버튼 클릭으로 정보를 다시 읽어오도록 할 수 있습니다.
- 네트워크 환경 설정
 1. DHCP 사용
 - 해당 BioEntry Plus가 DHCP를 지원하는 네트워크에 설치 되어 자동으로 IP를 부여 받도록 설정하는 경우 체크합니다. DHCP를 지원하지더라도 체크를 지우고 지정된 네트워크 정보를 입력할 수 있습니다.
 2. Server 사용
 - BioEntry Plus가 BioAdmin Server에 접속하여 동작하도록 설정할 경우 체크합니다.
 - 서버와 자동으로 시간 동기화 하는 경우 체크합니다.
 3. 포트
 - 서버 포트와 BioEntry Plus의 포트를 같은 값을 사용합니다. 기본적으로 BioEntry Plus 는 1471 포트를 사용하지만, BioAdmin Server를 사용하는 경우 서버 설정에서 정한 포트 번호를 입력해야 하며, 모르는 경우 Sever Configuration 을 다시 실행 시켜 확인할 수 있습니다. 기본값으로 1480을 사용하므로 서버사용에 체크하는 경우 대부분 1480으로 포트를 입력해야 합니다.



5.7.3. 동작 모드

- 시간 설정



처음에 보이는 날짜와 시간이 BioEntry Plus 에서 읽어온 값입니다. 시간가져 오기 버튼을 클릭하면 BioEntry Plus로 부터 날짜와 시간을 다시 읽어옵니다.

BioEntry Plus의 시간 변경 방법은 직접 입력 방법과 현재 PC 시간으로 동기화의 두 가지 방법으로 나뉩니다.

- 직접 입력: 날짜와 시간 창에서 숫자를 직접 입력하거나 숫자에 커서를 두고 위아래 화살표를 클릭하여 입력합니다. 입력 후 **시간적용** 버튼을 누르면 입력된 날짜와 시간이 선택된 BioEntry Plus로 전송됩니다.
- PC 시간으로 동기화: 현재 **PC시간으로 동기화**를 체크하고, 시간적용 버튼을 누르시면 선택된 BioEntry Plus 의 시간이 현재 PC의 시간으로 맞춰집니다.

BioEntry Plus 시간

날짜	<input type="text" value="2007-10-17"/>	<input type="checkbox"/> 현재 PC시간으로 동기화
시간	<input type="text" value="오후 9:01:06"/>	<input type="button" value="시간 가져오기"/> <input type="button" value="시간 적용"/>

● 동작 모드 설정

동작모드설정은 각각의 인증 방식을 언제 사용할 것인가에 대한 설정을 할 수 있습니다. 항상적용과 사용안함 및 미리 설정된 출입통제 메뉴의 출입시간을 선택할 수 있습니다. 두 가지의 다른 인증 방식이 동일 시간에 겹치지 않아야 합니다.

- 2중 인증 방식 : 15초 이내에 각각 다른 사용자의 인증이 이루어져야 출입문이 동작하는 기능으로 보안성을 강화할 때 적용할 수 있습니다.

동작 모드 설정

모두 허용	<input type="text" value="항상 적용"/>	<input checked="" type="checkbox"/> 2중 인증 방식 사용
카드+지문	<input type="text" value="사용 안함"/>	<input type="checkbox"/> 2중 인증 방식 사용
카드만 사용	<input type="text" value="사용 안함"/>	<input type="checkbox"/> 2중 인증 방식 사용
지문만 사용	<input type="text" value="사용 안함"/>	<input type="checkbox"/> 2중 인증 방식 사용

● 지문 설정

지문 설정

보안 등급	<input type="text" value="보통"/>	1:N 인식 속도	<input type="text" value="자동"/>
지문 입력 시간	<input type="text" value="10 초"/>	인증 제한 시간	<input type="text" value="3 초"/>

1. 보안 등급

보안 등급은 보통, 안전, 가장 안전 중에 선택할 수 있습니다. 내부적으로 보안 등급은 FAR(타인 수락 율, False Acceptance Ratio)을 조정합니다. FAR과 FRR(본인 거부 율, False Rejection Ratio)은 서로 반비례 관계이기 때문에 보안등급을 높이면 보안성은 높아지지만 FRR이 증가하여 거부 율이 올라갈 수 있습니다. 초기 설정 값은 보통입니다.

2. 1:N 인식 속도

수백 개 이상의 지문이 장치에 저장되어 있을 경우, 1:N 인식시간이 길어질 수 있습니다. 매칭 속도를 빠름이나 가장 빠름으로 설정하면 인증 성능이 다소 떨어지는 대신 1:N 인식 시간을 단축시킬 수 있습니다. 기본 설정 값은 보

통입니다.

3. 지문 입력 시간

지문 입력 시 대기시간을 말합니다. 이 시간 내에 사용자가 지문을 입력하지 않으면 입력 실패로 판단합니다. 기본 설정 값은 **10초**입니다.

4. 인증 제한 시간

지문 입력 후, 인증 결과를 나타내기까지의 최대 시간을 지정할 수 있으며, 설정된 시간이 경과되면 인증 결과가 나오지 않더라도 지문 검색을 중단 합니다. 이 기능은 입력된 지문의 정보가 너무 적어 검색 시간이 길어질 때 일정 시간이 지나면 검색을 중단하여 전체 사용자의 원활한 사용을 유도하기 위해 사용 됩니다.

● 지문 옵션 정보

Template Option Informations

ISO Format

- ISO 템플릿 사용
ISO 표준 템플릿 사용 유무를 나타냅니다.

● Mifare Setting

현재 BioEntry Plus가 Mifare 를 지원하는 경우 이 항목이 활성화 되며 설정을 변경할 수 있습니다. 그 외 모델에 대해서는 사용할 수 없습니다.

Mifare Setting

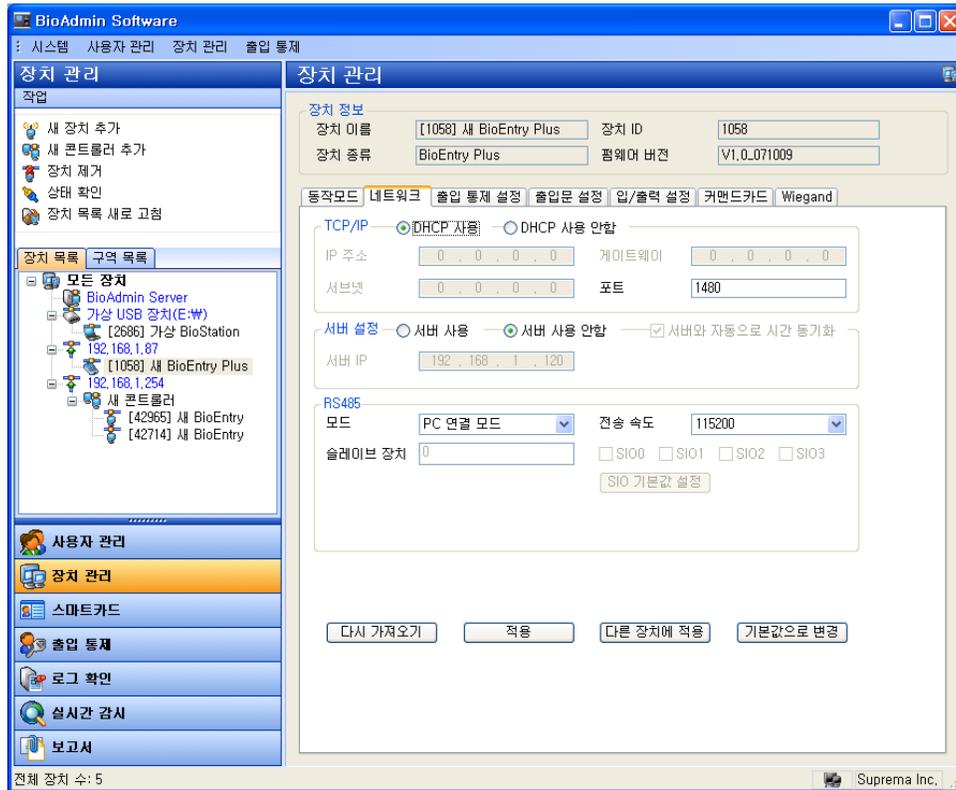
Disable Mifare Card

Use Template On Card

[View Card Layout](#)

- Mifare 사용 안 함
Mifare Card의 사용을 끄고 card입력을 받아들이지 않도록 설정할 수 있습니다.
- 템플릿 온 카드 사용
Mifare card에 사용자 정보를 저장하여 사용할 것인지, 아니면 RF-card와 같은 방식으로 Card ID만 사용할 것인지 설정할 수 있습니다.
- Mifare레이아웃보기
현재 BioEntry Plus에 설정된 Mifare Layout 정보를 확인할 수 있습니다. 이 정보는 6.5.7. Mifare 카드 레이아웃 설정 (BioStation / BioEntry Plus)절을 참고하여 수정할 수 있습니다.

5.7.4. 네트워크



● TCP/IP

1. TCP/IP 설정

- BioEntry Plus의 설정 값 중에서 IP주소를 자동으로 받을 것인지, 수동으로 설정할 것인지를 선택합니다. 네트워크 환경에 따라 DHCP를 지원하여 BioEntry Plus에 IP주소가 자동으로 부여될 경우 'DHCP 사용'을, 지정된 IP를 직접 설정할 경우에는 'DHCP 사용 안함'을 선택합니다.
- IP주소, 게이트웨이, 서브넷, 포트는 각각 알맞은 값으로 설정합니다.
- 포트는 기본값으로 1471을 사용하지만, 서버를 사용하는 경우에는 서버 포트로 설정하여야 합니다.



2. 서버 설정

- 해당 BioEntry Plus가 서버에 연결되어 있는지를 보여줍니다.
- 일반 TCP/IP로 연결된 BioEntry Plus를 서버에 연결시키고자 할 경우에는 서버 사용에 체크한 후 서버 IP 주소와 서버 포트를 설정하면 됩니다.
- 이처럼 서버에 연결하는 경우, 해당 BioEntry Plus는 원래 연결되어 TCP/IP 에서 연결이 즉시 해제되며, 목록에서 BioAdmin Server 아래로 다

시 연결되어 나타나게 됩니다. 다시 목록에 보여지기까지는 네트워크 환경에 따라 다소 시간이 걸릴 수 있습니다.

- 서버에 연결된 **BioEntry Plus**의 통신상태가 좋지 않을 때에는 장치목록에 있는 **BioAdmin Server** 서버에서 마우스 오른쪽 버튼을 클릭한 후 **서버 재접속**을 시도하십시오.

서버 설정 — 서버 사용 — 서버 사용 안함 — 서버와 자동으로 시간 동기화

서버 IP

3. RS485 설정

BioEntry Plus의 RS485 포트로 통신을 사용하는 경우에 대해 설정합니다.

RS485모드에서는 서로 연결된 장치가 호스트(Host)와 슬레이브(Slave) 역할을 나누어 하게 되며 해당 장치를 Host 로 할지 Slave 로 할지를 결정 합니다.

BioStation, BioEntry Plus 및 Secure I/O 로 구성되는 통합 시스템은 Host 장치 1대, Slave 장치 1대와 함께 4대의 Secure I/O 가 최대로 연결되며, Host 장치는 총 10개의 릴레이와 20개의 입력을 관리합니다.

- 시스템의 장치 구성에 따라 다음과 같이 설정 합니다.
- BioStation 을 출입문 바깥쪽에 설치하고 BioEntry Plus 를 안쪽에 설치하는 경우:

일반적으로 보안을 위해 안쪽에 설치된 장치에서 출입문 오픈 릴레이를 내 보내게 되므로 안쪽에 설치되는 BioEntry Plus 를 'Host'로 설정합니다. BioStation는 'Slave'로써 하위장치가 되며 RS485로 BioEntry Plus 에 연결합니다. 설정 방법으로는 BioEntry Plus의 장치관리 메뉴 내 네트워크 탭에서 'Host' 선택 후 하위장치인 BioStation의 ID를 입력하고, 'Slave' 장치가 되는 BioStation에서는 장치관리 메뉴의 네트워크 탭에서 'Slave' 로 지정해 두어야 합니다.

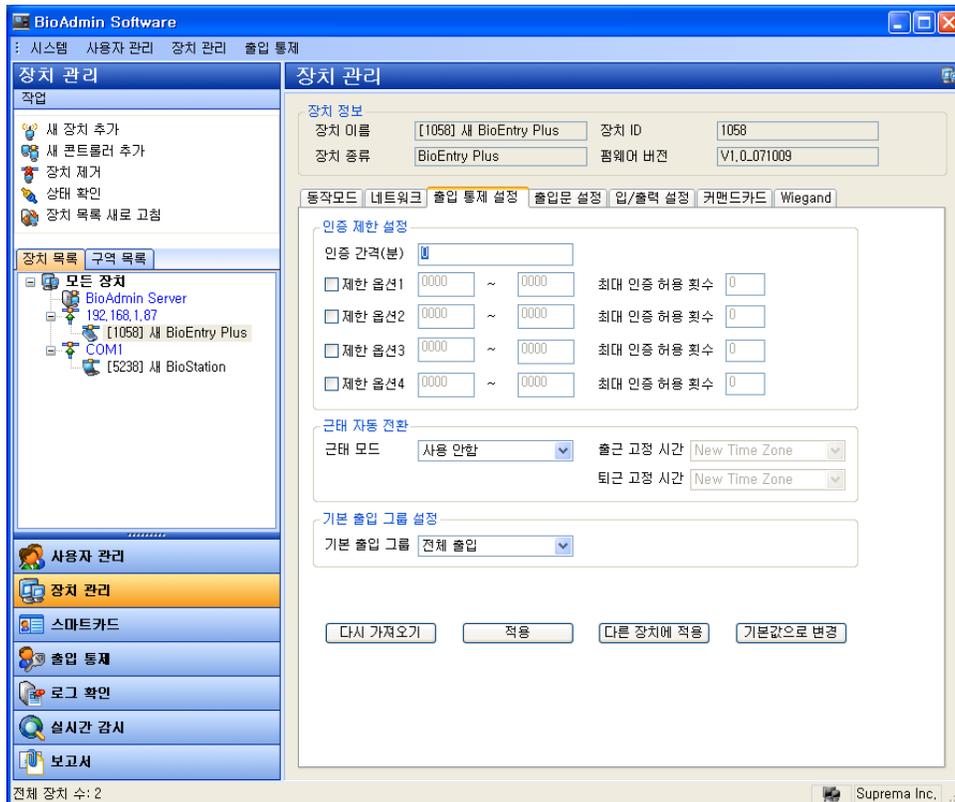
- BioEntry Plus를 출입문 바깥쪽에 설치하고 Secure I/O 를 설치하는 경우: BioEntry Plus가 'Host' 가 되어 Secure I/O 의 입출력을 제어하며, 인증에 성공하면 BioEntry Plus는 Secure I/O 를 통해 출입문을 열게 됩니다. 설정 방법으로는 BioEntry Plus를 'Host' 로 설정 후, 제어하고자 하는 SIO 를 Check 합니다. 총 4대까지 연결이 가능하며, Secure I/O 뒷면의 DIP스위치를 조정하여 부여된 번호를 선택합니다. Secure I/O 의 기본 입출력 설정을 통해 출입문이나 비상 경광등 등을 제어할 수 있습니다.
- Secure I/O 에 대한 자세한 설명은 Secure I/O 매뉴얼을 참조하시기 바랍니다.

RS485

모드 전송 속도

슬레이브 장치 SIO0 SIO1 SIO2 SIO3

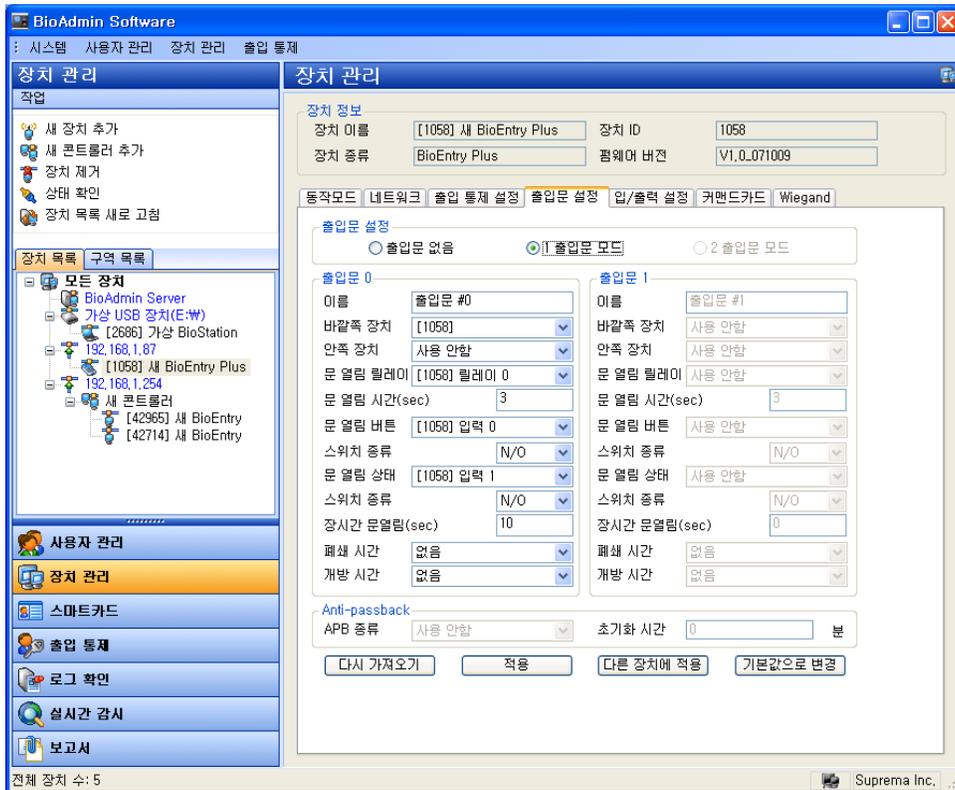
5.7.5. 출입 통제 설정



- 출입 통제 설정에서는 반복 인증을 제한하거나, 특정 시간 동안 반복 출입을 막는 등의 설정이 가능합니다. 이 기능은 특정 시간 사이에 한번만 인증 되도록 하는 식수 관리 등에 활용이 가능합니다.
- 인증 제한 설정
 1. 인증 간격 - 입력된 시간(분) 이내에 재 인증이 이루어지면 인증을 제한합니다.
 2. 제한옵션 1~4 - 각각의 옵션별 시작시간~끝시간을 입력하고 해당 시간에 대해서 최대 출입 허용 횟수를 적어주면, 지정된 시간 동안에는 지정된 횟수만큼만 인증을 허용합니다.
- 근태 자동 전환
 1. 선택된 BioEntry Plus를 어떤 근태모드로 사용할 것인지 설정 합니다.
 2. 근태 모드 : 사용 안함, 출근고정, 퇴근고정, 자동 설정 모드가 있습니다.
 - 자동 설정 : 지정된 시간에 따라 자동으로 출근과 퇴근 시간으로 변환 되도록 설정이 가능합니다. 출입통제에서 설정된 출입시간을 선택하여 지정된 시간에 인증이 이루어지면 출근 혹은 퇴근으로 자동으로 근태 모드가 변경됩니다.
 - 출근고정, 퇴근고정 : 특정 장치를 항상 선택된 근태모드로 적용되도록 하는 것으로 출근이나 퇴근 중 한가지 상태로 설정할 수 있습니다.
- 기본 출입 그룹 설정

아무런 출입 그룹 정보가 없는 사용자의 경우 여기서 설정된 출입 그룹이 적용 되도록 기본 내용을 설정할 수 있습니다.

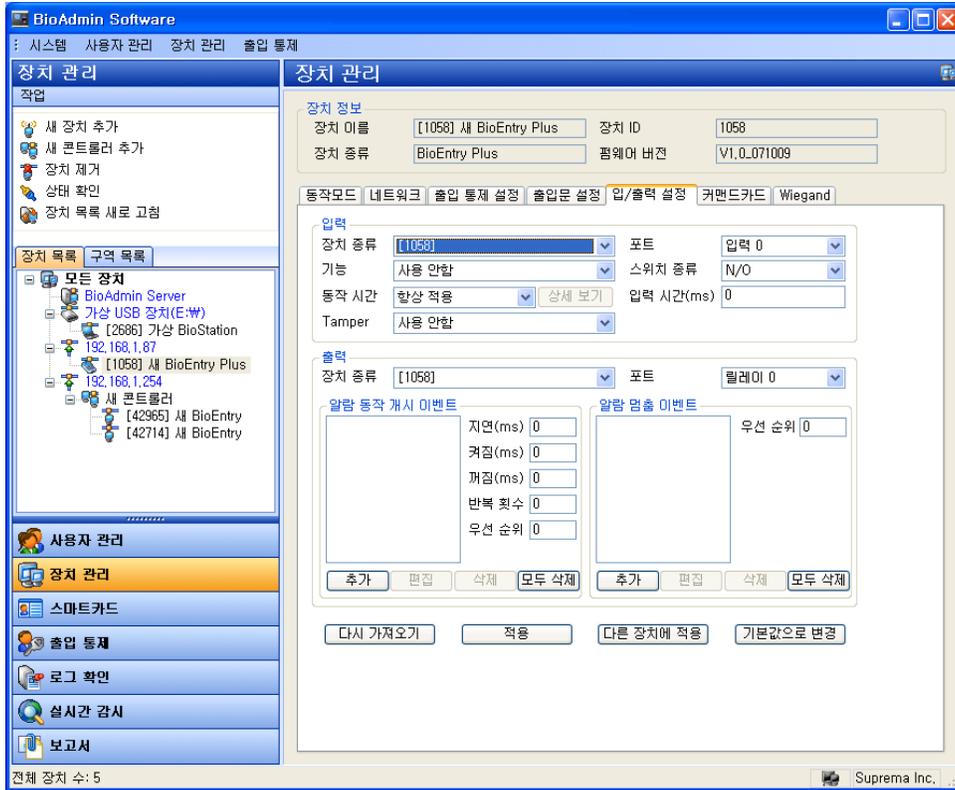
5.7.6. 출입문 설정



- 각 출입문을 제어하는 장치에 대해 입출력을 설정합니다.
- 바깥쪽 장치, 안쪽장치 - 1개의 출입문에 설치되어 동작하게 되는 2개의 장치를 위치에 따라 설정하여야 합니다.
- 문 열림 릴레이 - 연결된 장치들 중, 어떤 장치를 이용하여 출입문을 제어할지에 대한 출력 장치를 설정하거나 사용안함을 선택할 수 있습니다.
- 문 열림 시간(초) - 문 열림 릴레이에서 선택한 출력 단자가 동작하는 시간을 입력합니다.
- 문 열림 버튼 - 출입문을 여는데 버튼용 입력 단자를 사용할 것인지에 따라 사용을 원하면 원하는 장치의 입력을 선택합니다. 스위치의 종류는 입력 되는 신호에 따라 스위치가 평소에 오픈 상태로 유지할 경우엔 N/O 를, 평소에 닫힌 상태로 유지될 경우엔 N/C 를 선택합니다.
- 문 열림 상태 - 출입문의 상태를 파악하는데 사용할 센서를 사용할 것인지에 따라, 사용을 원하면 원하는 장치의 입력을 선택합니다.. 스위치의 종류는 입력 되는 신호에 따라 스위치가 평소에 오픈 상태로 유지할 경우엔 N/O 를, 평소에 닫힌 상태로 유지될 경우엔 N/C 를 선택합니다.
- 장시간 문열림(초) - 문이 오래 열려 있는 것을 판단하는 시간을 정합니다.
- 폐쇄 시간 - 출입 통제 항목에서 설정한 출입 시간에 연동되는 항목으로 항상 잠겨 있는 시간을 설정할 수 있습니다.
- 개방 시간 - 출입 통제 항목에서 설정한 출입 시간에 연동되는 항목으로 항상 열려 있는 시간을 설정할 수 있습니다.

- **Anti-passback**: 바깥쪽 장치와 안쪽 장치간의 **Anti-pass back**을 적용할지 여부를 설정할 수 있습니다.
Soft : 인증시 **APB** 위반이더라도 기록만 남기고 출입을 허용합니다.
Hard : 인증시 **APB** 위반일 경우 기록과 함께 출입도 제한합니다.
초기화시간 : **APB** 로 인해 출입이 통제 되더라도 지정된 시간이 지나면 출입을 허용하는 설정입니다.

5.7.7. 입/출력 설정



- 출입문 설정 이외에 입/출력 단자를 원하는 대로 설정이 가능합니다.
- 입력

입력

장치 종류	[1058]	포트	입력 0
기능	사용 안함	스위치 종류	N/O
동작 시간	합상 적용	입력 시간(ms)	0
Tamper	사용 안함		

1. 장치 종류 - 현재 설정 가능한 장치가 표시 되며, 선택할 수 있습니다.
2. 포트 - 선택한 장치에서 설정 가능한 입력 단자를 선택합니다.
3. 기능 - 입력으로 발생하도록 할 기능을 선택합니다.
4. 동작 시간 - 출입 통제에서 설정한 시간에 대해서만 해당 입력이 동작하도록 출입시간을 선택하여 설정이 가능합니다.

5. 입력 시간(ms) – 해당 시간이상 입력되어야 동작하도록 합니다.
 6. Tamper – Tamper의 기능을 선택하여 부여할 수 있습니다.
- 출력

출력

장치 종류 [1058] 포트 릴레이 0

알람 동작 개시 이벤트

지연(ms)

켜짐(ms)

꺼짐(ms)

반복 횟수

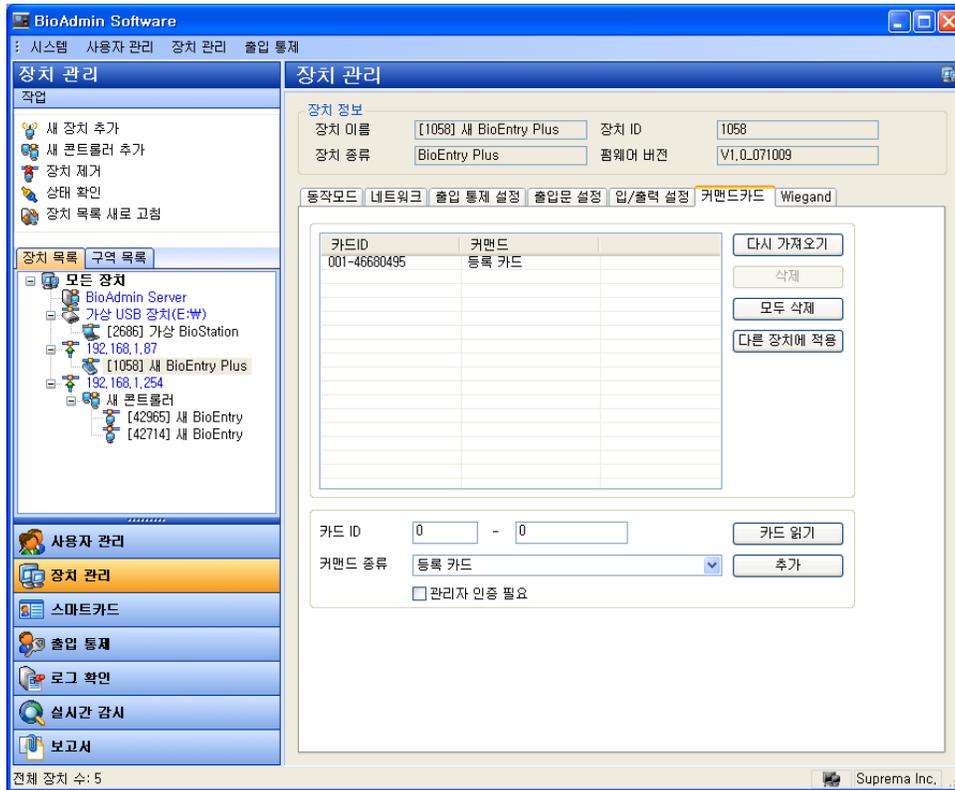
우선 순위

알람 멈춤 이벤트

우선 순위

1. 장치 종류 – 현재 설정 가능한 장치가 표시 되며, 선택할 수 있습니다.
2. 포트 – 선택한 장치에서 설정 가능한 출력 단자를 선택합니다.
3. 알람 동작 개시 이벤트 – 나열된 이벤트가 발생을 하면 현재 선택된 장치의 해당 포트에서 출력이 발생하도록 설정할 수 있습니다.
 - 이벤트 추가
 - 이벤트: 선택된 이벤트가 발생을 하면 앞에서 선택한 장치의 포트로 출력이 나가도록 설정합니다.
 - 장치: 이벤트가 발생할 장치를 선택합니다.
 - 우선 순위: 해당 기능에 대해서 우선순위를 부여하여 낮은 우선 순위를 가진 기능이 보다 중요한 우선 순위의 이벤트를 가리거나 끄는 것을 방지할 수 있습니다.
 - 신호 파형
 - 지연: 출력이 나가도록 하기 전의 지연 시간
 - 켜짐: 출력이 발생할 시간
 - 꺼짐: 출력이 발생하지 않을 시간
 - 반복 횟수: 켜짐~꺼짐의 구간을 반복할 횟수
4. 알람 멈춤 이벤트 – 나열된 이벤트가 발생을 하면 선택된 장치의 해당 포트에 설정된 우선순위와 같거나 낮은 출력을 해제할 수 있습니다.

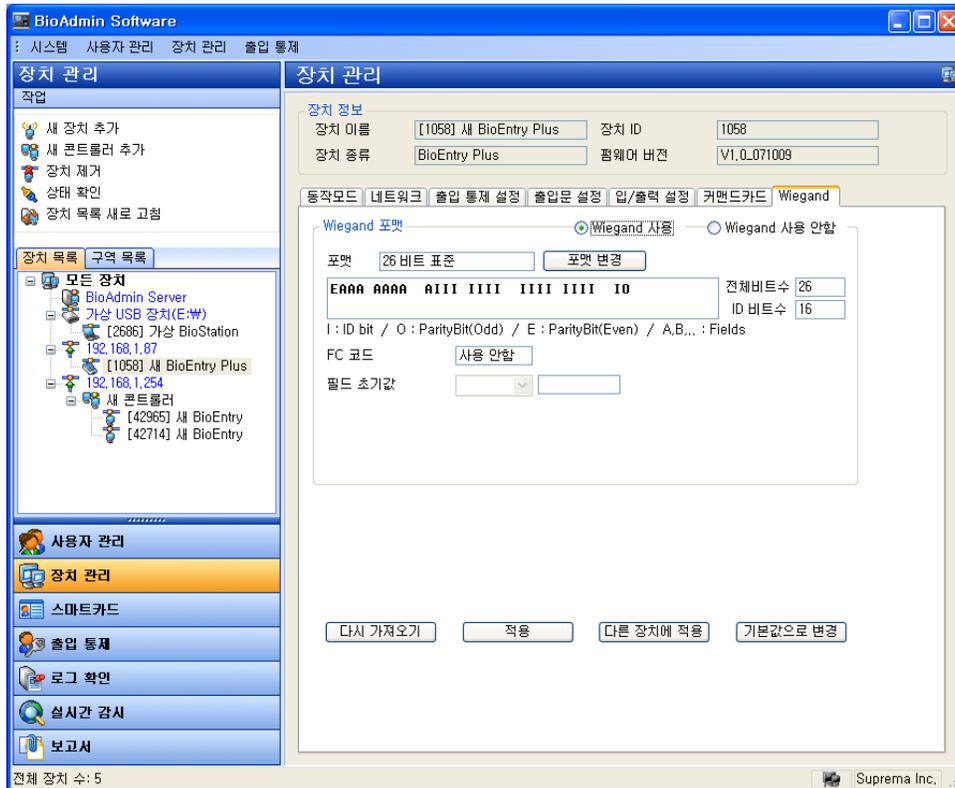
5.7.8. 커맨드카드



- 커맨드 카드는 BioEntry Plus 에서 제공하는 가장 뛰어난 기능 중에 하나입니다. 커맨드 카드를 이용하여 장치에서 간편하게 새 사용자를 추가하거나 삭제 또는 전체삭제를 할 수 있습니다.
- 커맨드 카드 탭에서는 카드의 생성과 권한 설정이 가능합니다.
- 카드 리스트- 현재 선택된 BioEntry Plus에 등록된 커맨드 카드 리스트를 보여 주며, 특정 카드를 삭제 하거나, 전체 삭제 및 다른 장치에서도 사용이 가능하도록 전송이 가능합니다.
- 카드ID - 등록할 RF카드의 ID를 입력하거나 장치로부터 읽은 카드 번호를 표시합니다.
- 커맨드 카드의 등록을 위해서는 카드읽기 버튼을 클릭 하고 장치에서 등록하고자 하는 RF카드를 인식시키면 해당 카드의 ID 가 나타나게 됩니다.
- 커맨드 종류 - 입력하려는 RF 카드에 부여할 기능을 선택합니다.
- 관리자 인증 필요 - 해당 커맨드 카드를 사용할 때 관리자의 지문을 입력하도록 설정할 수 있으며, 무단 사용으로 인한 오용이나 남용을 막을 수 있습니다.

Note: 카드 내에 설정된 기능을 식별하기 어려우므로 커맨드 카드 생성 시 항상 카드에 커맨드 종류를 표시해 주는 것이 좋습니다.
BioEntry Plus Mifare 는 이 기능을 지원하지 않습니다.

5.7.9. Wiegand



- Wiegand 탭은 장치의 Wiegand 출력/입력 포맷을 관리하기 위해 사용됩니다. 이 메뉴를 선택하면 Wiegand 설정 페이지가 주 윈도우에 갱신됩니다.

- Wiegand 포맷

Wiegand 설정 마법사를 이용하여 새로운 Wiegand 포맷을 설정할 수 있습니다. **포맷 변경** 버튼을 누르면 Wiegand 설정 마법사가 나타납니다.

첫 번째 페이지에서 지원되는 3개의 포맷 중 하나를 선택해야 합니다.

- 26 비트 표준 Wiegand 포맷

26 bit standard 형식은 가장 광범위하게 쓰이며 8비트 FC 코드와 16비트 ID로 구성됩니다. 26 bit standard 형식에서 비트 정의와 패리티 비트는 변경할 수 없습니다.

- 패스 스루 Wiegand 포맷

패스 스루 포맷은 ID 필드의 형식을 알고 있을 때만 사용됩니다. Wiegand 입력 문자열이 감지되면, 장치는 ID 비트들을 찾아내고 그 ID로 인증을 시작합니다. 인증이 성공하면 장치는 Wiegand 입력 문자열을 바꾸지 않고 출력합니다. 패리티 체크와 고급 옵션들은 이 형식에서는 무시됩니다. 정의에 따르면 패스 스루 포맷은 사용 모드가 1:1인 경우에만 유용하다고 합니다. 사용 모드가 1:N일 때는 ID 필드 이외에 비트 오더가 0으로 설정되어야 합니다.

가령 32비트 Pass Through format이 다음과 같다고 가정합니다.:

XIIIIII IIIIIIX XXXIIII IIIIIIX

(가장 왼쪽 비트가 0번째 비트, BIT0) I: Id field, X: Unknown field

이 형식을 다음과 같은 순서로 설정할 수 있습니다.

Total Bits 필드에 32를 입력합니다.

정의에 따라 ID 비트를 선택합니다.

Next 버튼을 누릅니다. 패스 스루 모드에서는 패리티 비트를 특정할 수 없습니다.

- 사용자 설정 Wiegand 포맷

사용자가 Wiegand 형식에 대한 모든 정보를 갖고 있다면, 맞춤 포맷을 정의할 수 있습니다. Wiegand 입력 문자열이 감지되면, 장치는 우선 패리티 비트를 확인합니다. 모든 패리티 비트가 정확하면 장치는 ID 비트를 추출하고 그 ID로 인증을 시작합니다. 사용자는 또한 각 필드를 대체 값으로 설정할 수 있고 Fail ID와 같은 고급 옵션을 설정할 수 있습니다. 인증에 성공하면 장치는 Wiegand 문자열을 출력합니다. 출력 문자열은 대체 값과 고급 옵션에 따라 입력 문자열과 다를 수 있습니다.

가령, 44비트 맞춤 포맷이 다음과 같이 구성되었다고 가정합니다:

EAAAAAAAA IIIIIIII IIIIIIII BBBBBI IIIIIIII IIIIO

(가장 왼쪽 비트가 0번째 비트, BIT0)

E: Even parity for BIT1 ~ BIT22

O: Odd parity for BIT23 ~ BIT42

I: ID bits(Field1 and Field 3), A: Field 0, B: Field 2

이 형식을 다음과 같은 순서로 설정할 수 있습니다.

Total Bits 필드에 44를 입력합니다..

Even Parity를 선택합니다.

even parity bit를 누릅니다. 이 예제에서는 BIT0을 말합니다.

정의에 따라 Odd Parity와 User ID에 대해서 (2)와 (3)을 반복합니다.

Next 버튼을 누릅니다.

첫 번째 패리티 비트를 계산하는데 쓰이는 비트들을 누릅니다. 이 예제에서는 BIT1 ~ BIT22 입니다.

>> 버튼을 누릅니다.

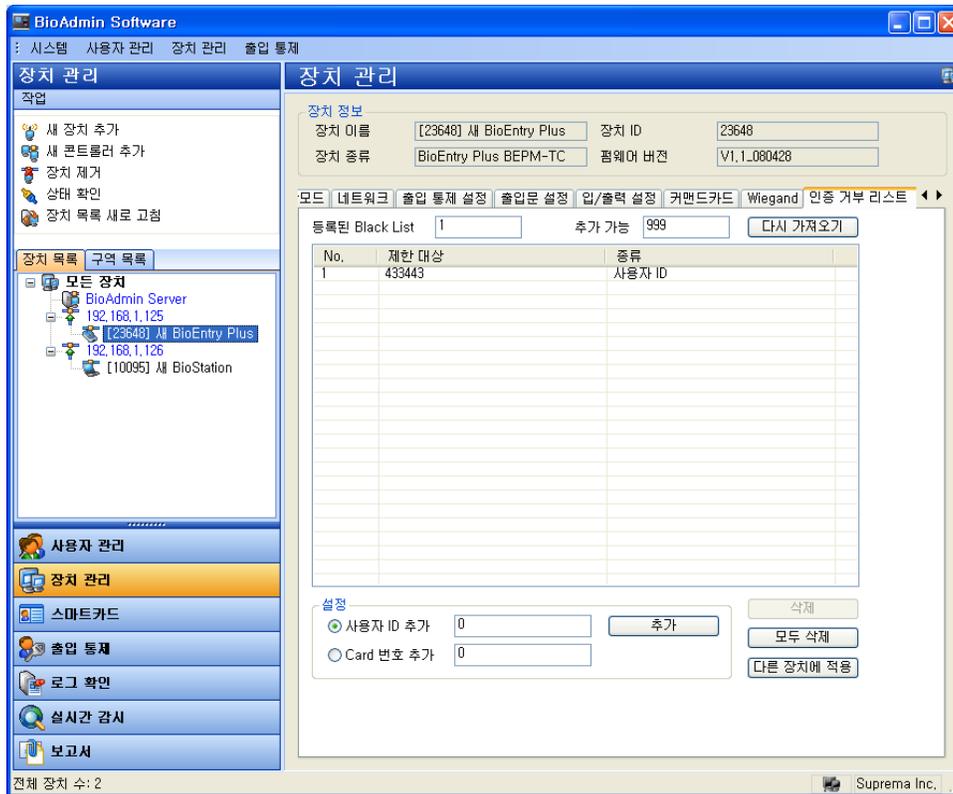
두 번째 패리티 비트를 계산하는데 쓰이는 비트들을 누릅니다. 이 예제에서는 BIT23~ BIT42 입니다.

Next 버튼을 누릅니다.

- 대체 값

26 비트 표준에서 다른 FC code를 특정할 수 있습니다. 맞춤 포맷에서는 non-ID 필드에서 대체 값을 특정할 수 있습니다. 대체 값이 설정되면 장치는 출력을 보내기 전에 해당 필드들을 이 대체 값으로 바꿉니다.

5.7.10. 인증 거부 리스트



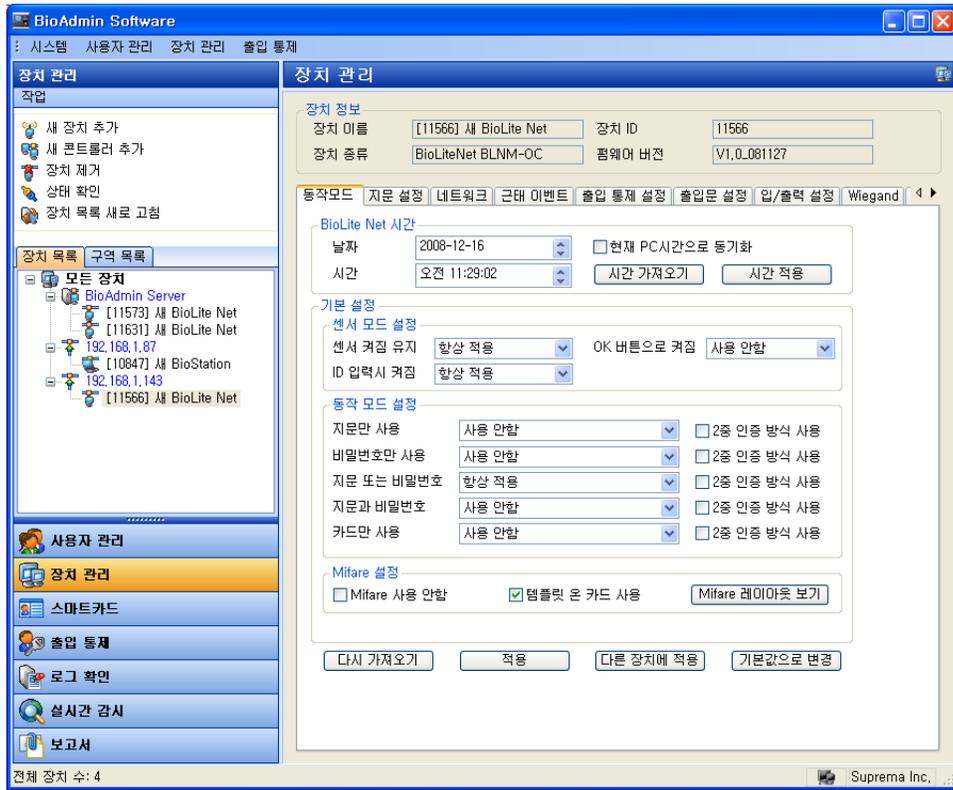
인증을 거부할 리스트를 따로 관리할 수 있습니다. 이 리스트에 등록된 카드번호나 사용자 ID에 대한 인증 요청이 들어오면 단말기는 인증을 거부하고 실패 로그를 남기게 됩니다. 모두 1000개의 리스트를 등록할 수 있습니다.

- **등록된 Black List:** 현재 등록된 list의 수입니다.
- **추가 가능:** 추가로 등록 가능한 list 수입니다.
- **다시 가져오기:** 리스트를 장치로부터 다시 읽어옵니다.
- **추가 :** 사용자 ID 혹은 카드 번호를 체크하여 어떤 항목을 차단할 것인지 결정한 뒤, 번호를 입력하고 '추가'를 클릭합니다. 이미 등록되어 있거나, 1000개를 초과하는 항목을 추가하려고 할 경우에는 등록할 수 없습니다.
- **삭제 :** 리스트에서 삭제하려는 항목을 클릭한 뒤에 '삭제'버튼을 클릭합니다.
- **모두 삭제 :** 현재 등록된 모든 Black list가 삭제됩니다.
- **다른 장치에 적용 :** 현재 black list를 다른 장치에 적용합니다.

5.8. BioLite Net 장치 관리

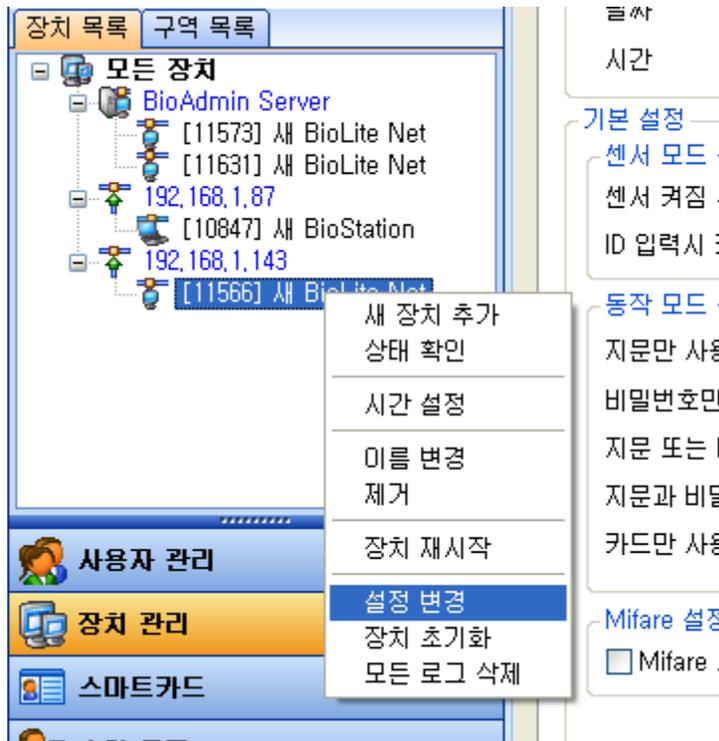
5.8.1. 장치 정보

- 선택한 BioLite Net의 장치 이름, 장치 종류 및 단말기 ID와 펌웨어 버전을 확인할 수 있습니다. 단말기 ID번호와 펌웨어 버전 등은 설치 후 기술 지원 등에서 제품을 확인하기 위해 필요한 정보입니다.



5.8.2. UDP로 환경 설정하기

- BioEntry Plus 아이콘이나 이름 위에서 마우스 오른쪽 버튼 클릭으로 '설정 변경' 메뉴를 선택할 수 있습니다.



- 시스템 정보 – 현재 BioLite Net에 부여된 ID 및 MAC 어드레스를 확인 할 수 있으며, 새로고침 버튼 클릭으로 정보를 다시 읽어오도록 할 수 있습니다.
- 네트워크 환경 설정
 1. DHCP 사용
 - 해당 BioLite Net 이 DHCP를 지원하는 네트워크에 설치 되어 자동으로 IP 를 부여 받도록 설정하는 경우 체크합니다. DHCP를 지원하지더라도 체크 를 지우고 지정된 네트워크 정보를 입력할 수 있습니다.
 2. Server 사용
 - BioLite Net 이 BioAdmin Server에 접속하여 동작하도록 설정할 경우 체크 합니다.
 - 서버와 자동으로 시간 동기화 하는 경우 체크합니다.
 3. 포트
 - 서버 포트와 BioLite Net의 포트를 같은 값을 사용합니다. 기본적으로 BioLite Net 은 1471 포트를 사용하지만, BioAdmin Server를 사용하는 경우 서버 설정에서 정한 포트 번호를 입력해야 하며, 모르는 경우 Sever Configuration 을 다시 실행 시켜 확인할 수 있습니다. 기본값으로 1480을 사용하므로 서버사용에 체크하는 경우 대부분 1480으로 포트를 입력해야 합니다.

BioEntry Plus / BioLite Net 설정 변경

192.168.1.143(11566)

시스템 정보

ID 11566 새로 고침

MAC 00:17:fc:20:2d:2e 장치 재시작

네트워크 환경 설정

DHCP 사용 Server 사용 저장

서버와 자동으로 시간 동기화 새로 고침

IP 주소 192 . 168 . 1 . 143

게이트웨이 192 . 168 . 1 . 10

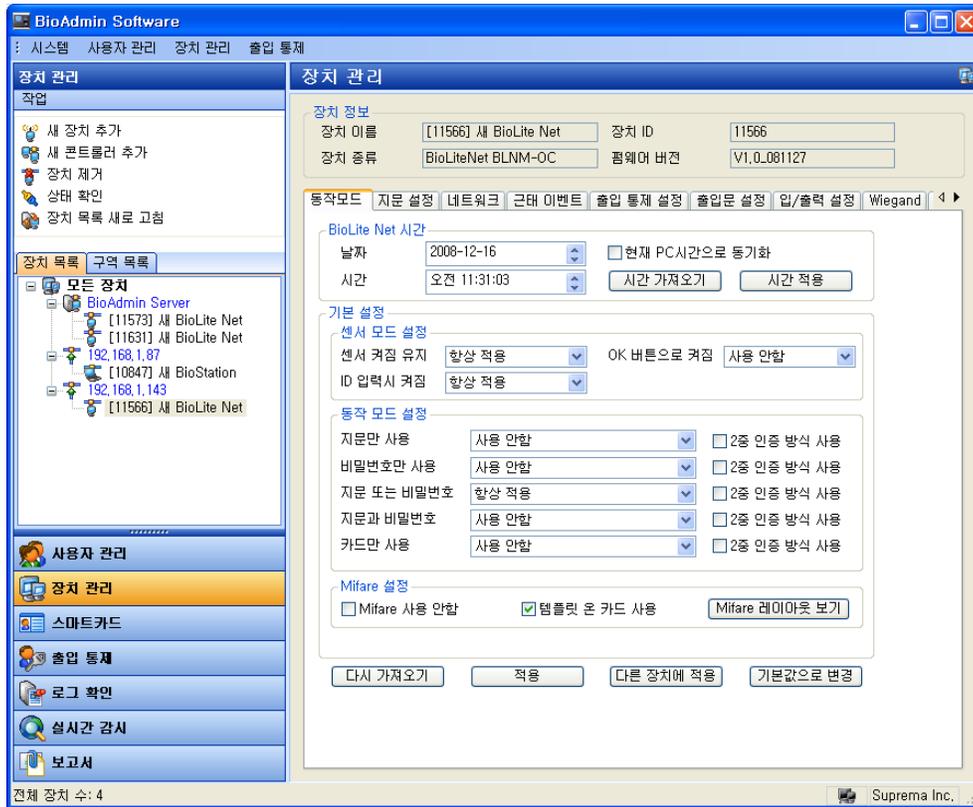
서브넷 255 . 255 . 255 . 0

서버 IP 주소 0 . 0 . 0 . 0

포트 1471

확인

- 5.8.3. 동작 모드
- 시간 설정



처음에 보이는 날짜와 시간이 BioLite Net 에서 읽어온 값입니다. 시간가져오기 버튼을 클릭하면 BioLite Net으로 부터 날짜와 시간을 다시 읽어옵니다. BioLite Net의 시간 변경 방법은 직접 입력 방법과 현재 PC 시간으로 동기화의 두 가지 방법으로 나뉩니다.

- 직접 입력: 날짜와 시간 창에서 숫자를 직접 입력하거나 숫자에 커서를 두고 위아래 화살표를 클릭하여 입력합니다. 입력 후 시간적용 버튼을 누르면 입력된 날짜와 시간이 선택된 BioLite Net으로 전송됩니다.
- PC 시간으로 동기화: 현재 PC시간으로 동기화를 체크하고, 시간적용 버튼을 누르시면 선택된 BioLite Net 의 시간이 현재 PC의 시간으로 맞춰집니다.

BioLite Net 시간

날짜	2008-12-09	<input type="checkbox"/> 현재 PC시간으로 동기화
시간	오전 4:56:21	<input type="button" value="시간 가져오기"/> <input type="button" value="시간 적용"/>

● 센서 모드 설정

상황에 따른 센서 사용 여부를 설정할 수 있는 센서 모드는 항상적용과 사용안함 및 미리 설정된 출입통제 메뉴의 출입시간으로 설정할 수 있습니다. 설정된 시간은 각각 중복하여 적용할 수 있으며 선택된 시간이 되면 해당 모드로 동작하게 됩니다.

센서 모드 설정

센서 켜짐 유지	<input type="text" value="항상 적용"/>	OK 버튼으로 켜짐	<input type="text" value="사용 안함"/>
ID 입력시 켜짐	<input type="text" value="항상 적용"/>		

● 동작 모드 설정

동작모드설정은 각각의 인증 방식을 언제 사용할 것인가에 대한 설정을 할 수 있습니다. 항상적용과 사용안함 및 미리 설정된 출입통제 메뉴의 출입시간을 선택할 수 있습니다. 두 가지의 다른 인증 방식이 동일 시간에 겹치지 않아야 합니다.

- 2중 인증 방식 : 15초 이내에 각각 다른 사용자의 인증이 이루어져야 출입문이 동작하는 기능으로 보안성을 강화할 때 적용할 수 있습니다.

동작 모드 설정

지문만 사용	<input type="text" value="항상 적용"/>	<input type="checkbox"/> 2중 인증 방식 사용
비밀번호만 사용	<input type="text" value="사용 안함"/>	<input type="checkbox"/> 2중 인증 방식 사용
지문 또는 비밀번호	<input type="text" value="사용 안함"/>	<input type="checkbox"/> 2중 인증 방식 사용
지문과 비밀번호	<input type="text" value="사용 안함"/>	<input type="checkbox"/> 2중 인증 방식 사용
카드만 사용	<input type="text" value="사용 안함"/>	<input type="checkbox"/> 2중 인증 방식 사용

● Mifare Setting

현재 BioLite Net이 Mifare 를 지원하는 경우 이 항목이 활성화 되며 설정을 변경할 수 있습니다. 그 외 모델에 대해서는 사용할 수 없습니다.

Mifare 설정

<input type="checkbox"/> Mifare 사용 안함	<input checked="" type="checkbox"/> 템플릿 온 카드 사용	<input type="text" value="Mifare 레이아웃 보기"/>
---------------------------------------	-------------------------------------------------	---------------------------------------------

- Mifare 사용 안 함
Mifare Card의 사용을 끄고 card입력을 받아들이지 않도록 설정할 수 있습니다.
- 템플릿 온 카드 사용
Mifare card에 사용자 정보를 저장하여 사용할 것인지, 아니면 RF-card와 같은 방식으로 Card ID만 사용할 것인지 설정할 수 있습니다.
- Mifare레이아웃보기
현재 BioLite Net 에 설정된 Mifare Layout 정보를 확인할 수 있습니다. 이 정보는 6.5.7. Mifare 카드 레이아웃 설정 (BioStation / BioEntry Plus)절을 참고하여 수정할 수 있습니다.

5.8.4. 지문 설정

지문 설정

보안 등급	<input type="text" value="보통"/>	1:N 인식 속도	<input type="text" value="자동"/>
지문 입력 시간	<input type="text" value="10 초"/>	인증 제한 시간	<input type="text" value="3 초"/>

1. 보안 등급

보안 등급은 보통, 안전, 가장 안전 중에 선택할 수 있습니다. 내부적으로 보

안 등급은 FAR(타인 수락 율, False Acceptance Ratio)을 조정합니다. FAR과 FRR(본인 거부 율, False Rejection Ratio)은 서로 반비례 관계이기 때문에 보안등급을 높이면 보안성은 높아지지만 FRR이 증가하여 거부 율이 올라갈 수 있습니다. 초기 설정 값은 보통입니다.

2. 1:N 인식 속도

수백 개 이상의 지문이 장치에 저장되어 있을 경우, 1:N 인식시간이 길어질 수 있습니다. 매칭 속도를 **빠름**이나 **가장 빠름**으로 설정하면 인증 성능이 다소 떨어지는 대신 1:N 인식 시간을 단축시킬 수 있습니다. 기본 설정 값은 보통입니다.

3. 지문 입력 시간

지문 입력 시 대기시간을 말합니다. 이 시간 내에 사용자가 지문을 입력하지 않으면 입력 실패로 판단합니다. 기본 설정 값은 **10초**입니다.

4. 인증 제한 시간

지문 입력 후, 인증 결과를 나타내기까지의 최대 시간을 지정할 수 있으며, 설정된 시간이 경과되면 인증 결과가 나오지 않더라도 지문 검색을 중단 합니다. 이 기능은 입력된 지문의 정보가 너무 적어 검색 시간이 길어질 때 일정 시간이 지나면 검색을 중단하여 전체 사용자의 원활한 사용을 유도하기 위해 사용됩니다.

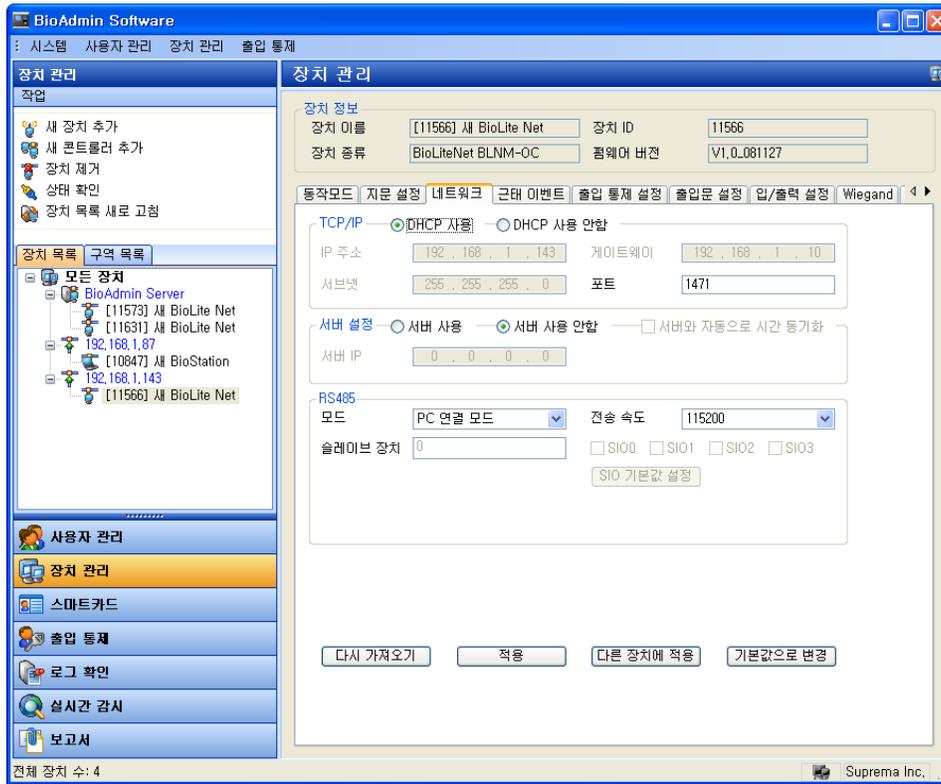
● 지문 옵션 정보

지문 옵션 정보

ISO 템플릿 사용 위조 지문 검사

- ISO 템플릿 사용
ISO 표준 템플릿 사용 유무를 나타냅니다.
- 위조 지문 검사
위조 지문 검사 기능의 사용 유무를 나타냅니다.

5.8.5. 네트워크



● TCP/IP

1. TCP/IP 설정

- BioLite Net 의 설정 값 중에서 IP주소를 자동으로 받을 것인지, 수동으로 설정할 것인지를 선택합니다. 네트워크 환경에 따라 DHCP를 지원하여 BioLite Net 에 IP주소가 자동으로 부여될 경우 'DHCP 사용'을, 지정된 IP 를 직접 설정할 경우에는 'DHCP 사용 안함'을 선택합니다.
- IP주소, 게이트웨이, 서브넷, 포트는 각각 알맞은 값으로 설정합니다.
- 포트는 기본값으로 1471을 사용하지만, 서버를 사용하는 경우에는 서버 포트로 설정하여야 합니다.



2. 서버 설정

- 해당 BioLite Net 이 서버에 연결되어 있는지를 보여줍니다.
- 일반 TCP/IP로 연결된 BioLite Net 을 서버에 연결시키고자 할 경우에는 서버 사용에 체크한 후 서버 IP 주소와 서버 포트를 설정하면 됩니다.
- 이처럼 서버에 연결하는 경우, 해당 BioLite Net 은 원래 연결되어 TCP/IP 에서 연결이 즉시 해제되며, 목록에서 BioAdmin Server 아래로 다시 연결 되어 나타나게 됩니다. 다시 목록에 보여지기 까지는 네트워크 환경에 따

라 다소 시간이 걸릴 수 있습니다.

- 서버에 연결된 BioLite Net 의 통신상태가 좋지 않을 때에는 장치목록에 있는 BioAdmin Server 서버에서 마우스 오른쪽 버튼을 클릭한 후 서버 재접속을 시도하십시오.

서버 설정 — 서버 사용 — 서버 사용 안함 — 서버와 자동으로 시간 동기화

서버 IP

3. RS485 설정

BioLite Net 의 RS485 포트로 통신을 사용하는 경우에 대해 설정합니다.

RS485모드에서는 서로 연결된 장치가 호스트(Host)와 슬레이브(Slave) 역할을 나누어 하게 되며 해당 장치를 Host 로 할지 Slave 로 할지를 결정 합니다.

BioStation, BioEntry Plus, BioLite Net 및 Secure I/O 로 구성되는 통합 시스템 은 Host 장치 1대, Slave 장치 1대와 함께 4대의 Secure I/O 가 최대로 연결되며, Host 장치는 총 10개의 릴레이와 20개의 입력을 관리합니다.

- 시스템의 장치 구성에 따라 다음과 같이 설정 합니다. (편의상 BioStation 및 Secure I/O와의 연결에 대해서 예를 들었으며, 경우에 따라서 BioStation 대신 BioEntry Plus를 사용하는 경우도 동일하게 설정하면 됩니다.)
- BioStation 을 출입문 바깥쪽에 설치하고 BioLite Net 을 안쪽에 설치하는 경우:
일반적으로 보안을 위해 안쪽에 설치된 장치에서 출입문 오픈 릴레이를 내 보내게 되므로 안쪽에 설치되는 BioLite Net 을 'Host'로 설정합니다. BioStation는 'Slave'로써 하위장치가 되며 RS485로 BioLite Net 에 연결합니다. 설정 방법으로는 BioLite Net의 장치관리 메뉴 내 네트워크 탭에서 'Host' 선택 후 하위장치인 BioStation의 ID를 입력하고, 'Slave' 장치가 되는 BioStation에서는 장치관리 메뉴의 네트워크 탭에서 'Slave' 로 지정해 두어야 합니다.
- BioLite Net을 출입문 바깥쪽에 설치하고 Secure I/O 를 설치하는 경우:
BioLite Net이 'Host' 가 되어 Secure I/O 의 입출력을 제어하며, 인증에 성공하면 BioLite Net은 Secure I/O 를 통해 출입문을 열게 됩니다. 설정 방법으로는 BioLite Net을 'Host' 로 설정 후, 제어하고자 하는 SIO 를 Check 합니다. 총 4대까지 연결이 가능하며, Secure I/O 뒷면의 DIP스위치를 조정하여 부여된 번호를 선택합니다. Secure I/O 의 기본 입출력 설정을 통해 출입문이나 비상 경광등 등을 제어할 수 있습니다.
- Secure I/O 에 대한 자세한 설명은 Secure I/O 매뉴얼을 참조하시기 바랍니다.

RS485

모드 전송 속도

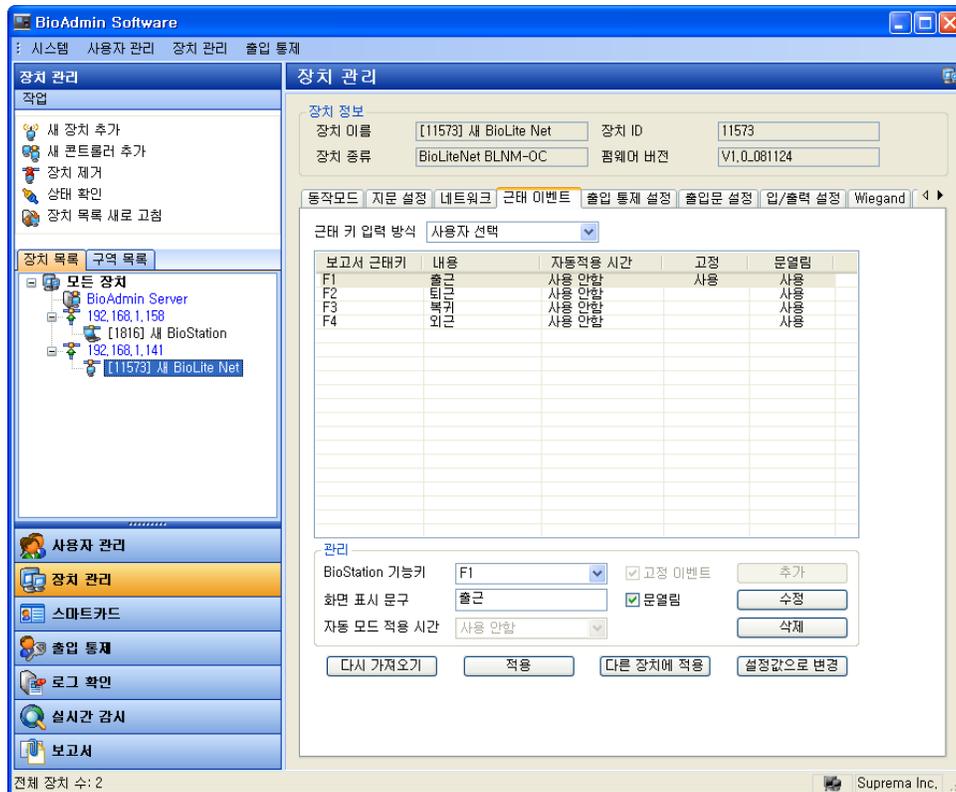
슬레이브 장치 SIO0 SIO1 SIO2 SIO3

5.8.6. 근태 이벤트

근태 기능키는 출근, 퇴근, 외근, 복귀 등과 같이 근태관리 용도로 지문 입력 전에 근태이벤트를 입력하기 위한 키를 의미합니다. **BioLite Net**에서는 좌/우 키를 이용해 설정된 근태 이벤트 중 원하는 이벤트를 선택할 수 있으며, 16개까지 기능키를 사용할 수 있습니다. **BioLite Net**에서 근태 이벤트를 먼저 선택한 뒤 지문 입력을 하면 해당 근태이벤트가 로그에 기록되게 되며, 향후 근태관리 소프트웨어에서 이 로그정보를 이용하여 각종 근태 및 급여 관리 데이터로 사용할 수 있습니다.

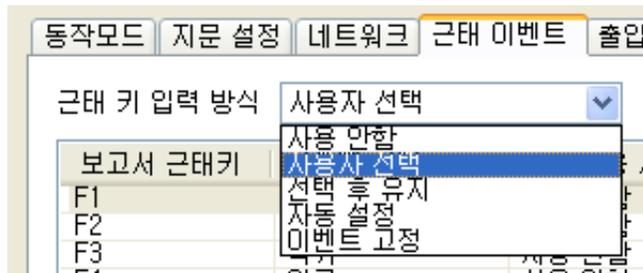
BioAdmin 소프트웨어에서 근태 기능키와 관련하여, 장치관리 메뉴에서의 내용과 보고서 메뉴에서 근태관리 규칙에서의 내용을 모두 참조해야 합니다.

여기서 설명하는 장치관리 메뉴에서의 근태 기능키 설정은 **BioLite Net**의 화면에서 보이는 근태 이벤트의 메시지를 설정하는 것이고, 보고서 메뉴의 근태관리 규칙에서의 근태 이벤트 설정은 근태 보고서 생성시 적용할 근태 이벤트 메시지를 설정하는 것입니다. **BioLite Net**의 로그에서는 실제 근태 이벤트 메시지가 기록되지 않고 눌러진 근태 이벤트의 번호가 기록됩니다. **BioAdmin**에서는 이 값을 읽어 미리 정의된 기능키와 근태이벤트 간의 테이블을 참조하여 그에 맞는 근태 보고서를 작성하는 것입니다. 따라서, 이 장에서 설정하는 근태 기능키의 이벤트는 실제 **BioAdmin**의 보고서나 로그확인 시에는 나타나지 않습니다.



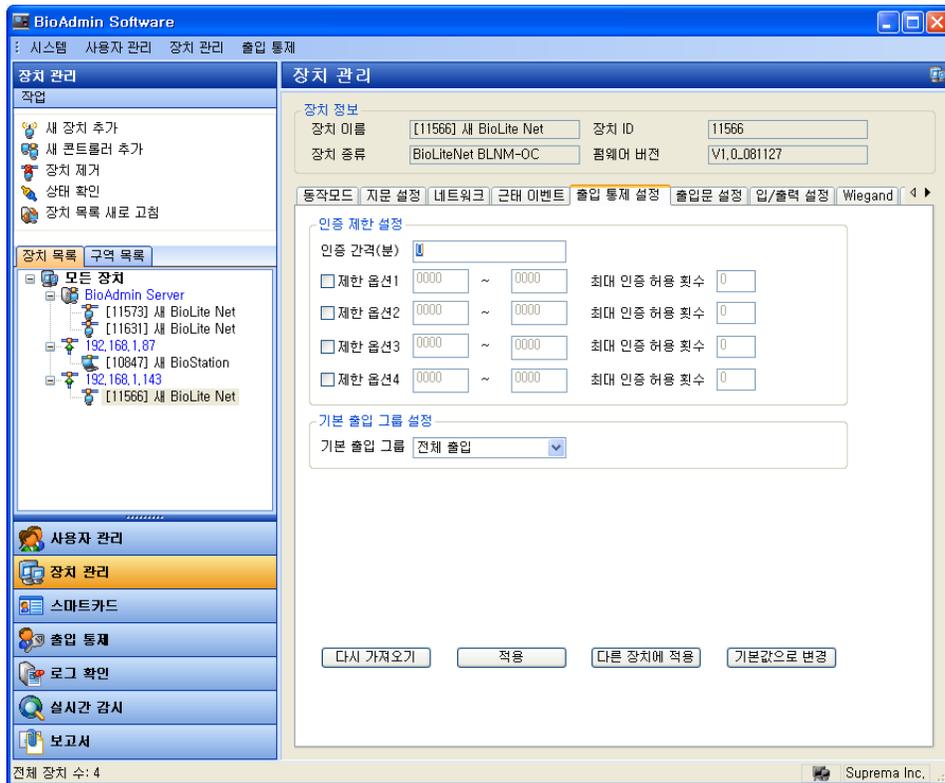
장치에서의 16개 이벤트의 설정을 하며, 근태 이벤트에서 16개 중에서 하나를 선택하여 BioLite Net 의 LCD 창에 표시될 이벤트의 메시지와, 릴레이 사용여부 체크를 합니다.

- 근태 키 입력 방식에서 원하는 방식을 선택합니다. 선택할 수 있는 항목으로는 사용 안함, 사용자 선택, 선택 후 유지, 자동 설정, 이벤트고정 이 있습니다.
 - 사용 안함: 근태 이벤트를 사용하지 않는 경우 선택합니다.
 - 사용자 선택: 평상시에는 이벤트를 사용하지 않다가, 필요한 경우 사용자가 매번 선택하여 인증을 하는 경우 선택합니다.
 - 선택 후 유지: 사용자가 필요에 의해 특정 이벤트를 선택한 뒤에 다른 사용자가 이벤트를 변경하기 전까지 계속 동일한 이벤트를 사용하도록 유지할 경우 선택합니다.
 - 자동 설정: 관리자가 출입 통제에서 미리 설정한 시간대에 맞춰서 자동으로 변경되도록 할 경우 선택합니다.
 - 이벤트 고정: 항상 동일한 이벤트로 동작하도록 할 경우 선택합니다.



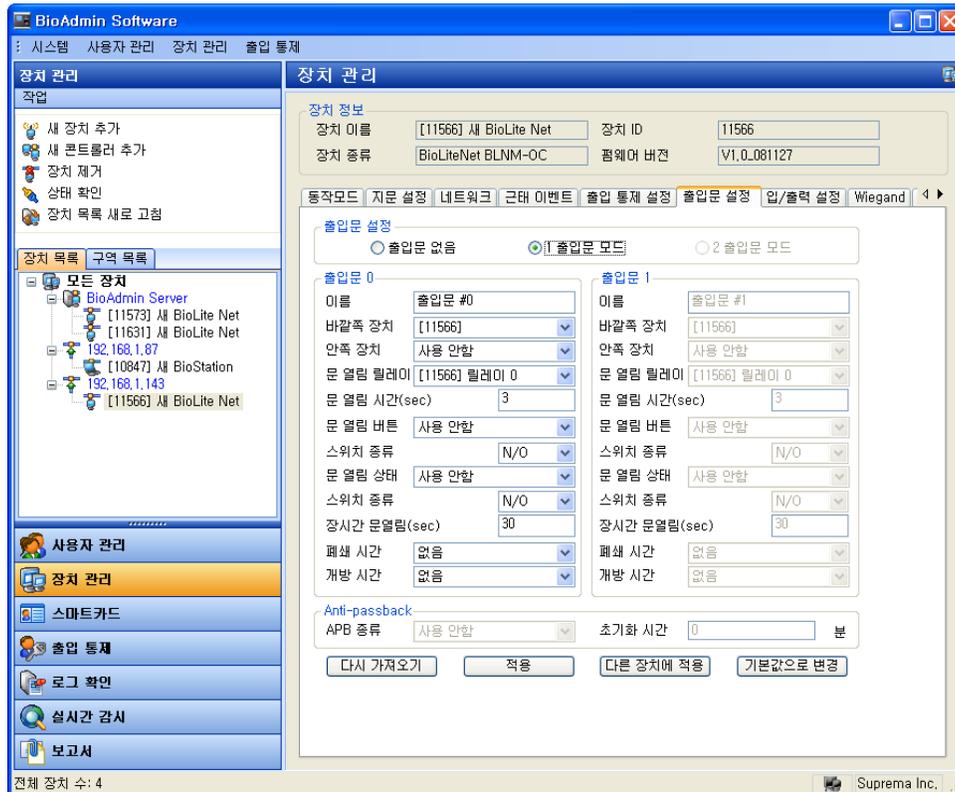
- 설정할 BioStation 기능을 선택합니다. 이 기능키는 BioStation에서 사용하는 근태 키의 역할을 의미하는 것으로 실제 키가 BioLite Net에는 존재하지 않지만 로그에서는 BioStation에서 해당 키를 누른 것과 같은 효과를 주기 위한 정보입니다.
- 화면 표시 문구 난에 이벤트 명을 직접 입력합니다.
- 선택된 이벤트의 릴레이 사용유무를 위해 문열림의 체크를 결정합니다. 릴레이는 보통 출입문의 락 제어장치와 연결되어 문을 개폐하는데 사용됩니다.
- 근태 키 입력 방식을 고정으로 선택한 경우, BioStation 기능키 옆에 고정을 할 것인지는 묻는 체크박스가 활성화 되며, 특정 근태기능키에서 고정을 체크하는 경우 장치는 해당 근태기능 상태만 입력을 받습니다. 예를 들어 출 퇴근용 입력 장치를 각각 사용하는 경우, 적용할 수 있습니다.
- 근태 키 입력 방식을 자동 설정으로 선택한 경우, 자동 모드 적용 시간이 활성화 됩니다. 출입통제에서 미리 설정한 출입시간을 선택하여 각 기능키에 자동으로 근태 이벤트를 적용할 수 있도록 설정할 수 있습니다.

5.8.7. 출입 통제 설정



- 출입 통제 설정에서는 반복 인증을 제한하거나, 특정 시간 동안 반복 출입을 막는 등의 설정이 가능합니다. 이 기능은 특정 시간 사이에 한번만 인증 되도록 하는 식수 관리 등에 활용이 가능합니다.
- 인증 제한 설정
 1. 인증 간격 - 입력된 시간(분) 이내에 재 인증이 이루어지면 인증을 제한합니다.
 2. 제한옵션 1~4 - 각각의 옵션별 시작시간~끝시간을 입력하고 해당 시간에 대해서 최대 출입 허용 횟수를 적어주면, 지정된 시간 동안에는 지정된 횟수만큼만 인증을 허용합니다.
- 근태 자동 전환
 1. 선택된 **BioLite Net**을 어떤 근태모드로 사용할 것인지 설정 합니다.
 2. 근태 모드 : 사용 안함, 출근고정, 퇴근고정, 자동 설정 모드가 있습니다.
 - 자동 설정 : 지정된 시간에 따라 자동으로 출근과 퇴근 시간으로 변환 되도록 설정이 가능합니다. 출입통제에서 설정된 출입시간을 선택하여 지정된 시간에 인증이 이루어지면 출근 혹은 퇴근으로 자동으로 근태 모드가 변경됩니다.
 - 출근고정, 퇴근고정 : 특정 장치를 항상 선택된 근태모드로 적용되도록 하는 것으로 출근이나 퇴근 중 한가지 상태로 설정할 수 있습니다.
- 기본 출입 그룹 설정
아무런 출입 그룹 정보가 없는 사용자의 경우 여기서 설정된 출입 그룹이 적용 되도록 기본 내용을 설정할 수 있습니다.

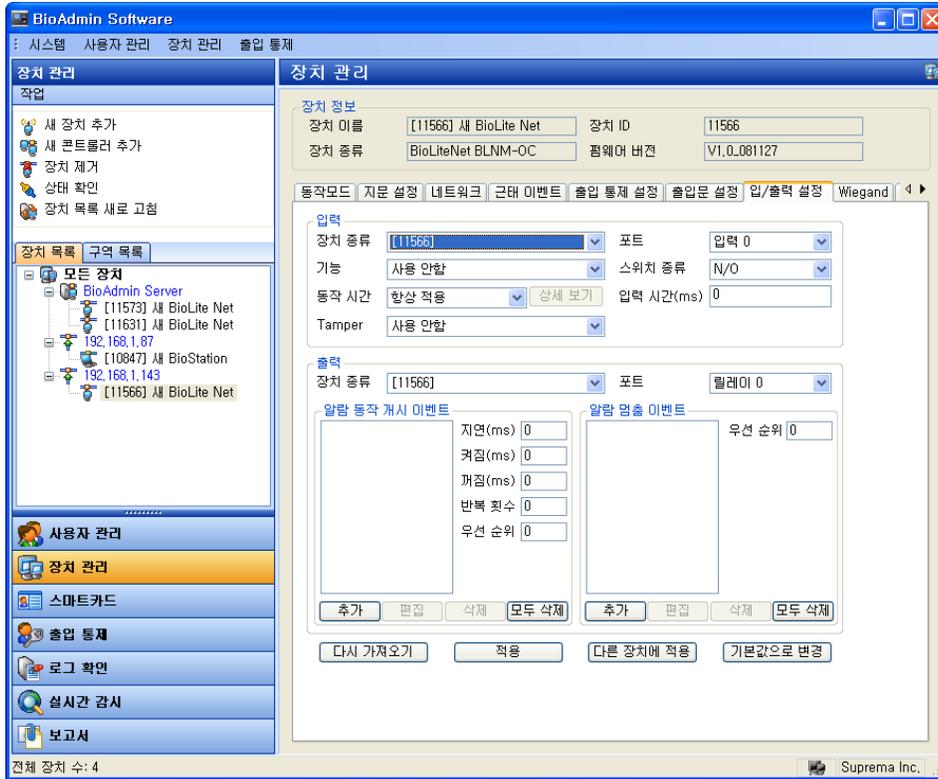
5.8.8. 출입문 설정



- 각 출입문을 제어하는 장치에 대해 입출력을 설정합니다.
- 바깥쪽 장치, 안쪽장치 - 1개의 출입문에 설치되어 동작하게 되는 2개의 장치를 위치에 따라 설정하여야 합니다.
- 문 열림 릴레이 - 연결된 장치들 중, 어떤 장치를 이용하여 출입문을 제어할지에 대한 출력 장치를 설정하거나 사용안함을 선택할 수 있습니다.
- 문 열림 시간(초) - 문 열림 릴레이에서 선택한 출력 단자가 동작하는 시간을 입력합니다.
- 문 열림 버튼 - 출입문을 여는데 버튼용 입력 단자를 사용할 것인지에 따라 사용을 원하면 원하는 장치의 입력을 선택합니다. 스위치의 종류는 입력 되는 신호에 따라 스위치가 평소에 오픈 상태로 유지할 경우엔 N/O 를, 평소에 닫힌 상태로 유지될 경우엔 N/C 를 선택합니다.
- 문 열림 상태 - 출입문의 상태를 파악하는데 사용할 센서를 사용할 것인지에 따라, 사용을 원하면 원하는 장치의 입력을 선택합니다.. 스위치의 종류는 입력 되는 신호에 따라 스위치가 평소에 오픈 상태로 유지할 경우엔 N/O 를, 평소에 닫힌 상태로 유지될 경우엔 N/C 를 선택합니다.
- 장시간 문열림(초) - 문이 오래 열려 있는 것을 판단하는 시간을 정합니다.
- 폐쇄 시간 - 출입 통제 항목에서 설정한 출입 시간에 연동되는 항목으로 항상 잠겨 있는 시간을 설정할 수 있습니다.
- 개방 시간 - 출입 통제 항목에서 설정한 출입 시간에 연동되는 항목으로 항상 열려 있는 시간을 설정할 수 있습니다.

- **Anti-passback:** 바깥쪽 장치와 안쪽 장치간의 **Anti-pass back**을 적용할지 여부를 설정할 수 있습니다.
Soft : 인증시 **APB** 위반이더라도 기록만 남기고 출입을 허용합니다.
Hard : 인증시 **APB** 위반일 경우 기록과 함께 출입도 제한합니다.
초기화시간 : **APB** 로 인해 출입이 통제 되더라도 지정된 시간이 지나면 출입을 허용하는 설정입니다.

5.8.9. 입/출력 설정



- 출입문 설정 이외에 입/출력 단자를 원하는 대로 설정이 가능합니다.
- 입력

입력

장치 종류	[11566]	포트	입력 0
기능	사용 안함	스위치 종류	N/O
동작 시간	항상 적용	상세 보기	입력 시간(ms) 0
Tamper	사용 안함		

1. 장치 종류 - 현재 설정 가능한 장치가 표시 되며, 선택할 수 있습니다.
2. 포트 - 선택한 장치에서 설정 가능한 입력 단자를 선택합니다.
3. 기능 - 입력으로 발생하도록 할 기능을 선택합니다.
4. 동작 시간 - 출입 통제에서 설정한 시간에 대해서만 해당 입력이 동작하도록

출입시간을 선택하여 설정이 가능합니다.

5. 입력 시간(ms) - 해당 시간이상 입력되어야 동작하도록 합니다.

6. Tamper - Tamper의 기능을 선택하여 부여할 수 있습니다.

● 출력

출력

장치 종류 [11566] ▼ 포트 릴레이 0 ▼

알람 동작 개시 이벤트

지연(ms)	0
켜짐(ms)	0
꺼짐(ms)	0
반복 횟수	0
우선 순위	0

알람 멈춤 이벤트

우선 순위	0
-------	---

추가 편집 삭제 모두 삭제

1. 장치 종류 - 현재 설정 가능한 장치가 표시되며, 선택할 수 있습니다.

2. 포트 - 선택한 장치에서 설정 가능한 출력 단자를 선택합니다.

3. 알람 동작 개시 이벤트 - 나열된 이벤트가 발생을 하면 현재 선택된 장치의 해당 포트에서 출력이 발생하도록 설정할 수 있습니다.

■ 이벤트 추가

- 이벤트: 선택된 이벤트가 발생을 하면 앞에서 선택한 장치의 포트로 출력이 나가도록 설정합니다.

- 장치: 이벤트가 발생할 장치를 선택합니다.

- 우선 순위: 해당 기능에 대해서 우선순위를 부여하여 낮은 우선 순위를 가진 기능이 보다 중요한 우선 순위의 이벤트를 가리거나 끄는 것을 방지할 수 있습니다.

- 신호 과형

■ 지연: 출력이 나가도록 하기 전의 지연 시간

■ 켜짐: 출력이 발생할 시간

■ 꺼짐: 출력이 발생하지 않을 시간

■ 반복 횟수: 켜짐~꺼짐의 구간을 반복할 횟수

4. 알람 멈춤 이벤트 - 나열된 이벤트가 발생을 하면 선택된 장치의 해당 포트에 설정된 우선순위와 같거나 낮은 출력을 해제할 수 있습니다.

5.8.10. Wiegand



- Wiegand 탭은 장치의 Wiegand 출력/입력 포맷을 관리하기 위해 사용됩니다. 이 메뉴를 선택하면 Wiegand 설정 페이지가 주 윈도우에 갱신됩니다.

- Wiegand 포맷

Wiegand 설정 마법사를 이용하여 새로운 Wiegand 포맷을 설정할 수 있습니다. **포맷 변경** 버튼을 누르면 Wiegand 설정 마법사가 나타납니다.

첫 번째 페이지에서 지원되는 3개의 포맷 중 하나를 선택해야 합니다.

- 26 비트 표준 Wiegand 포맷

26 bit standard 형식은 가장 광범위하게 쓰이며 8비트 FC 코드와 16비트 ID로 구성됩니다. 26 bit standard 형식에서 비트 정의와 패리티 비트는 변경할 수 없습니다.

- 패스 스루 Wiegand 포맷

패스 스루 포맷은 ID 필드의 형식을 알고 있을 때만 사용됩니다. Wiegand 입력 문자열이 감지되면, 장치는 ID 비트들을 찾아내고 그 ID로 인증을 시작합니다. 인증이 성공하면 장치는 Wiegand 입력 문자열을 바꾸지 않고 출력합니다. 패리티 체크와 고급 옵션들은 이 형식에서는 무시됩니다. 정의에 따르면 패스 스루 포맷은 사용 모드가 1:1인 경우에만 유용하다고 합니다. 사용 모드가 1:N일 때는 ID 필드 이외에 비트 오더가 0으로 설정되어야 합니다.

가령 32비트 Pass Through format이 다음과 같다고 가정합니다.:

XIIIIII IIIIIIX XXXIIII IIIIIIX

(가장 왼쪽 비트가 0번째 비트, BIT0) I: Id field, X: Unknown field

이 형식을 다음과 같은 순서로 설정할 수 있습니다.

Total Bits 필드에 32를 입력합니다.

정의에 따라 ID 비트를 선택합니다.

Next 버튼을 누릅니다. 패스 스루 모드에서는 패리티 비트를 특정할 수 없습니다.

- 사용자 설정 Wiegand 포맷

사용자가 Wiegand 형식에 대한 모든 정보를 갖고 있다면, 맞춤 포맷을 정의할 수 있습니다. Wiegand 입력 문자열이 감지되면, 장치는 우선 패리티 비트를 확인합니다. 모든 패리티 비트가 정확하면 장치는 ID 비트를 추출하고 그 ID로 인증을 시작합니다. 사용자는 또한 각 필드를 대체 값으로 설정할 수 있고 Fail ID와 같은 고급 옵션을 설정할 수 있습니다. 인증에 성공하면 장치는 Wiegand 문자열을 출력합니다. 출력 문자열은 대체 값과 고급 옵션에 따라 입력 문자열과 다를 수 있습니다.

가령, 44비트 맞춤 포맷이 다음과 같이 구성되었다고 가정합니다:

EAAAAAAAA IIIIIIII IIIIIIII BBBBBI IIIIIIII IO

(가장 왼쪽 비트가 0번째 비트, BIT0)

E: Even parity for BIT1 ~ BIT22

O: Odd parity for BIT23 ~ BIT42

I: ID bits(Field1 and Field 3), A: Field 0, B: Field 2

이 형식을 다음과 같은 순서로 설정할 수 있습니다.

Total Bits 필드에 44를 입력합니다..

Even Parity를 선택합니다.

even parity bit를 누릅니다. 이 예제에서는 BIT0을 말합니다.

정의에 따라 Odd Parity와 User ID에 대해서 (2)와 (3)을 반복합니다.

Next 버튼을 누릅니다.

첫 번째 패리티 비트를 계산하는데 쓰이는 비트들을 누릅니다. 이 예제에서는 BIT1 ~ BIT22 입니다.

>> 버튼을 누릅니다.

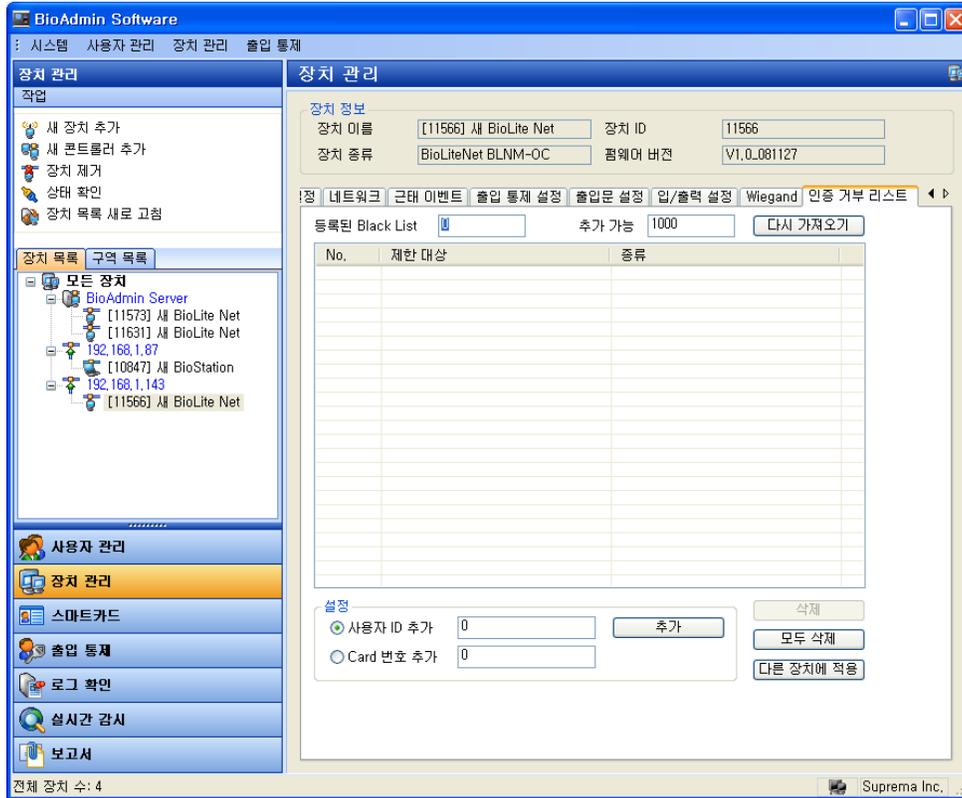
두 번째 패리티 비트를 계산하는데 쓰이는 비트들을 누릅니다. 이 예제에서는 BIT23~ BIT42 입니다.

Next 버튼을 누릅니다.

- 대체 값

26 비트 표준에서 다른 FC code를 특정할 수 있습니다. 맞춤 포맷에서는 non-ID 필드에서 대체 값을 특정할 수 있습니다. 대체 값이 설정되면 장치는 출력을 보내기 전에 해당 필드들을 이 대체 값으로 바꿉니다.

5.8.11. 인증 거부 리스트



인증을 거부할 리스트를 따로 관리할 수 있습니다. 이 리스트에 등록된 카드번호나 사용자 ID에 대한 인증 요청이 들어오면 단말기는 인증을 거부하고 실패 로그를 남기게 됩니다. 모두 1000개의 리스트를 등록할 수 있습니다.

- **등록된 Black List:** 현재 등록된 list의 수입입니다.
 - **추가 가능:** 추가로 등록 가능한 list 수입입니다.
 - **다시 가져오기:** 리스트를 장치로부터 다시 읽어옵니다.
 - **추가 :** 사용자 ID 혹은 카드 번호를 체크하여 어떤 항목을 차단할 것인지 결정한 뒤, 번호를 입력하고 '추가'를 클릭합니다. 이미 등록되어 있거나, 1000개를 초과하는 항목을 추가하려고 할 경우에는 등록할 수 없습니다.
 - **삭제 :** 리스트에서 삭제하려는 항목을 클릭한 뒤에 '삭제'버튼을 클릭합니다.
 - **모두 삭제 :** 현재 등록된 모든 Black list가 삭제됩니다.
- 다른 장치에 적용 :** 현재 black list를 다른 장치에 적용합니다.

5.9. BioEntry 장치 관리

장치 리스트에서 장치를 선택하면, 선택된 장치의 장치 관리 윈도우가 주 윈도우에서 갱신됩니다.



장치 관리 윈도우는 2개 영역으로 나누어 집니다.

- 장치 정보

장치 정보는 선택된 장치의 형태, 이름, 고유 번호, 펌웨어 버전을 표시합니다.

- 환경설정 윈도우

환경설정 윈도우는 선택된 BioEntry 장치의 현재 환경설정 값을 보여줍니다. 또한 이 윈도우에는 변경된 환경설정 값 들도 보여줍니다. 환경설정 메뉴들은 시스템 설정, 입출력 설정, LED/비프 음 설정, Wiegand 설정과 스마트 카드 등을 나타내는 분리된 탭들로 구성되어 있습니다.

5.9.1. 장치정보

선택한 BioEntry의 장치 이름, 장치 종류 및 단말기 ID와 펌웨어 버전을 확인할 수 있습니다. 단말기 ID 번호와 펌웨어 버전 등은 설치 후 기술 지원 등에서 제품을 확인하기 위해 필요한 정보입니다.

5.9.2. 시스템 설정

시스템 탭을 선택하면 시스템 설정 페이지가 주 윈도우에서 갱신되며, 아래의 주요 설정 값을 변경할 수 있습니다.

시스템		입출력	LED/비프음	Wiegand	스마트카드
운영 모드	Both	통신 속도	115200*		
영상 품질	Moderate*	보안 등급	Auto Normal*		
스캔 대기시간	10 sec*	센서 감도	7*(Highest)		
고속 인증모드	5(Fastest)	인증 제한시간	Infinite*		

- 운영 모드
 - 1:1 인증: BioEntry Smart 에서 1:1 인증 모드를 선택하면 사용자의 스마트 카드를 먼저 제시하고, 그 후 지문으로 본인 인증을 하게 됩니다. BioEntry Pass 의 경우에는 ID 카드와 같은 외부 장치로부터 Wiegand 입력과 사용자의 지문으로 본인 인증을 진행합니다.
 - 1:N 인식: 1:N 인식 모드에서는 사용자의 지문 만으로 본인 인증을 하게 됩니다. 장치는 항상 지문 센서가 입력 대기상태여서 손가락만 대면 자동으로 1:N 인식을 시작합니다.
 - 양쪽 모두: 1:1 인증과 1:N 인식 모두 지원됩니다.
- 통신속도

통신속도는 반송 파가 1초당 상태를 바꾸는 횟수를 나타냅니다. 장치와 통신 하는데 문제가 발생하면, 통신속도를 좀 더 낮은 값으로 바꾸는 것이 해결책 이 될 수도 있습니다.
- 영상 품질

입력되는 지문의 영상 품질이 일정 수준 이상인지를 판별하는 기준을 결정합니다. Weak, Moderate, Strong, Strongest 중에서 선택하시면 됩니다. 초기 설정 값은 Moderate 입니다.
- 보안 등급

보안 등급 메뉴에서 FAR(타인 수락 율, False Acceptance Ratio)을 지정할 수 있습니다. 이 값을 1/100,000으로 지정하면 잘못된 지문을 받아들일 확률이 1/100,000이라는 것을 의미합니다. FAR과 FRR(False Rejection Ratio)은 서로 반비례 관계이기 때문에 보안등급을 높이면 보안성은 높아지지만 FRR(본인 거부 율, False Reject Ratio)이 증가하여 거부 율이 올라갈 수 있습니다. 초기

설정 값은 Auto Normal입니다.

- 스캔 대기시간

지문 입력 시 대기시간을 말합니다. 이 시간 내에 사용자가 지문을 입력하지 않거나 카드를 대지 않으면 입력 실패로 판단합니다. 기본 설정 값은 10초입니다.

- 센서 감도

센서 감도는 손가락을 감지하는 센서의 감도를 정하게 됩니다. 높은 감도에서는 손가락 입력을 좀 더 쉽게 받아들여지게 됩니다. 반면, 감도를 낮추면 지문을 일정 영역 이상 입력을 해야 캡처가 되므로 입력 지문 영상이 보다 안정적이 됩니다. 광학식 모델의 경우에는 감도 설정 값을 낮게 함으로서 햇빛에 대한 감도를 완화시킬 수 있습니다. 기본 설정 값은 7(최대)입니다.

- 고속 인증모드

수 백 개 이상의 지문이 장치에 저장되어 있을 경우, 1:N 인식 대기시간이 길어질 수 있습니다. 고속 인증 모드를 적용하면 인증 성능이 다소 떨어지는 대신 1:N 인식 시간을 단축시킬 수 있습니다. FAR는 이 설정 값의 영향을 받지 않으나 FRR는 정상 모드보다 다소 높아질 수 있습니다. 전형적인 경우에는, 고속 인증모드 1이 정상 모드보다 두세 배 빠르고 고속 인증모드 5는 5 ~ 6 배 빠릅니다. 기본 설정 값은 0입니다.

- 인증 제한시간

1:N 인식을 위한 대기시간을 말합니다. 이 시간 내에 인식 과정이 완료되지 않으면, 오류로 판단합니다.

- 시스템 초기 설정 값

BioEntry 장치에 대한 시스템 초기 설정 값은 다음과 같습니다.

	초기 설정 값	선택 가능한 값
사용 모드	1:1 인증 (BioEntry Smart) 1:N 인증 (BioEntry Pass)	1:1 인증 1:N 인식 양쪽 모두
보안 등급	Auto Normal	1/1,000 3/10,000 1/10,000 3/100,000 1/100,000 3/1,000,000 1/1,000,000 3/10,000,000 1/10,000,000 3/100,000,000 1/100,000,000 Auto Normal Auto Secure Auto More Secure
영상 품질	Moderate	Weak Moderate Stronger Strongest
센서 감도	7	0(가장 낮을 때) to

		7(가장 높을 때)
스캔 대기시간	10 sec	1초에서 20초 또는 infinite(무한대)
인증 제한시간	Infinite(무한대)	1초에서 20초 또는 infinite(무한대)
고속 인증모드	0(Normal)	0(Normal) to 5(Fastest)

5.9.3. 입출력 설정

장치는 외부 장치와 접속할 수 있는 각각 두 개씩의 프로그램 가능한 입력과 출력을 제공합니다. 이 탭이 선택되면, 입출력 설정 페이지가 주 윈도우에서 갱신됩니다.

The screenshot shows the '입출력' (I/O) configuration window. It is divided into sections for '입력 0', '입력 1', '출력 0', and '출력 1'.
 - '입력 0': 기능 (Function) is 'No Action', 최소 입력시간 (Min Input Time) is 100 ms.
 - '입력 1': 기능 (Function) is 'No Action', 최소 입력시간 (Min Input Time) is 100 ms.
 - '출력 0': 설정 이벤트 (Set Event) list includes Enroll Success, Enroll Fail, Verify Success, Verify Fail, Identify Success. 해제 이벤트 (Release Event) list is empty. 지연(ms) (Delay) is 0, 켜짐(ms) (Dwell) is 0, 꺼짐(ms) (Pulse Width) is 0, 반복횟수 (Repetition Count) is 0.
 - '출력 1': 설정 이벤트 (Set Event) list includes Enroll Success, Enroll Fail, Delete Success, Delete Fail, Identify Not Granted. 해제 이벤트 (Release Event) list includes Verify Success, Verify Fail, Identify Success, Identify Fail, Verify Duress. 지연(ms) (Delay) is 0, 켜짐(ms) (Dwell) is 100, 꺼짐(ms) (Pulse Width) is 0, 반복횟수 (Repetition Count) is 1.
 Buttons at the bottom include '다시 가져오기' (Reset), '적용' (Apply), '다른 장치에 적용' (Apply to other device), and '기본값으로 변경' (Restore defaults).

- 입력 포트의 환경설정
입력 포트의 환경설정을 정하기 위해서는 이벤트와 최소 기간이 지정되어야 합니다. 이벤트란 입력 포트가 활성화될 때 해야 하는 기능을 말하고 최소 지속시간은 입력 포트를 활성화시키는 펄스의 최소 지속시간을 의미합니다.

- 입력 이벤트 설명

함수	설명
No Action	입력포트를 해제
Enroll by Scan	지문 스캔을 이용하여 등록을 초기화
Identify by Scan	지문 스캔을 이용하여 인식을 초기화
Delete by Scan	입력 지문을 인식하여 사용자를 제거
Delete All	모든 사용자 데이터를 삭제
Enroll by Wiegand ID	Wiegand 입력 포트에서 입력 받은 사용자 ID를

	스캔 하여 등록
Verify by Wiegand ID	Wiegand 입력 포트에서 입력 받은 지문 스캔으로 등록
Delete by Wiegand ID	Wiegand 입력 포트에서 입력 받은 사용자 ID를 가진 사용자를 제거
Controller Reject	컨트롤러로부터 온 신호를 거부하기 위한 입력
Controller Accept	컨트롤러로부터 온 신호를 수락하기 위한 입력
Software Reset	소프트웨어 리셋

▪ 입력 포트에 대한 프로그램 예제

사용자가 Wiegand 입력으로부터 입력된 사용자 ID를 이용한 등록을 초기화 하기 위해 입력 버튼에 연결하고 싶다면, 다음 과정이 필요합니다.

입력 포트 0을 사용한다고 가정하고 함수를 활성화하기 위해 적어도 500 ms 동안 버튼을 눌러야 합니다.

우선, 장치 리스트 윈도우에서 해당 장치를 선택하십시오.

입력 포트 0의 함수를 Enroll by Wiegand ID로 선택합니다..

입력 포트 0의 최소 입력시간에 500을 입력합니다.

새로운 환경설정을 해당 장치에 전송하기 위해 적용 버튼을 누릅니다.

● 출력 포트 환경설정

출력 포트를 설정할 때, 각 이벤트에 대해 다른 출력 양식을 생성하기 위해 다수의 함수를 프로그램 할 수 있습니다. 이벤트란 출력 포트를 활성화한 시간과 방법을 의미하며 각각 프로그램 하는 과정은 다음과 같습니다.:

- 해제된 이벤트에서 이벤트를 선택하여 필요한 이벤트를 설정합니다.
- 지연, 켜짐, 꺼짐과 반복횟수 칸에 값을 입력하여 출력 양식을 정합니다.

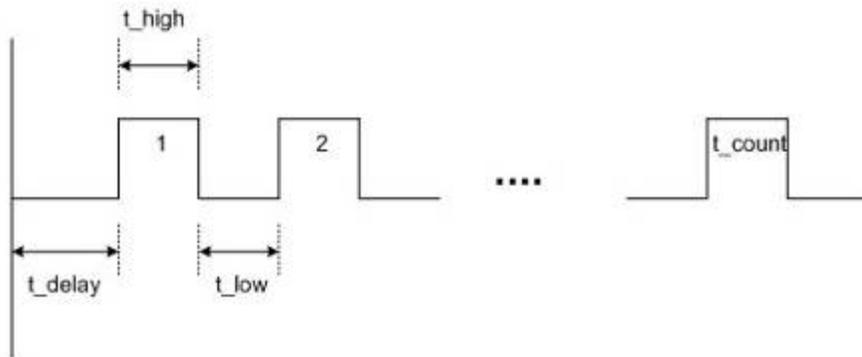
● 출력 이벤트 설명

이벤트	설명(출력 포트가 활성화 될 때)
Enroll Success	사용자가 장치에 성공적으로 등록될 때
Enroll Fail	등록이 실패했을 때
Identify Success	인식이 성공적으로 수행될 때
Identify Fail	장치가 일치하는 사용자를 찾지 못했을 때
Verify Success	인증이 성공적으로 수행될 때
Verify Fail	사용자가 인증되지 못했을 때
Delete Success	사용자 제거가 성공적으로 수행됐을 때
Identify Not Granted	인식을 성공했으나 입장은 거부됐을 때
Verify Not Granted	인증을 성공했으나 입장은 거부됐을 때
Delete Fail	사용자 제거에 실패했을 때
Verify Duress	협박모드용 손가락이 인증됐을 때
Identify Duress	인식된 손가락이 협박모드용 손가락일 때
Temper Switch On	장치의 온도 스위치가 활성화 되었다는 것이 장치가 열려있다는 것을 의미할 때
Command Card Success	명령 카드 동작이 성공적으로 끝났을 때
Command Card Fail	명령 카드 동작이 실패했을 때
Controller Reject	컨트롤러 거부 함수가 지정된 입력 포트가 활성화됐을 때

Controller Accept	컨트롤러 수락 함수가 지정된 입력 포트가 활성화됐을 때
Detect Input 0	지정된 함수와 관계없이 입력 포트 0이 활성화됐을 때
Detect Input 1	지정된 함수와 관계없이 입력 포트 1이 활성화됐을 때

● 출력 양식 설명

각 설정된 이벤트에서는, 아래 그림에서와 같은 의미를 갖는 4개의 설정 값을 이용하여 출력 양식을 융통성 있게 기술할 수 있습니다.



매개 변수	의 미	허 용 값
Delay	출력 펄스(msec)가 발생되기 전 초기 지연 값	0 ~ 65535
High duration	높은 상태에서 펄스의 지속시간 (msec)	0 ~ 65534 65535 : 새로운 출력 이벤트가 나타날 때까지 계속 활성화
Low duration	연속된 펄스에서 신호 출력이 낮은 상태일 때 간격	0 ~ 65535
Count	펄스들의 수	0 : 새로운 출력 이벤트가 나타날 때까지 무한 반복 1 ~ 255

■ 출력 양식 작성 예

사용자가 출력 포트 0 에서 다음 유형들이 발생하면 경고 신호를 지정하고 싶다고 가정합니다.:

협박 모드용 손가락 인식 또는 인증했을 때, 장치는 5초간 깜박이는 출력을 보냅니다.

온도 스위치가 켜져 있을 때, 장치는 10초간 지속적인 출력을 보냅니다.

프로그래밍 과정은 다음과 같습니다.:

우선, 네트워크 윈도우에서 대상 장치를 선택합니다.

출력 0 에서 현재 선택된 이벤트들을 설정 구역에서 해제 구역으로 옮겨 해제시킵니다.

다음과 같은 출력 양식 설정 값에 값을 입력하여 각 이벤트를 설정하여 필요한 이벤트를 프로그램 합니다.

설정할 이벤트	출력 양식 설정 값
Verify Duress	Delay : 0 High : 500 Low : 500 Count : 5
Identify Duress	Delay : 0 High : 500 Low : 500 Count : 5
Tamper Switch On	Delay : 0 High : 10000 Low : 0 Count : 1

해당 장치에 새로운 설정 값을 전송하려면 적용 버튼을 누릅니다.

5.9.4. LED / 비프 음 설정

BioEntry 장치에는 사용자들에게 처리 상태와 결과를 알려주기 위해 두 개의 LED와 한 개의 비프가 있습니다. 두 개의 LED의 색상은 3개의 색상 즉 녹색, 빨강과 황색을 나타내도록 혼합되어 있습니다. LED/비프 음 탭을 선택하면 LED/비프 음 환경설정 페이지가 주 윈도우에 갱신됩니다.



● LED/비프 음 설정

LED와 비프 음을 작성하는 방법은 출력 환경설정과 비슷합니다. 아래 리스트에서는 LED와 비프 음에 대한 이벤트를 선택할 수 있습니다.

이벤트	설명 (출력 포트가 활성화됐을 때)
Enroll Wait Finger	장치가 등록할 손가락을 스캔 하기 위해 대기 중 일 때
Enroll Processing	장치가 등록 과정 중일 때
Identify Wait Finger	장치가 인식하기 위해 손가락을 스캔 하려고 대기 중일 때
Identify Processing	장치가 인식 과정 중일 때
Verify Wait Finger	장치가 인증하기 위해 손가락을 스캔 하려고 대기 중일 때
Verify Processing	장치가 인증 과정 중 일 때
Delete Wait Finger	장치가 삭제하려는 손가락을 스캔 하기 위해 대기 중 일 때

● LED/비프 음 기본 설정에 대한 설명

현재 상태와 처리 결과를 보여주기 위해, 다양한 출력 양식 설정 값들이 다음과 같은 초기 설정 값으로 LED와 비프 음에 대해 설정되어 있습니다. 기본값으로 설정된 LED / 비프 음에 대한 설명은 아래 리스트와 같습니다.

이벤트	LED	비프 음
Enroll Wait Finger	황색이 느리게 점멸	없음
Verify Wait Finger	황색이 빠르게 점멸	없음
Identify Wait Finger	황색이 느리게 점멸	없음

Delete Wait Finger	황색이 빠르게 점멸	없음
Enroll Processing Identify Processing Verify Processing	황색이 계속 나타남	없음
Enroll Success Verify Success Identify Success Delete Success Command Card Success Verify Duress Identify Duress	녹색이 계속 나타남	한 번의 비프 음
Enroll Fail Verify Fail Identify Fail Delete Fail Command Card Fail	빨강색이 계속 나타남	세 번의 짧은 비프 음
Waiting Smart Card Input	빨강색이 빠르게 점멸 (고정됨)	없음

5.9.5. Wiegand 설정

Wiegand 탭은 장치의 Wiegand 출력/입력 포맷을 관리하기 위해 사용됩니다. 이 메뉴를 선택하면 Wiegand 설정 페이지가 주 윈도우에 갱신됩니다.

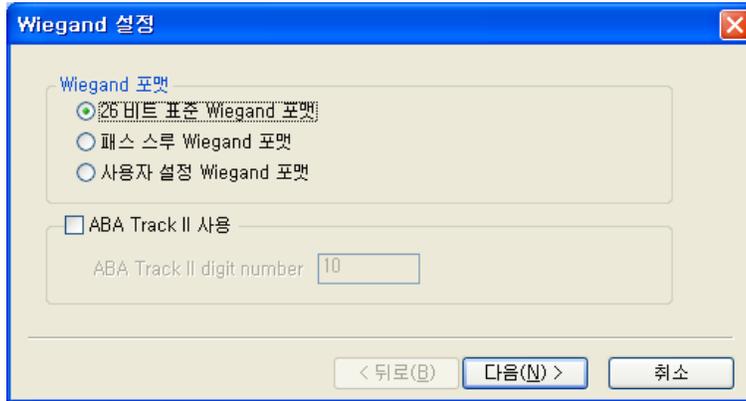
- Wiegand 포맷

Wiegand 설정 마법사를 이용하여 새로운 Wiegand 포맷을 설정할 수 있습니다. **포맷 변경** 버튼을 누르면 Wiegand 설정 마법사가 나타납니다.

첫 번째 페이지에서 지원되는 3개의 포맷 중 하나를 선택해야 합니다.

장치가 Wiegand 인터페이스가 아닌 ABA Track II 출력에 의해 컨트롤러에 연

결되면, Use ABA Track II를 선택해야 합니다. 그 경우에는 출력 신호가 ABA Track II 포맷이 됩니다. ABA Track II 출력의 문자 개수를 특정할 수 있습니다.



- 26 비트 표준 Wiegand 포맷

26 bit standard 형식은 가장 광범위하게 쓰이며 8비트 FC 코드와 16비트 ID로 구성됩니다. 26 bit standard 형식에서 비트 정의와 패리티 비트는 변경할 수 없습니다.

- 패스 스루 Wiegand 포맷

패스 스루 포맷은 ID 필드의 형식을 알고 있을 때만 사용됩니다. Wiegand 입력 문자열이 감지되면, 장치는 ID 비트들을 찾아내고 그 ID로 인증을 시작합니다. 인증이 성공하면 장치는 Wiegand 입력 문자열을 바꾸지 않고 출력합니다. 패리티 체크와 고급 옵션들은 이 형식에서는 무시됩니다. 정의에 따르면 패스 스루 포맷은 사용 모드가 1:1인 경우에만 유용하다고 합니다. 사용 모드가 1:N일 때는 ID 필드 이외에 비트 오더가 0으로 설정되어야 합니다.

가령 32비트 Pass Through format이 다음과 같다고 가정합니다.:

XIIIIIIII IIIIIIX XXXIIIIII IIIIIIX

(가장 왼쪽 비트가 0번째 비트, BIT0) I: Id field, X: Unknown field

이 형식을 다음과 같은 순서로 설정할 수 있습니다.



Total Bits 필드에 32를 입력합니다.

정의에 따라 ID 비트를 선택합니다.

Next 버튼을 누릅니다. 패스 스루 모드에서는 패리티 비트를 특정할 수 없습니다.

- 사용자 설정 Wiegand 포맷

사용자가 Wiegand 형식에 대한 모든 정보를 갖고 있다면, 맞춤 포맷을 정의할 수 있습니다. Wiegand 입력 문자열이 감지되면, 장치는 우선 패리티 비트를 확인합니다. 모든 패리티 비트가 정확하면 장치는 ID 비트를 추출하고 그 ID로 인증을 시작합니다. 사용자는 또한 각 필드를 대체 값으로 설정할 수 있고 Fail ID와 같은 고급 옵션을 설정할 수 있습니다. 인증에 성공하면 장치는 Wiegand 문자열을 출력합니다. 출력 문자열은 대체 값과 고급 옵션에 따라 입력 문자열과 다를 수 있습니다.

가령, 44비트 맞춤 포맷이 다음과 같이 구성되었다고 가정합니다:

EAAAAAAAA IIIIIIII IIIIIIII BBBBBI IIIIIIII IO

(가장 왼쪽 비트가 0번째 비트, BIT0)

E: Even parity for BIT1 ~ BIT22

O: Odd parity for BIT23 ~ BIT42

I: ID bits(Field1 and Field 3), A: Field 0, B: Field 2

이 형식을 다음과 같은 순서로 설정할 수 있습니다.



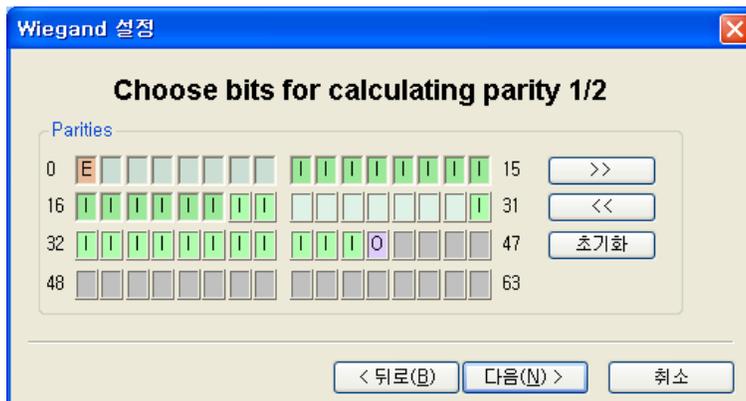
Total Bits 필드에 44를 입력합니다..

Even Parity를 선택합니다.

even parity bit를 누릅니다. 이 예제에서는 BIT0을 말합니다.

정의에 따라 **Odd Parity**와 **User ID**에 대해서 (2)와 (3)을 반복합니다.

Next 버튼을 누릅니다.



첫 번째 패리티 비트를 계산하는데 쓰이는 비트들을 누릅니다. 이 예제에서는 BIT1 ~ BIT22 입니다.

>> 버튼을 누릅니다.

두 번째 패리티 비트를 계산하는데 쓰이는 비트들을 누릅니다. 이 예제에서

는 BIT23~ BIT42 입니다.
Next 버튼을 누릅니다.

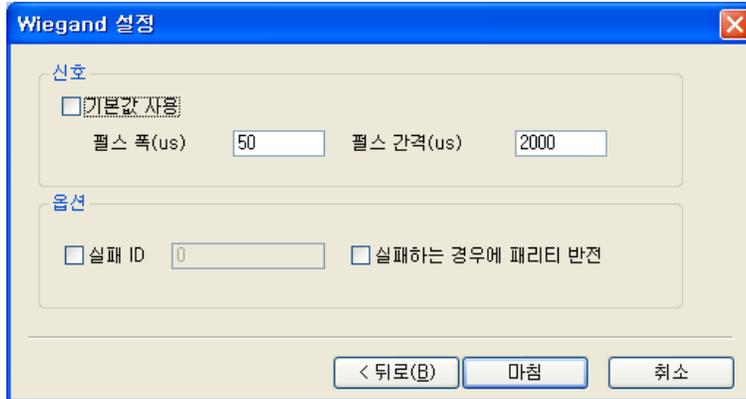
- 대체 값

26 비트 표준에서 다른 FC code를 특정할 수 있습니다. 맞춤 포맷에서는 non-ID 필드에서 대체 값을 특정할 수 있습니다. 대체 값이 설정되면 장치는 출력을 보내기 전에 해당 필드들을 이 대체 값으로 바꿉니다.



- 고급 옵션

마법사의 마지막 장에서 Wiegand 신호의 특징과 고급 옵션을 설정할 수 있습니다. 패스 스루 포맷에서는 고급 옵션을 설정할 수 없습니다.

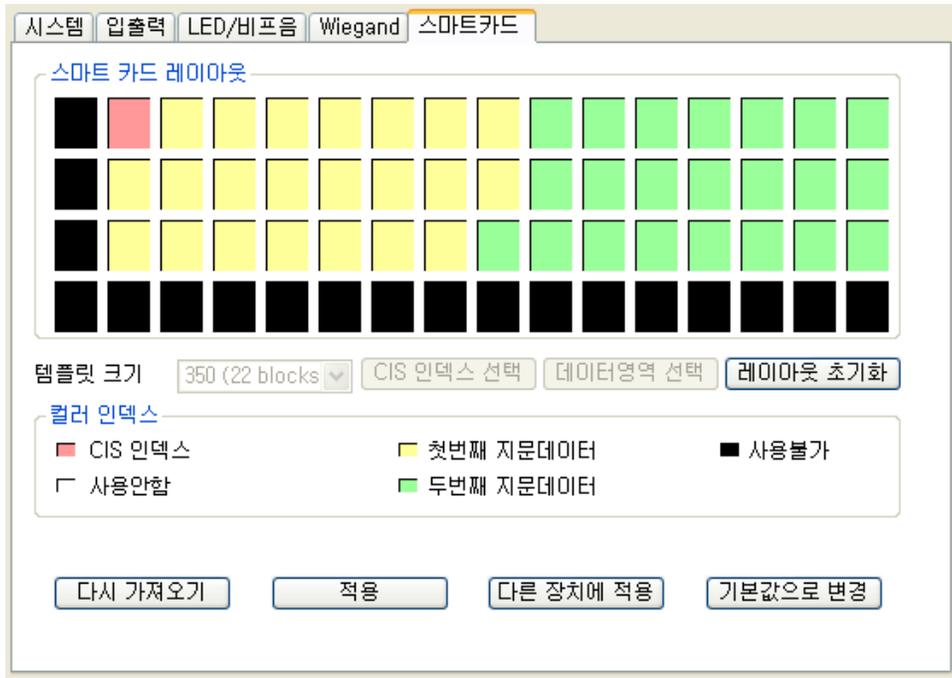


- 기본값 사용: Wiegand 신호에 대해 기본값들을 사용합니다.
- 펄스 폭: 펄스의 너비. 기본값은 50 us.
- 펄스 간격: 펄스의 간격. 기본값은 2000 us.
- 실패 ID: 정상적인 경우에는 인식이 성공하면 모듈이 Wiegand 신호를 출력합니다. 이 옵션이 표시되면, 인식이 실패할 경우 모듈은 실패 ID를 출력합니다.
- 실패하는 경우에 패리티 반전: 이 옵션이 표시되면, 인식이 실패할 경우 모듈은 Wiegand 신호를 출력합니다.

5.9.6. 스마트 카드 설정

스마트 카드 레이아웃 설정은 사용자 ID와 지문 정보를 포함하는 사용자 정보를 저장하기 위해 사용자의 스마트카드 위해 맞춤 영역을 정의하는 과정입니다. 스마트카드 메뉴를 선택하면, 스마트카드 레이아웃 페이지가 주 윈도우에 갱신됩니다.

Note: 레이아웃을 부적절하게 바꿀 경우 스마트카드를 쓸 수 없게 될 수 있기 때문에 고급 사용자들만 레이아웃을 변경할 것을 권고합니다. 레이아웃을 기본 설정으로부터 변경하기 위해 이장을 주의 깊게 읽어 보시기 바랍니다.



● 스마트카드 레이아웃 편집

- 지문인식정보 크기는 254에서 382까지 정할 수 있습니다. 제조사에서 지문인식정보 크기를 기본으로 카드에 두 개의 지문인식정보를 저장할 수 있는 350 바이트로 정하고 있습니다.
- CIS 인덱스 블록: 헤더 정보는 빨강색으로 칠해진 CIS 인덱스 블록에 저장됩니다.
- 지문인식정보 데이터 블록: 첫 번째 지문인식정보 데이터와 두 번째 지문인식정보 데이터에 대한 블록들. 각 지문인식정보 데이터에 대한 블록 개수는 지문인식정보 크기에 의해 정해집니다. 첫 번째 지문인식정보 데이터 블록들은 노란색, 두 번째 지문인식정보 데이터 블록들은 녹색으로 각각 그려집니다.
- 사용 안 함 블록: 레이아웃에서 정해지지 않은 빈 블록
- 사용 불가 블록: 사용할 수 없는 블록

● 편집 과정

고객의 레이아웃을 설정하기 위해 다음과 같은 과정이 필요합니다.

- 레이아웃 초기화 버튼을 눌러서 모든 블록 들을 사용되지 않는 것으로 초기합니다.
- 필요한 지문인식정보 크기를 선택합니다.
- CIS 인덱스 선택 버튼을 누르고 CIS 인덱스 블록을 선택하기 위해 미사용 블록을 클릭합니다.
- 데이터영역 선택 버튼을 누르고 지문인식정보 데이터의 시작 블록을 나타내는 미사용 블록을 클릭합니다. 그러면, 첫 번째 지문데이터 블록들이 선택된 시작 블록으로부터 자동적으로 정해집니다.
- 데이터영역 선택 버튼을 다시 누르고 두 번째 지문데이터의 시작 블록을 나타내는 미사용 블록을 클릭합니다.
- 적용 버튼은 스마트카드의 레이아웃을 선택된 장치들에게 전송합니다.

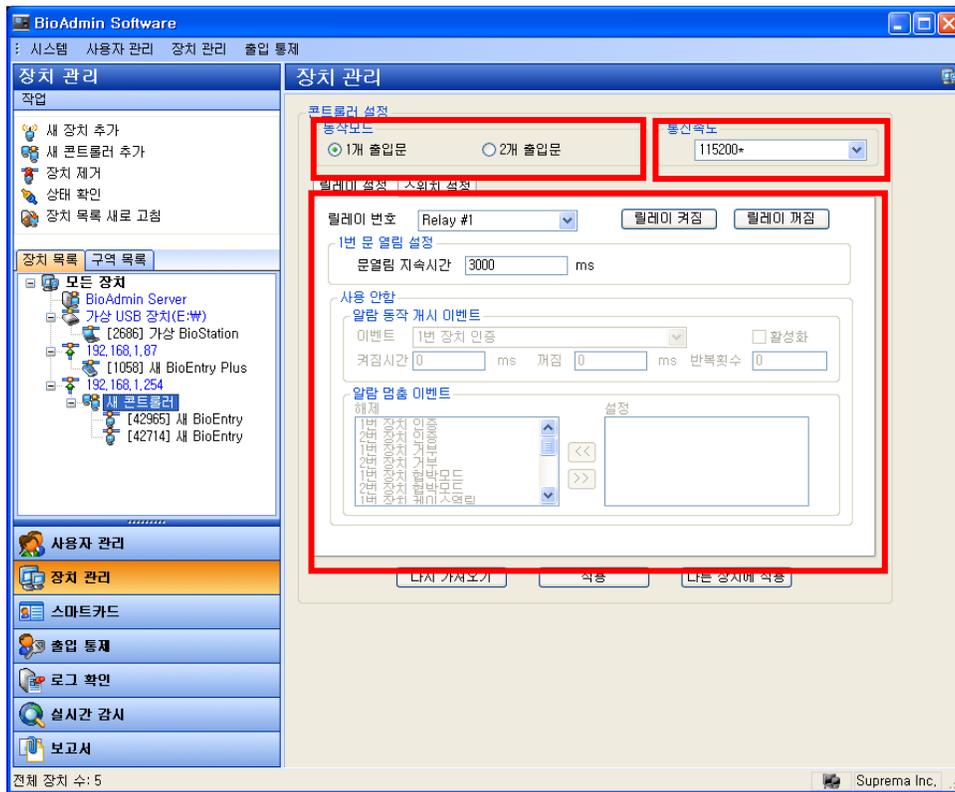
● 초기 설정 기본 레이아웃

스마트카드의 초기 설정 기본 레이아웃은 다음과 같습니다.



5.10. BEACon 환경설정

장치 리스트에서 BEACon 을 선택하면, 선택된 BEACon의 장치 설정 윈도우가 주 윈도우에서 갱신됩니다.



장치 설정 윈도우는 3개의 영역으로 나뉘어 집니다.:

- 동작 모드
BEACon 은 두 개 출입문까지 통제할 수 있습니다. 동작 모드 윈도우는 선택된 BEACon 이 한 개 출입문과 두 개 출입문 중 어느 모드로 설정되었는지 보여줍니다.
- 통신속도
통신속도 윈도우는 선택된 BEACon 의 전송 속도를 보여줍니다. BEACon 의 통신속도는 BioEntry의 통신속도와 일치하여야 합니다.
- 환경설정 윈도우
환경설정 윈도우는 선택된 BEACon의 현재 설정을 보여줍니다. 또한 이 윈도우에서는 설정이 변경되었는지도 보여줍니다. 환경설정 메뉴는 BEACon 릴레이 설정과 BEACon 스위치 설정 탭들로 나뉘어 있습니다.

BEACon의 구체적인 작동에 대해서는, BEACon 사용 설명서를 참조하시기 바랍니다.

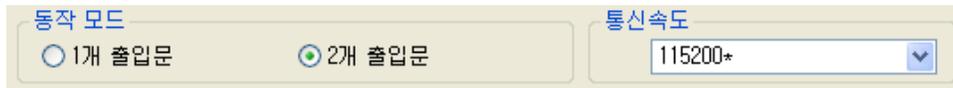
5.10.1. 동작 모드

BEACon은 두 개의 출입문까지 통제할 수 있습니다. 동작 모드 윈도우는 선택된 BEACon이 한 개 출입문 또는 두 개 출입문 중 어느 모드로 설정되어 있는지 보여줍니다.

5.10.2. 통신속도

통신속도 윈도우는 선택된 BEACon의 전송 속도를 보여줍니다.

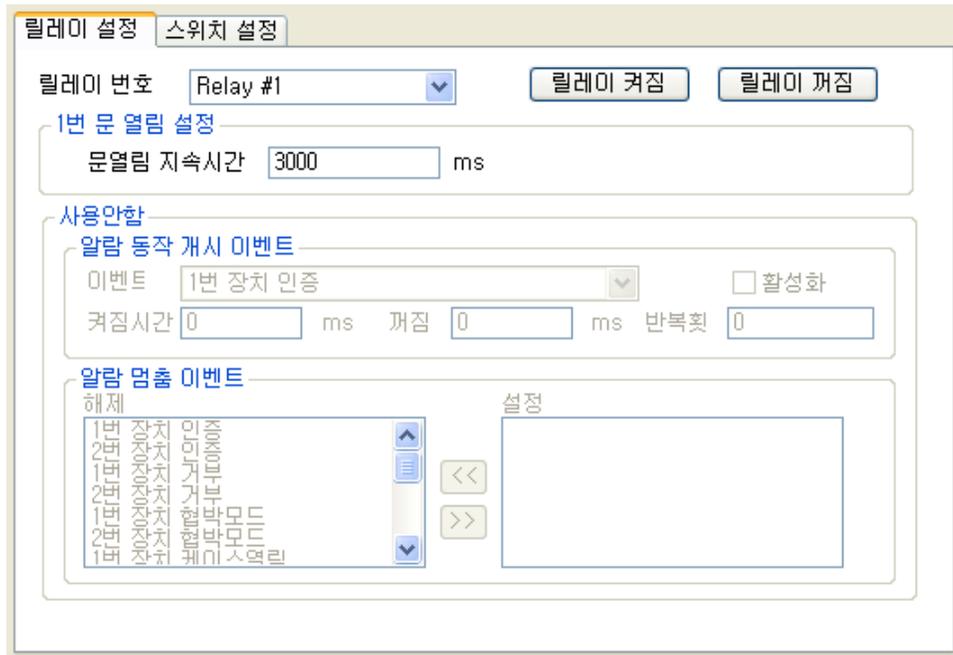
- 이 메뉴에서 통신속도를 변경하면, BEACon과 호스트PC사이의 전송 속도가 바뀌게 될 것입니다.
- 일단 BEACon의 통신속도를 변경하면, BEACon의 변경된 통신속도에 장치의 통신속도를 일치시켜야 합니다.



5.10.3. BEACon 릴레이 설정

이 메뉴에서는 BEACon의 릴레이 설정을 변경할 수 있습니다. BEACon 작동 모드에 따라 릴레이 설정은 다르게 설정될 수 있습니다.

- 한 개 출입문 모드에서, 첫 번째 릴레이는 자동적으로 출입문 개방에 설정됩니다. 그러므로 두 번째, 세 번째와 네 번째 릴레이를 경보로 설정할 수 있습니다.
- 두 개 출입문 모드에서, 첫 번째와 두 번째 릴레이는 자동적으로 출입문 개방에 설정됩니다. 세 번째와 네 번째 릴레이를 경보로 설정할 수 있습니다.



상세한 동작은 다음과 같습니다.

- 설정을 하기 위해 릴레이를 선택합니다. 릴레이를 선택하면, 선택된 릴레이에 대해 적용할 수 있는 항목들이 릴레이 설정 윈도우에서 활성화됩니다.
- 릴레이 켜짐 / 릴레이 꺼짐 버튼을 누르면 릴레이를 개방/폐쇄 할 수 있습니다

릴레이 번호

● 문 열림 설정

문 열림 시간을 입력합니다. 일단 출입문이 해제되면, 지정된 문 열림 시간이 지난 후에 출입문은 다시 잠길 수 있습니다.

1번 문 열림 설정

문열림 지속시간 ms

● 알람 동작 개시 이벤트

이벤트 체크 박스를 표시하면 콤보 박스상에서 경고 켜짐 이벤트를 선택할 수 있습니다. 경고 빈도를 설정하기 위해 켜짐 시간, 꺼짐, 반복횟수를 입력합니다. 알람 켜짐 이벤트들 중 어느 것이라도 발생하면, 지정된 빈도만큼 경보가 활성화됩니다.

1번 경고 설정

알람 동작 개시 이벤트

이벤트 활성화

켜짐시간 ms 꺼짐 ms 반복횟

● 알람 멈춤 이벤트:

알람 멈춤 이벤트를 선택하십시오. 해제된 이벤트 리스트에서 이벤트를 더블 클릭 하면 간단히 알람 꺼짐 이벤트를 활성화할 수 있습니다. 알람 멈춤 이벤트 중에서 어느 것이라도 발생하면, 지속시간이나 펄스 수가 남아있는 것에 관계없이 경보가 비활성 될 것입니다.

알람 멈춤 이벤트

해제	설정
1번 장치 인증	
2번 장치 인증	
1번 장치 인증	
2번 장치 인증	
1번 장치 인증	
2번 장치 인증	
1번 장치 인증	

이벤트 리스트: 1번 장치 인증, 2번 장치 인증, 1번 장치 인증, 2번 장치 인증, 1번 장치 인증, 2번 장치 인증, 1번 장치 인증

이벤트 선택: 이중모드, 이중모드, 이중모드, 이중모드, 이중모드, 이중모드, 이중모드

이벤트 이동: << >>

5.10.4. 스위치 설정

이 메뉴에서는 BEACon 스위치 설정을 변경할 수 있습니다. BEACon 의 작동 모드에 따라서 스위치 설정은 다르게 설정될 수 있습니다.

- 한 개 출입문 모드에서 첫 번째 스위치는 출입문 센서로 세 번째 스위치는 문 나가기 버튼으로 자동적으로 설정됩니다. 따라서 두 번째, 네 번째, 다섯 번째와 여섯 번째 스위치는 정상 스위치 설정에서 그 밖의 다양한 기능에 설정할 수 있습니다.
- 두 개 출입문 모드에서 첫 번째와 두 번째 스위치는 출입문 센서로 자동적으로

로 설정됩니다. 또한 세 번째와 네 번째 스위치는 문 나가기 버튼으로 자동적으로 설정됩니다. 따라서 다섯 번째와 여섯 번째 스위치는 정상 스위치 설정에서 그 밖의 다양한 기능에 설정할 수 있습니다.

- 설정할 스위치를 선택합니다. 일단 스위치를 선택하면, 선택된 스위치에 대해 적용 가능한 항목들이 스위치 설정 윈도우에 활성화될 것입니다.

스위치 스위치형태

- 출입문 상태 설정
출입문 센서 스위치를 선택하면, 연결된 BEACon의 자동 잠금 시간과 장시간 문 열림 시간을 설정할 수 있습니다. 출입문이 닫혀 있다면, 정해진 자동 잠금 시간 후에 출입문은 잠길 것입니다. 출입문이 정해진 장시간 문 열림 시간 이상 열려 있다면, 장시간 문 열림 이벤트가 발생할 것입니다.

- 출입문 문 나가기 버튼 설정
문 나가기 버튼 스위치를 선택하면 최소 입력 시간을 설정할 수 있습니다. 문 나가기 버튼 스위치가 정해진 최소 입력 시간 이상 활성화되었다면, 출입문은 개방될 것입니다.

1번 문 나가기 버튼 설정

최소입력시 ms

- 일반 스위치 설정

남아 있는 스위치들에 대해서 기능 해제, 케이스 열림, 경보 해제 등 과 같은 다양한 기능들을 설정할 수 있습니다. 스위치가 정해진 최소입력시간 이상 활성화되었다면, 선택된 기능이 수행될 것입니다.

일반 스위치 설정

기능 ▼
최소입력시 ms

5.10.5. 다시 가져오기 / 적용 / 다른 장치에 적용

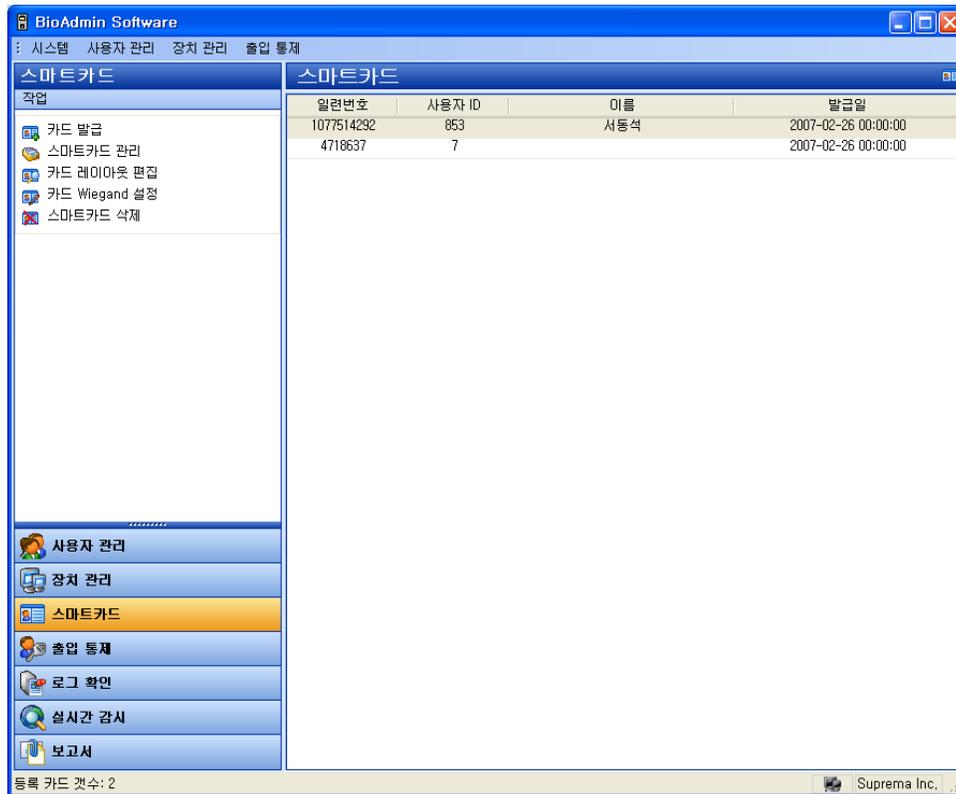
- 다시 가져오기: 적용 버튼을 누르기 전에 다시 가져오기 버튼을 눌러 원래 설정을 복구할 수 있습니다.
- 적용: 설정을 변경한 후에 저장하려면 적용 버튼을 눌러야 합니다.
- 다른 장치에 적용: 다른 장치에 적용 버튼을 누르면 변경된 설정사항을 다른 장치들로 전송할 수 있습니다.

6. 스마트 카드 / Mifare 카드

스마트카드 메뉴는 BioEntry™ 관리 소프트웨어에서 발급한 스마트카드의 리스트를 볼 수 있는 메뉴입니다. 사용자 관리 메뉴에서 발급한 사용자들의 스마트카드들이 자동으로 이 메뉴의 스마트카드 리스트에 표시됩니다.

스마트카드 메뉴는 다음 동작들을 포함합니다.:

- 카드 발급
- 스마트 카드 관리
- 카드 레이아웃 설정
- 카드 Wiegand 설정
- 스마트카드 삭제



6.1. 스마트카드 페이지의 구성

스마트카드 메뉴를 선택하면, 스마트카드 관리 페이지가 메인 윈도우에 갱신됩니다.

스마트카드 페이지는 다음 2개의 영역으로 구성되어 있습니다.

- 스마트카드 리스트

호스트 PC가 스마트카드 데이터베이스를 주로 관리합니다. 스마트카드 리스트에는 BioAdmin 소프트웨어에서 발급한 스마트카드의 상세한 리스트가 있습니다.

- 작업 박스

작업 박스에는 스마트카드 페이지의 기본 동작들을 제어하는 버튼들이 있습니다.

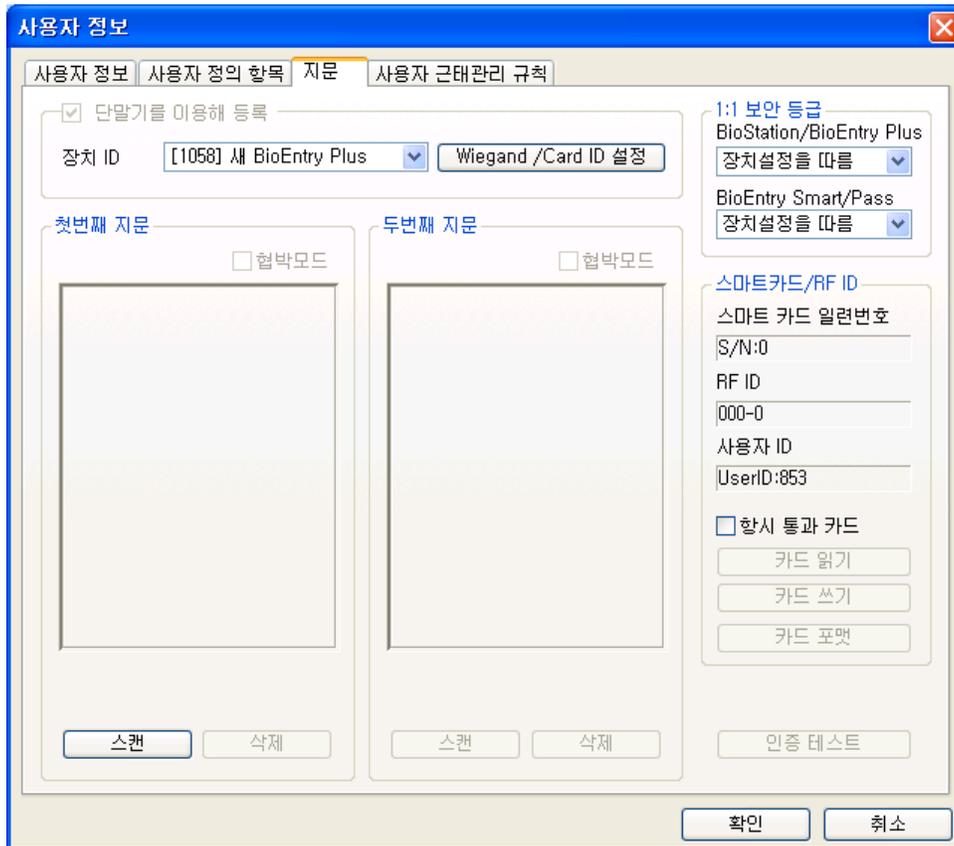
6.2. 스마트카드 리스트

스마트카드 리스트에는 스마트카드에 대한 다음 사항이 포함됩니다.

- 카드 번호
- 사용자 ID
- 사용자 이름
- 발급 날짜
- 유효 기일

6.3. 카드 발급

카드 발급 메뉴는 사용자의 스마트카드를 발급하는 팝업 윈도우를 활성화합니다. 상세한 동작에 대해서는 사용자 관리 메뉴에 있는 발급 과정을 참조하시기 바랍니다.



6.4. 스마트카드 관리

스마트카드 관리 메뉴는 스마트카드의 정보를 읽고 스마트카드를 포맷하기 위한 팝업 윈도우를 활성화합니다. 이 윈도우에서 일련번호, Wiegand 문자열(가능하다면), 사용자 ID, 보안 등급, 사용자 이름, 출입 그룹과 지문인식정보 데이터와 같은 스마트카드 정보를 확인할 수 있습니다.

USB 스마트카드 Reader./Writer가 없다면, **BioEntry**를 이용해 등록 에 표시하여 BioEntry를 통해 직접 스마트카드 정보를 읽을 수 있습니다.



6.4.1. 발급된 스마트카드 읽기

스마트카드 윈도우에서는, 발급된 스마트카드에 저장된 정보를 제5장 사용자 관리 편에서 설명된 읽어오기 과정과 비슷한 방법으로 불러올 수 있습니다.

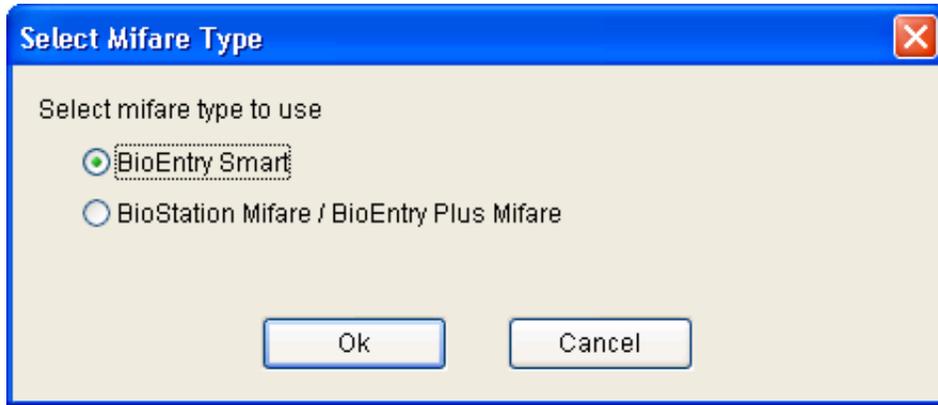
6.4.2. 스마트카드 포맷

스마트카드 윈도우에서는, 제5장 사용자 관리 편에서 설명된 포맷하기 과정과 비슷한 방법으로 포맷할 수 있습니다.

6.5. 카드 레이아웃 편집

스마트카드 레이아웃 편집은 지문인식정보를 포함한 사용자 정보를 저장할 사용자의 스마트카드의 맞춤 섹터를 설정하는 과정입니다. **스마트카드 설정** 버튼을 선택하면 스마트카드 레이아웃 페이지가 주 윈도우에 갱신됩니다. **레이아웃을 잘못 변경하면 스마트카드를 사용할 수 없을 수도 있으니 능숙한 사용자들만 시도하시기 바랍니다. 기본 설정에서 레이아웃을 변경하려면 이 장의 설명을 주의 깊게 읽어보시기 바랍니다.**

6.5.1. Mifare 설정



Layout을 편집하려는 형식을 선택합니다. 이 항목에서 선택하는 사항과 Preference에서 선택하는 Mifare Type과는 서로 상관이 없으며 단지 편집하려고 하는 Type만 선택하는 절차입니다.

6.5.2. 스마트카드 레이아웃 편집



스마트카드 레이아웃 설정 페이지는 3개 영역으로 나누어집니다:

- 스마트카드 레이아웃
호스트 PC에 연결된 스마트카드 읽기/쓰기 장치의 스마트카드 레이아웃을 보여줍니다.
- 스마트카드 레이아웃
현재 선택된 리더의 이름과 그 레이아웃을 보여줍니다. 그룹이나 모든 리더들이 선택하면 그 내용이 유효하지 않습니다.
- 새로운 설정
이 색서는 리더들과 사용자 스마트카드에 적용되는 새로운 레이아웃을 편집하

기 위해 사용됩니다.

- 레이아웃을 관리하기 위한 제어 값
다른 장치에 적용 버튼은 선택된 BioEntry 리더, 선택된 그룹 또는 모든 BioEntry™ 리더들에게 새로운 레이아웃을 전송합니다. 또한 레이아웃을 편집하기 위해 몇 개의 control 버튼들이 있습니다.

6.5.3. 지문 데이터 크기

지문인식정보 크기는 254에서 382까지 조정 가능합니다. 지문 데이터 크기는 초기 설정 값으로 카드에 두 개의 지문인식정보를 저장할 수 있는 350 바이트로 설정되어 있습니다.

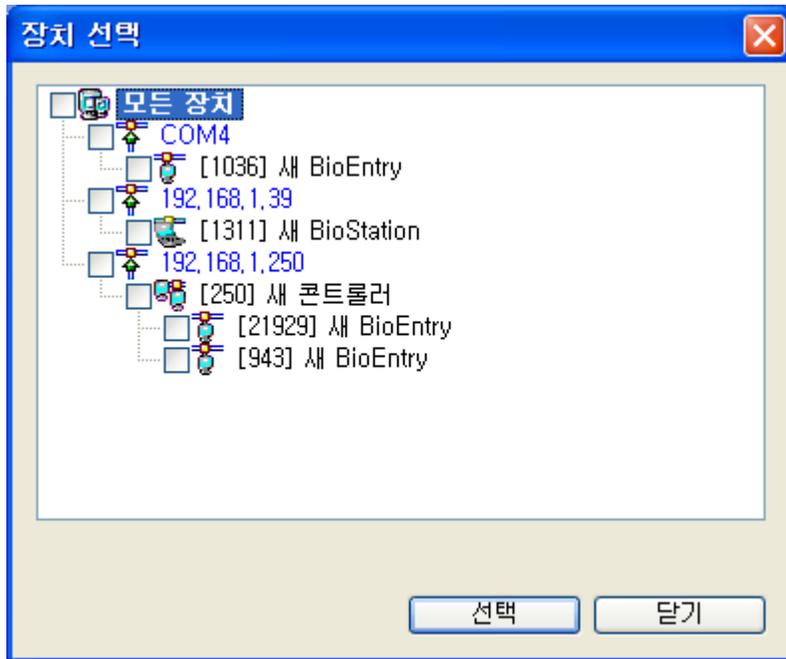
6.5.4. 블록

- CIS 인덱스 블록: 헤더 정보는 빨간색으로 표시된 CIS 인덱스 블록에 저장됩니다.
- 지문인식정보 데이터 블록: 첫 번째와 두 번째 지문인식정보 데이터를 위한 블록들. 각 지문인식정보 데이터의 블록 수는 지문인식정보 크기에 의해 정해집니다. 첫 번째 지문인식정보 데이터는 노란색, 두 번째 지문인식정보 데이터는 녹색으로 각각 표시됩니다.
- 미사용 블록: 레이아웃에서 정의되지 않은 빈 블록
- 사용불가 블록: 사용 금지된 블록.

6.5.5. 편집과정

고객의 레이아웃을 설정하기 위해, 다음 과정이 필요합니다.

- 레이아웃 초기화 버튼을 눌러 사용되지 않는 모든 블록 들을 초기합니다.
- 필요한 지문인식정보 크기를 선택합니다.
- CIS Index 선택 버튼을 누르고 CIS 인덱스 블록을 선택하기 위해 미사용 블록을 클릭합니다.
- 데이터 영역 선택 버튼을 누르고 첫 번째 지문인식정보 데이터의 시작 블록을 표시하기 위해 미사용 블록을 클릭합니다. 그러면 첫 번째 지문인식정보 데이터의 블록들이 시작 블록들로부터 자동으로 정해집니다.
- 데이터 영역 선택 버튼을 다시 누르고 두 번째 지문인식정보 데이터의 시작 블록을 표시하기 위해 미사용 블록을 클릭합니다.
- 새로운 스마트 카드의 레이아웃을 선택된 리더로 전송하기 위해 다른 장치에 적용 버튼을 누릅니다.



- 스마트카드 레이아웃 윈도우는 BioEntry Smart 모델을 위해서만 활성화됩니다. BioEntry Pass 또는 BioStation 이 선택되면 이 메뉴는 비활성화될 것입니다.
- 새로운 스마트카드 레이아웃을 PC USB 스마트카드 reader/writer에 저장하기 위해 **확인** 버튼을 누릅니다.
- 저장된 레이아웃은 PC USB 스마트카드 reader/writer를 사용하여 새로운 스마트카드를 발급할 때 적용됩니다.

6.5.6. 초기 설정 레이아웃

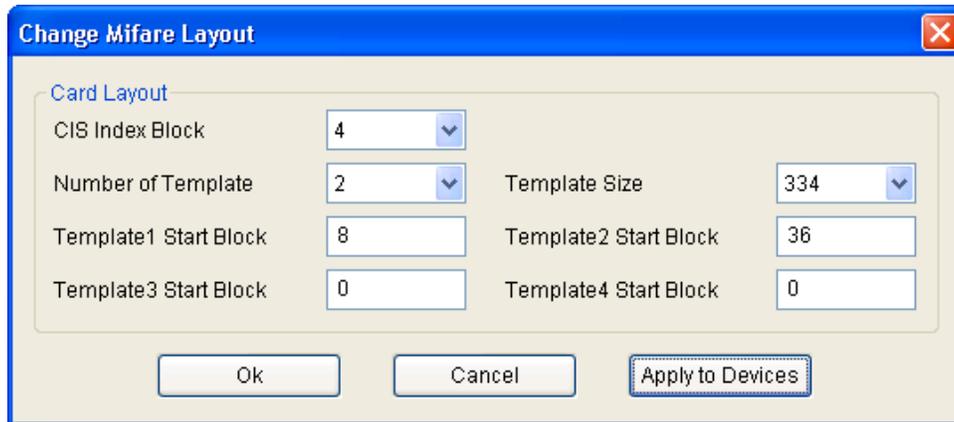
초기 설정 스마트카드 레이아웃은 다음과 같습니다.

0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62
3	7	11	15	19	23	27	31	35	39	43	47	51	55	59	63

CIS 인덱스 첫번째 지문 데이터 사용불가
 사용안함 두번째 지문 데이터

6.5.7. Mifare 카드 레이아웃 설정 (BioStation / BioEntry Plus)

Mifare 카드 레이아웃 설정 화면은 4K 카드 지원을 위해 블록을 표시하지 않고 수치로 입력하도록 되어 있습니다.

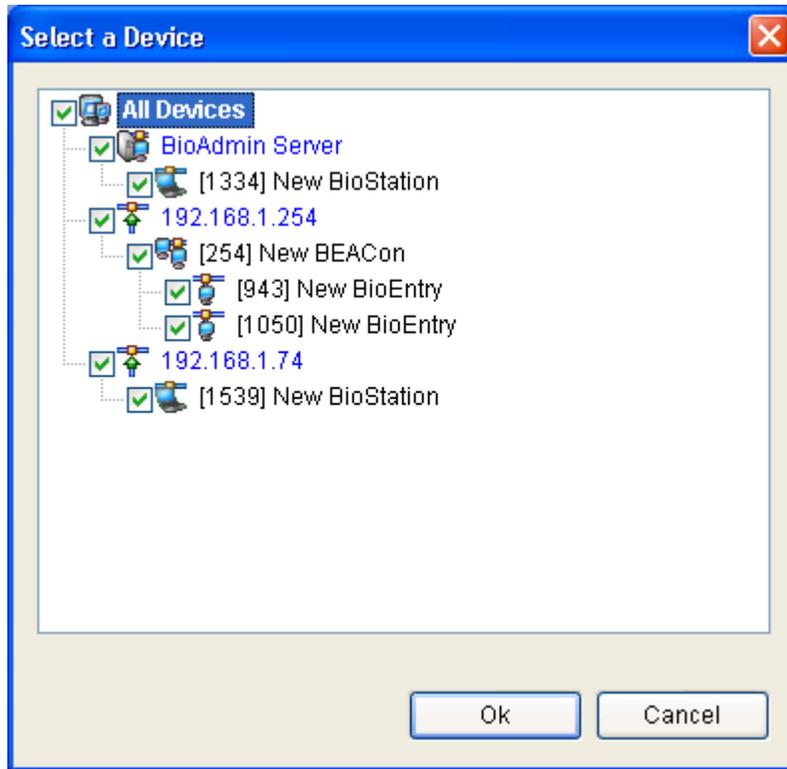


- CIS Index 블록
- 템플릿 수
- 템플릿 크기
- 각 템플릿의 시작 블록
- Mifare 카드를 템플릿 온 카드 모드로 사용하지 않는 경우에는 카드 레이아웃이 설정이 되어 있어도 이 정보를 사용하지 않습니다.

6.5.8. 편집 과정

고객의 레이아웃을 설정하기 위해, 다음 과정이 필요합니다.

- CIS 인덱스 블록을 선택합니다.
- 저장될 템플릿의 개수 및 크기를 설정합니다.
- 각 템플릿이 저장될 시작 블록을 설정합니다.
- 다른 장치에 적용 버튼을 클릭하여 현재 설정을 연결된 단말기에 전송합니다.

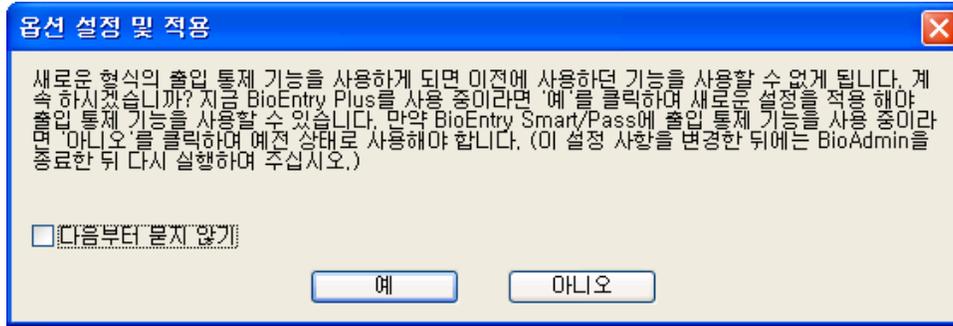


- 새로운 Mifare 카드 레이아웃을 PC USB 스마트카드 reader/writer에 저장하기 위해 **확인** 버튼을 누릅니다.
- 저장된 레이아웃은 PC USB 스마트카드 reader/writer를 사용하여 새로운 Mifare 카드를 발급할 때 적용됩니다.

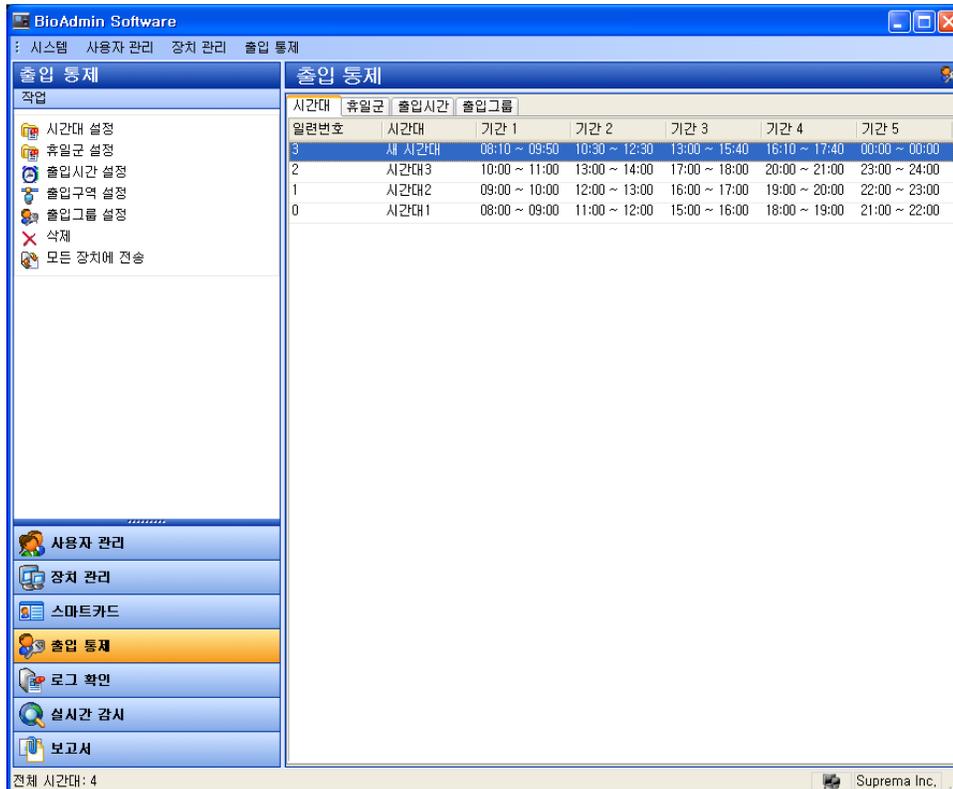
7. 출입 통제

이 메뉴에서는, 출입 시간과 출입 그룹을 지정할 수 있습니다. 출입시간과 출입 그룹은 이전에 지정된 규정에 따라 출입할 수 있는 사용자 권리를 제한하는데 사용됩니다.

BioAdmin 4.1 버전까지의 출입 통제 설정을 그대로 사용할 수도 있지만, 새로운 출입 통제기능을 사용하여 보다 쉽게 설정할 수 있는 기능을 사용할 수도 있습니다. 단, 새로운 출입 통제 기능을 사용하려면 기존 설정을 사용할 수는 없게 되며, 만약 이전 항목을 가진 상태에서 새로운 출입 통제 기능을 사용하려고 할 경우에는 어느 기능을 사용할 것인지 선택할 수 있습니다. 선택이 바뀌는 경우에는 BioAdmin Client를 다시 시작해야 할 필요가 있으며, 기존 것을 계속 사용하는 경우에는 다시 시작하지 않아도 됩니다.



- 사용자가 어느 출입 그룹에도 포함되지 않았다면 모든 출입문에 들어가는 것이 허용됩니다. 단, 장치의 기본 출입 그룹 설정이 있을 경우에는 기본 출입 그룹 설정을 따릅니다.
- 사용자가 한 출입 그룹에 포함되어 있지만 장치가 출입 그룹에 대한 정보를 가지지 않았다면, 사용자는 제한 없이 출입문에 들어갈 수 있습니다. 단, 새로운 출입 그룹 기능을 사용하는 경우에는 장치가 출입 그룹 정보를 가지고 있지 않을 경우는 거의 없습니다.

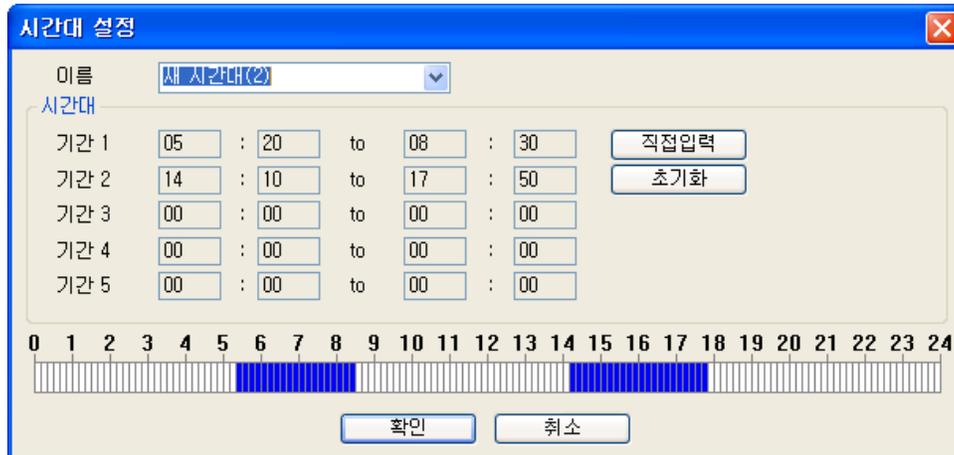


7.1. 시간대 설정

몇 개의 시간대를 통합하여 출입시간을 설정할 수 있습니다. 따라서 출입시간을 설정하기 전에 먼저 시간대를 설정해야 합니다. 각 시간대마다 최대 5개의 시간 구역을 선택할 수 있습니다.

상세한 작동 방법은 다음과 같습니다.

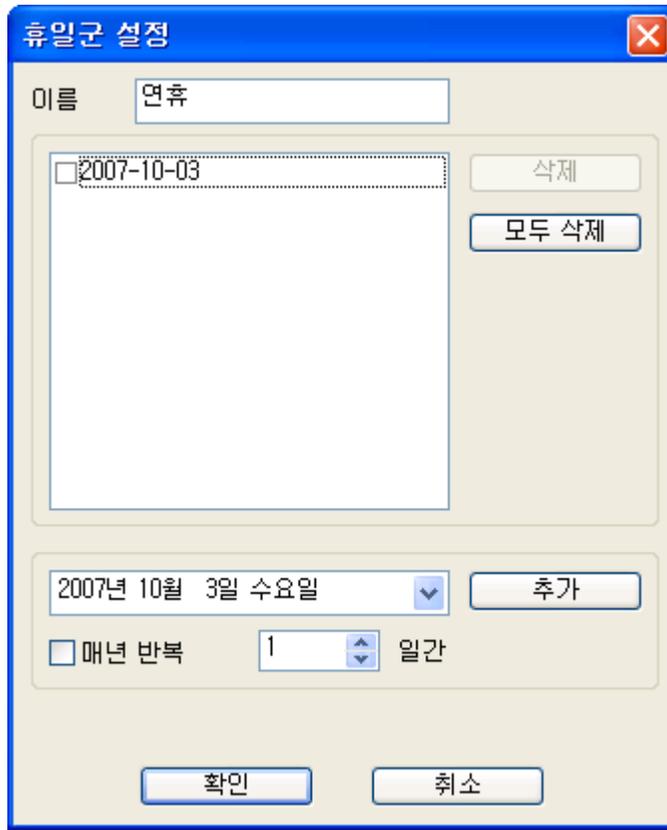
- 시간대 설정 버튼을 누릅니다.



- 시간대 이름을 입력합니다.
- 시간을 박스 안에 입력하여 시간 코드를 설정합니다.
- 하단에 표시된 타임 바를 드래그하여 손쉽게 시간대를 설정할 수 있습니다. 윈도우 아래에 끌어다 놓음으로써 시간 코드를 설정할 수 있습니다.
- 시간을 직접 입력하는 경우에는 '직접 입력' 버튼을 클릭합니다.
- 직접 입력하는 경우에는 각 입력 란들이 입력 가능한 상태로 변경됩니다.
- 입력을 마친 뒤에는 '적용'을 눌러서 값을 저장합니다.
- 직접 입력한 뒤에 하단의 타임 바를 드래그 하게 되면 설정된 내용은 타임 바의 내용으로 변경되게 됩니다. 또한 10분 미만의 단위 시간들은 모두 0 혹은 10분으로 변경되므로 주의가 필요합니다.
- 시간대 리스트에 시간대를 추가하기 위해 **확인** 버튼을 누릅니다.

7.2. 휴일 균 설정

출입시간에 휴일들을 포함시키기 위해서는 휴일 균을 미리 설정해야 합니다. 상세한 설정 방법은 다음과 같습니다.



- 휴일 군 설정 버튼을 누릅니다.
- 휴일 군 설정 윈도우에서 휴일설정 버튼을 누릅니다.

- 휴일군의 이름을 입력합니다.
- 휴일에 해당하는 날짜를 입력한 후 추가 버튼을 누릅니다.
- 이때, 해당 날짜의 옵션에 따라서 기간 및 반복 여부도 같이 지정할 수 있습니다.
- 원하는 만큼 날짜를 입력 합니다. 단, 최대 항목 수는 32개를 초과할 수 없습니다. 이럴 경우에는 휴일 군을 추가로 생성해야 합니다.
- 휴일 추가를 완료한 후 확인 버튼을 누릅니다.
- 이 곳에서 설정된 휴일목록은 근태리포트에도 적용할 수 있습니다.

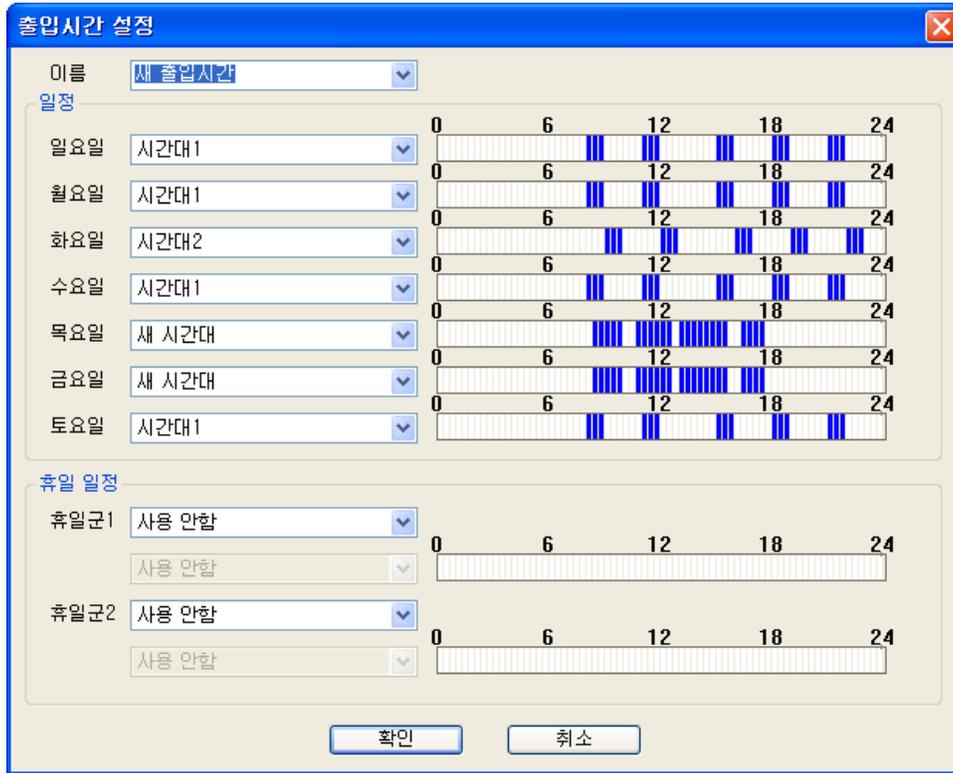
7.3. 출입시간 설정

시간대와 휴일 군을 합하여 출입시간을 설정할 수 있습니다. 월요일부터 일요일까지 각 요일마다 한 개의 시간대가 선택됩니다.

출입 시간대는 출입 통제와 관련된 대부분의 설정에서 선택하여 적용할 수 있기 때문에 각각의 근무 형태나 출입자에 대해 선택할 수 있도록 모든 형태의 출입 시간 설정을 생성하여 저장하도록 합니다.

상세한 설정 방법은 다음과 같습니다.

- 출입시간 설정 버튼을 누릅니다.
- 출입시간 이름을 입력합니다.



- 월요일부터 일요일까지 각 요일마다 미리 설정한 각 시간대를 선택합니다.
- 미리 설정해 놓은 휴일군 중에서 생성하고 있는 출입시간에 적용하고 싶은 설정이 있다면 선택하거나 직접 시간대를 입력 합니다.
- 휴일군은 2가지로 설정이 가능합니다.
- 설정된 출입시간을 출입시간 리스트에 추가하려면 **확인** 버튼을 누릅니다.

7.4. 출입구역 설정

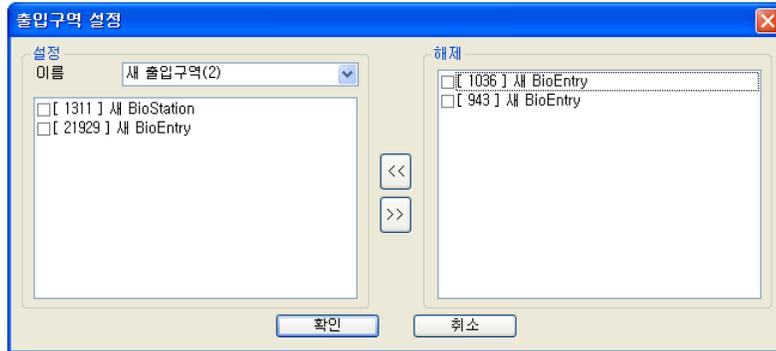
BioAdmin 4.2 버전 부터는 출입구역의 설정을 별도로 하지 않으며, 새로운 형식의 출입통제 기능을 사용하게 되며, 이전 버전의 사용자라면 계속 사용하지만, 새로 설치 하는 사용자는 안내에 따라 BioAdmin 4.2 전용 출입통제 형식으로 전환하시면 됩니다. 단, 한번 전환된 설정은 복구 되지 않으므로 신중하게 결정하시길 바랍니다. 새로운 설정을 적용하기 위해서는 프로그램을 재 실행 하셔야 합니다.

전환은 출입통제 메뉴에 들어갈 때 나타나는 질문에 '예' 를 누르거나, BioAdmin 메뉴 중에 '시스템' 을 클릭하시면 '옵션' 이라는 소메뉴가 나타나며 이 곳에서 버전관리 항목에 체크하시면 됩니다.

프로그램을 재 시작하시면 출입구역 설정 탭은 보이지 않습니다.

여러 대의 장치들을 결합하여 출입구역을 설정할 수 있습니다.
상세한 설정 방법은 다음과 같습니다.

- 출입구역의 이름을 입력합니다.
- 대상 장치를 표시하고 << 버튼을 클릭합니다.



- 출입구역 리스트에 추가하려면 **확인** 버튼을 누릅니다.

7.5. 출입 그룹 설정

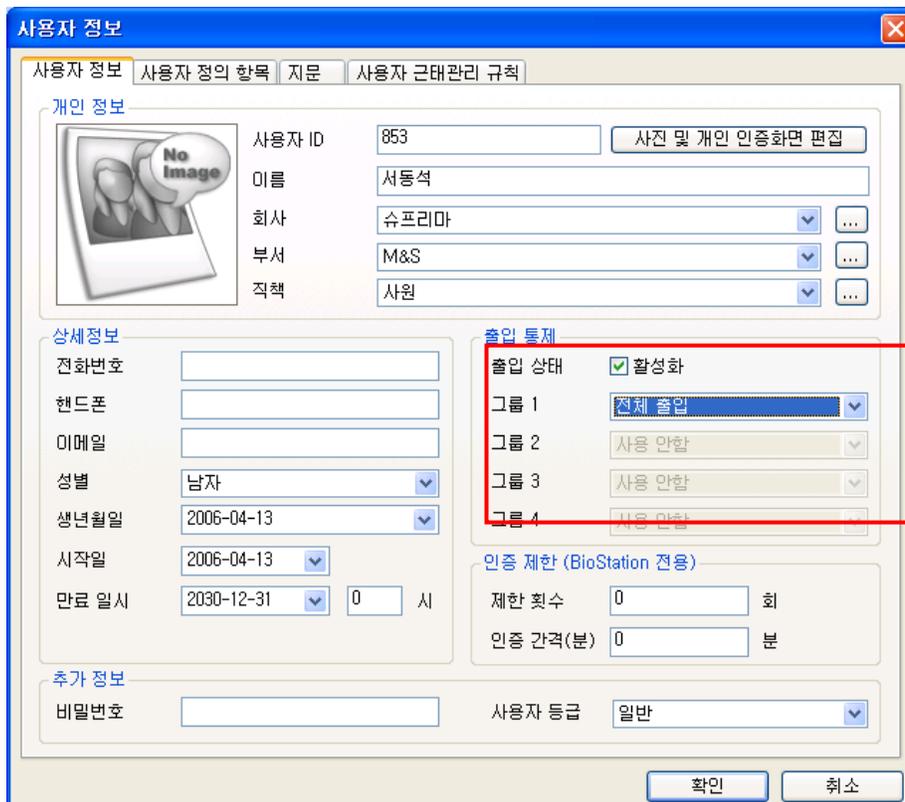
6.4 항목과 마찬가지로 BioAdmin 4.2 버전에서는 이전 버전 방식과, 새로운 방식의 두가지 출입그룹 설정이 있으며, 다음은 이전 방식의 출입그룹 설정 방식을 설명합니다.

출입시간과 출입구역을 결합하여 출입그룹을 만들 수 있습니다. 출입그룹에 의해서 각 사용자의 출입 권한을 제한할 수 있습니다..

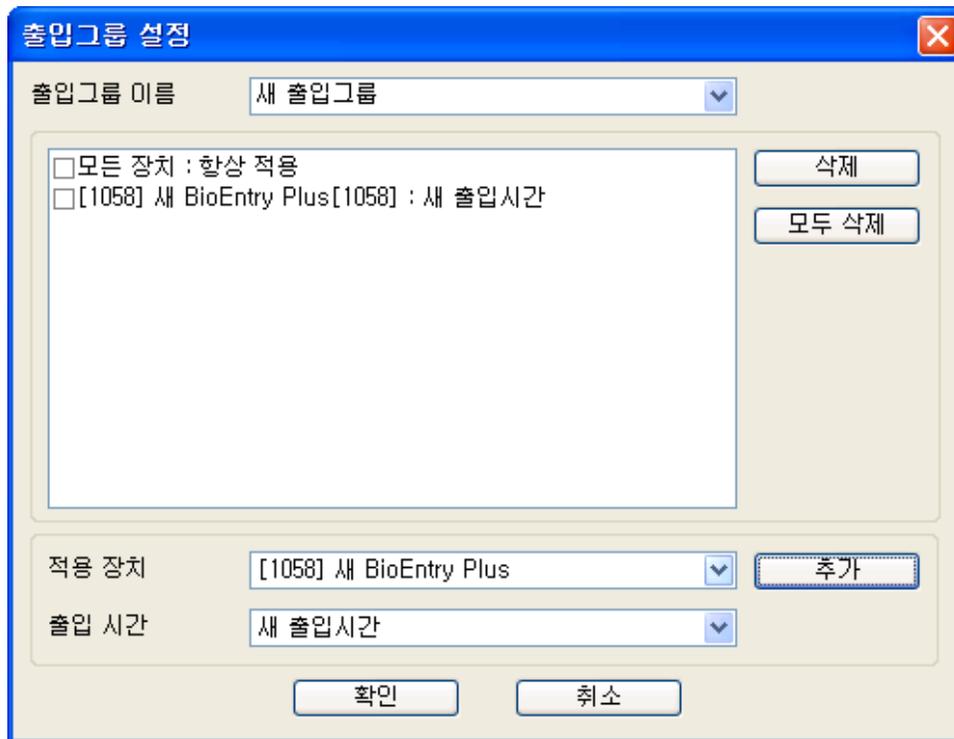
- **출입그룹 설정** 버튼을 누릅니다.
- 출입 그룹의 이름을 입력합니다.
- 시간대와 출입구역에 표시하고 << 버튼을 누릅니다.



- 선택된 출입 그룹을 출입 그룹 리스트에 추가하려면 **확인** 버튼을 누릅니다. 사용자 관리 메뉴에서 이 출입 그룹을 사용자에게 적용할 수 있습니다.
- 사용자 데이터에 대한 구체적인 작동 방법은 제3장 사용자 관리 편을 참조하시기 바랍니다.



- BioAdmin 4.2 버전 전용 출입통제 그룹설정은 먼저 장치를 선택하고 해당 장치에 적용할 출입 시간을 추가하거나 삭제 할 수 있습니다. 특정 시간대를 사용하는 사용자만을 출입허용으로 설정하길 원하는 경우에는 장치관리 메뉴에서 해당 장치를 선택하고, 출입통제설정 탭에 있는 '기본출입그룹' 설정을 전체제한으로 정한 다음, 본 출입그룹 설정 탭에서 특정 출입시간만을 허용하면 쉽게 설정할 수 있습니다.

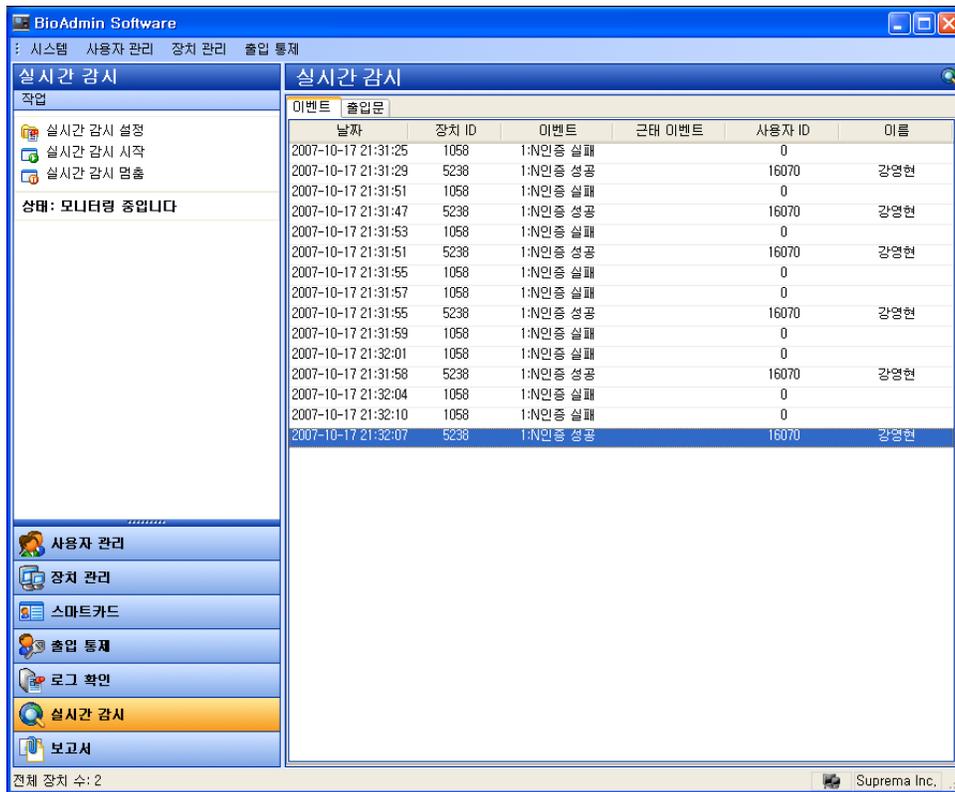


7.6. 출입 그룹 장치에 적용

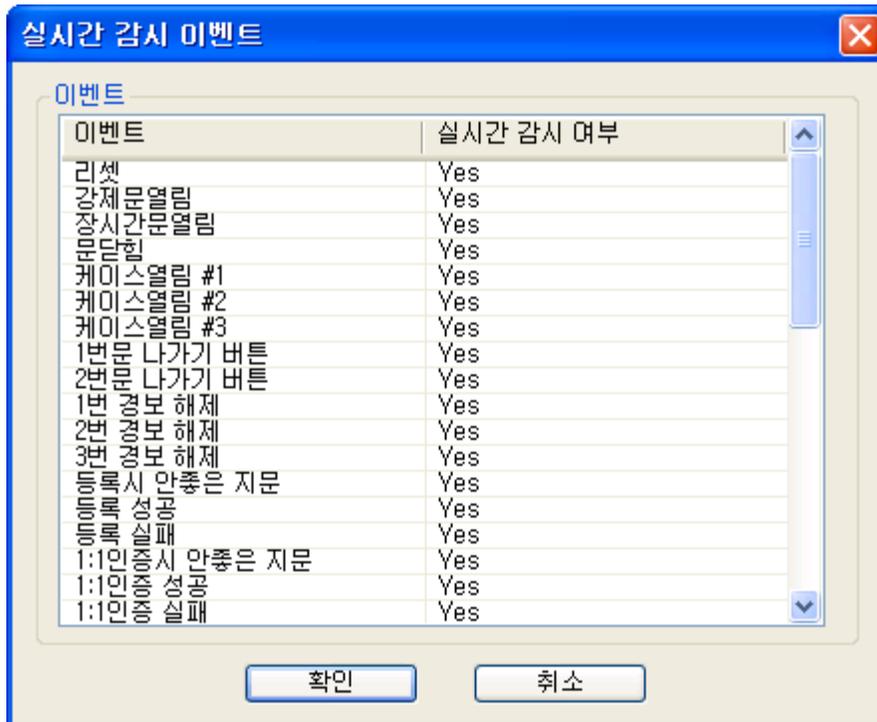
원활한 설정 적용을 위해 모든 장치에 전송 버튼을 눌러 설정된 출입시간과 출입그룹을 장치에 적용합니다.

8. 실시간 감시

BioAdmin은 실시간 감시 기능을 지원합니다. 실시간 감시 메뉴를 선택하여 연결된 장치들의 로그 이벤트를 실시간으로 확인할 수 있습니다.



8.1. 실시간 감시 설정



이 메뉴에서는 각 이벤트의 Yes/No 필드를 단순히 더블 클릭하는 것으로 실시간 감시 윈도우에 나타날 이벤트를 선택할 수 있습니다.

만약 Yes 필드를 선택한다면 이 필드는 No로 바뀌게 되며 이 이벤트는 실시간 감시 모드에 표시되지 않게 됩니다. 만약 No 필드를 선택한다면 이 필드는 Yes로 바뀌게 되며 이 이벤트는 실시간 감시 모드로 표시됩니다.

실시간 감시 모드에서 이 메뉴를 활성화하면 감시는 중단될 것입니다. 따라서 실시간 감시 시작 메뉴를 눌러 감시를 다시 시작할 수 있습니다.

8.2. 실시간 감시 시작

- 실시간 감시 시작 메뉴를 누르면, 연결된 장치들의 로그 이벤트에 대해 실시간 감시를 시작할 수 있습니다.
- 실시간 감시 모드 중에 다른 메뉴를 선택하면 감시는 중단될 것입니다.
- 실시간 감시 윈도우상의 이벤트 리스트는 5000개 이벤트까지 보여줍니다. 이벤트의 수가 5000개를 초과하면 제일 오래된 이벤트가 리스트에서 삭제될 것입니다. 제일 오래된 이벤트가 실시간 감시 리스트에서 삭제된다 해도 장치의 로그 데이터에는 남아 있습니다.

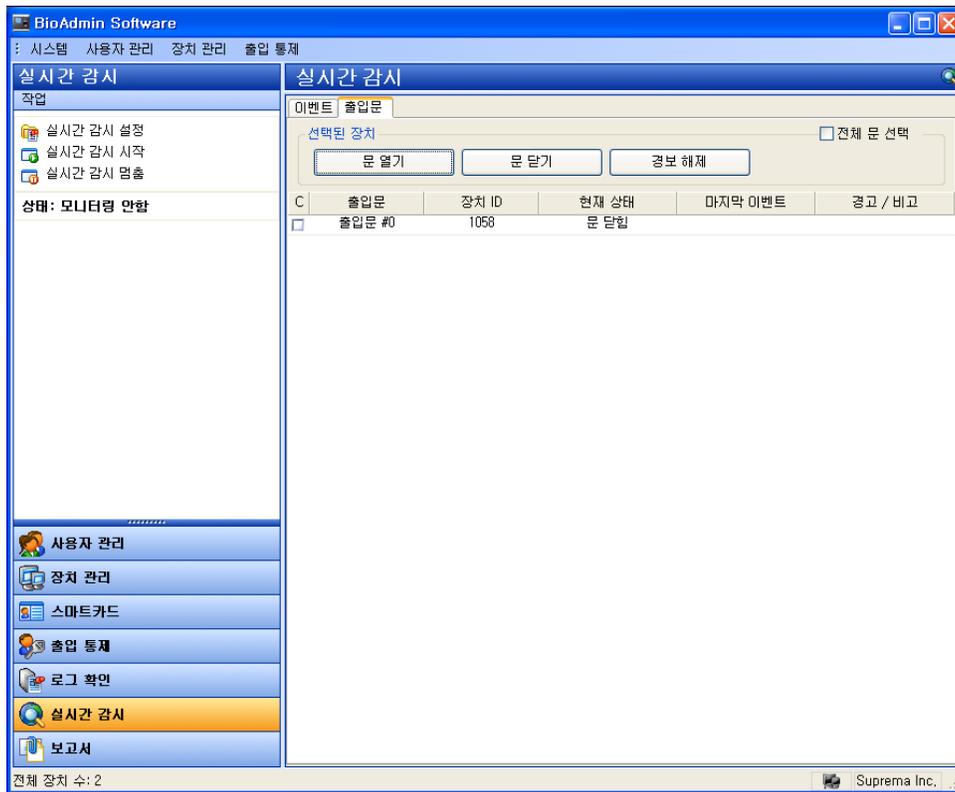
타 메뉴에서 실시간 감시 메뉴를 선택할 경우 실시간 감시 시작 버튼을 누르지 않아도 자동으로 실시간 감시가 시작됩니다. 즉, 실시간 감시 시작 버튼은 실시간 감시가 멈춘 상황에서 다시 감시를 시작할 경우에만 필요한 버튼입니다.

8.3. 실시간 감시 멈춤

실시간 감시 멈춤 버튼을 누르면 감시를 중지할 수 있습니다.

8.4. 출입문 실시간 감시

출입문 상태를 실시간으로 감시하는 기능을 지원합니다. 실시간 감시 메뉴를 선택하여 오른쪽 '출입문'을 선택하면 출입문 실시간 감시 화면을 볼 수 있습니다.



8.4.1.

문열기/문닫기

- 출입문 리스트 중에서 문을 열려고 하는 출입문의 체크 박스에 체크한 뒤에 '문열기' 버튼을 클릭하면 연결된 출입문을 열고 닫을 수 있습니다.
- 단, 이 경우 실제 문이 닫혔는지의 판단 여부와는 달리 장치로 입력되는 정보만으로 상황을 분석하기 때문에 실제 동작과 차이가 나타날 수도 있습니다.

8.4.2.

경보 해제

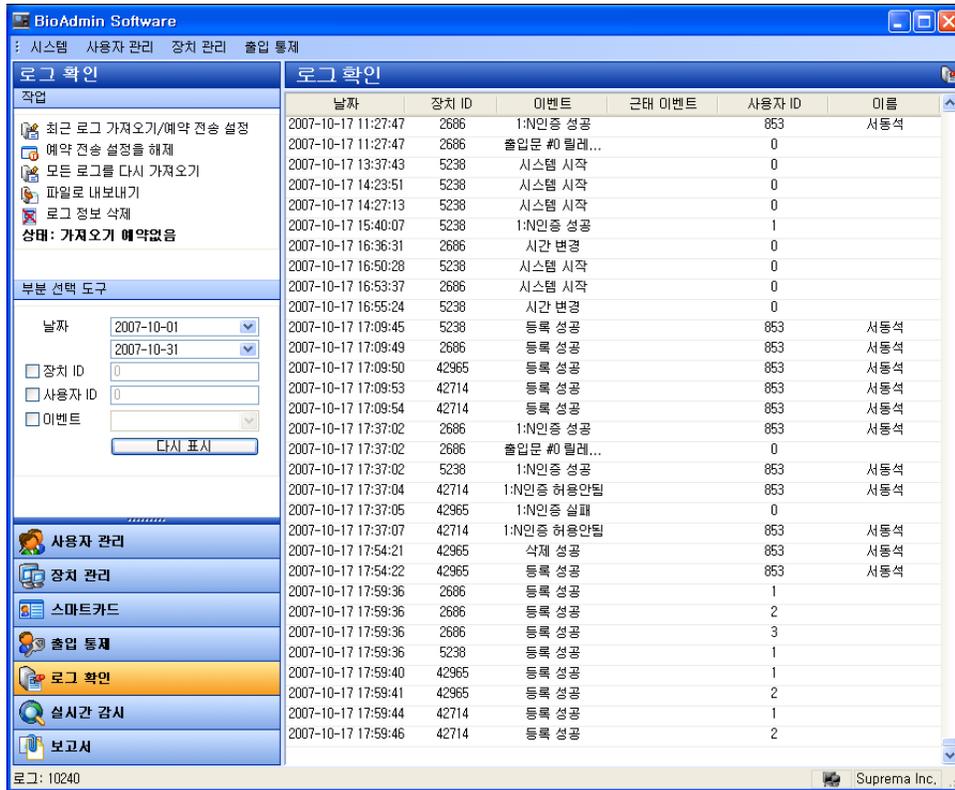
- 장시간 문열림이나 강제 문 열림 같은 경보가 발생하는 이벤트가 있는 경우 해제하려는 경보를 가진 출입문의 체크 박스에 체크한 뒤에 '경보 해제' 버튼을 클릭하여 현재 PC화면에 나타난 경보 상태를 해제할 수 있습니다.
- 단, 경보 해제의 경우 실제 경보를 끄는 것은 관리자의 조작이 필요할 수도 있습니다.

9.

로그 확인

로그 확인 메뉴는 다음과 같은 동작들을 포함합니다..

- BioAdmin 서버에 저장된 로그 데이터베이스의 관리
- 장치로부터의 새로운 로그 이벤트를 로그 데이터베이스에 업 로드 하기



9.1. 로그 확인 페이지의 구성

로그 확인 페이지는 3가지 구성요소로 이루어져 있습니다.:

- 부분 선택 도구

사용자들은 로그 기록들을 날짜, 리더 ID, 사용자 ID, 이벤트 ID와 이벤트 소스에 따라 정렬할 수 있습니다. 가령, 리더 ID를 선택한다면 그 리더의 로그 기록들만이 나타날 것입니다.

- 로그 확인 페이지

로그 데이터베이스는 구 로그 데이터를 보존할 수 있는 호스트 PC에 저장되어 있습니다. 로그 확인 페이지는 날짜, 시간, 소스 리더, 이벤트와 이벤트 소스를 말해주는 저장되어 있는 로그 이벤트를 보여줍니다.

- 작업 박스

작업 박스에는 로그 확인 페이지의 기본 동작들을 제어하는 버튼들이 있습니다.

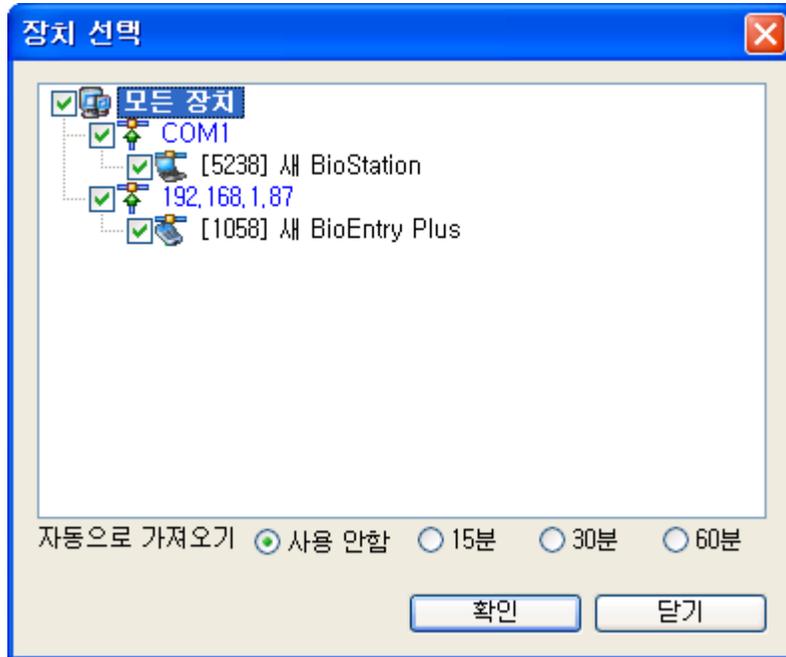
9.2. 로그 데이터베이스 관리

9.2.1. 최근 로그 가져오기

최근 로그 가져오기/ 예약전송 설정 버튼을 누를 경우 장치선택을 위한 창이 뜨고, 여기에서 선택한 장치에 대해 BioAdmin 에 있는 로그 정보 이후의 새로이

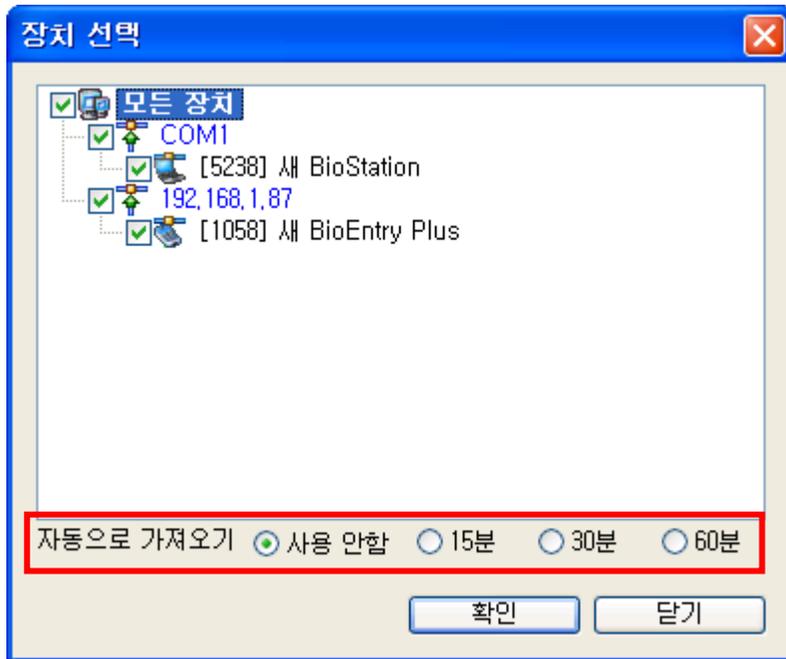
생성된 로그 정보를 가져옵니다.

단, 서버에 연결된 **BioStation**에 대해서는 서버에 해당 **BioStation**들의 로그가 실시간으로 저장되고 있으므로 로그 가져오기를 하지 않아도 됩니다.

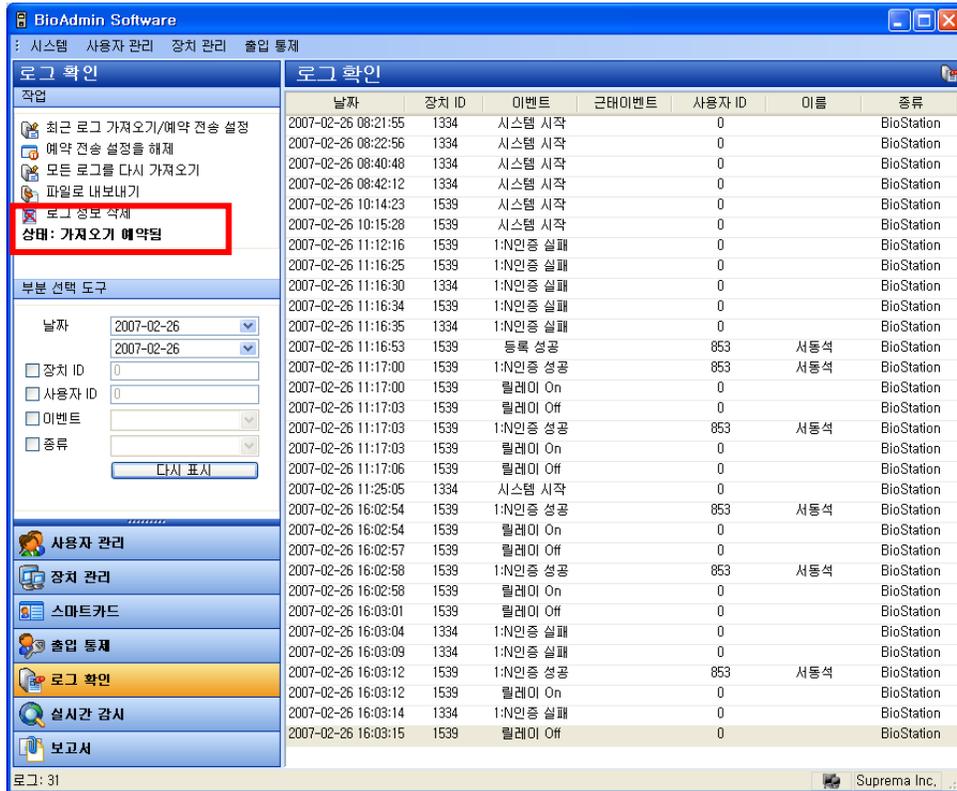


9.2.2. 예약 전송 설정

최근 로그 가져오기/ 예약전송 설정 버튼을 누를 경우 지정된 기간 동안 BioEntry 및 BioStation 에서 생성된 로그정보를 자동으로 BioAdmin으로 가져올 수 있습니다. 관리자는 적용환경에 따라 15분 / 30분 / 60분 중 선택하여 예약전송을 실행할 수 있습니다.



예약 전송이 적용되면 작업 박스에 상태: 가져오기 예약됨으로 표시됩니다.



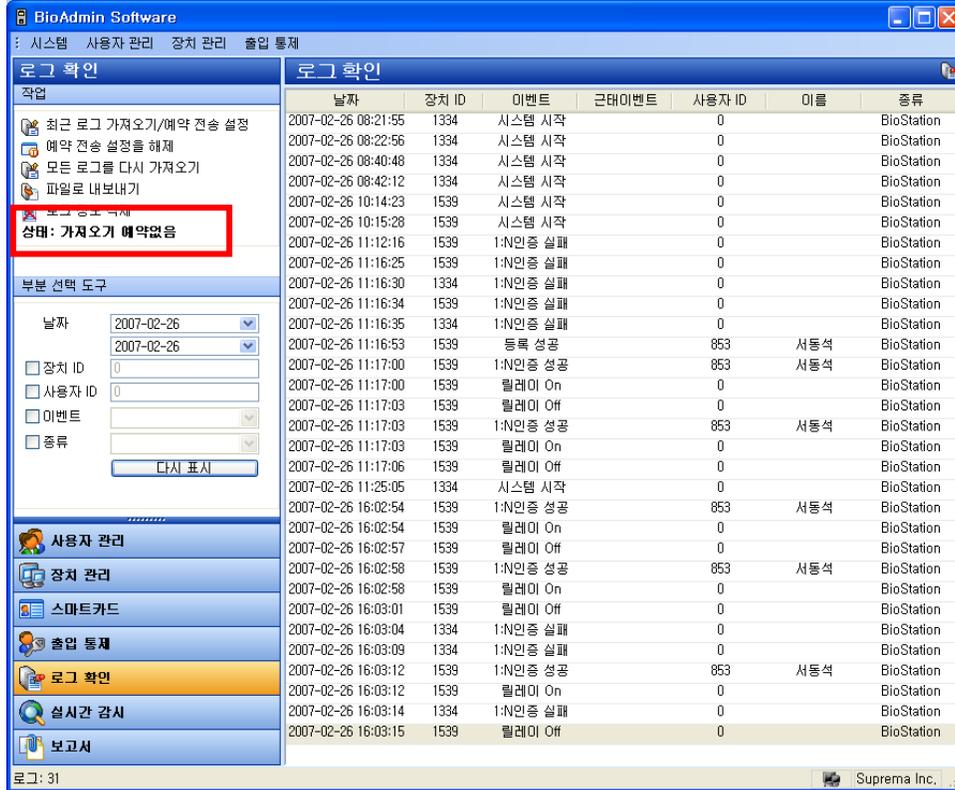
9.2.3.

예약 전송 설정을 해제

예약 전송 설정을 해제 버튼을 누를 경우 설정되어있던 예약 전송을 해제 할

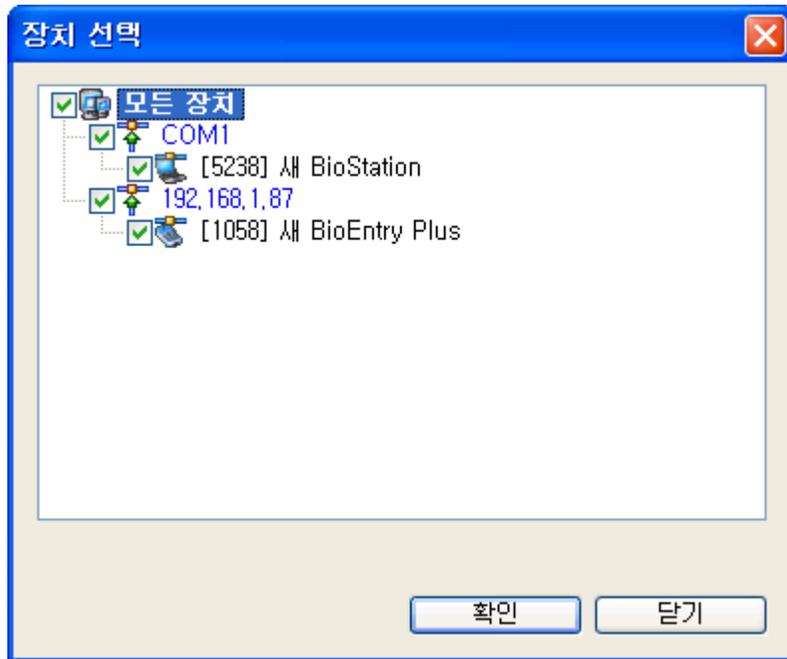
수 있습니다. 또한, 예약 전송 설정 시 **사용 안 함**으로 할 경우에도 예약전송을 해제할 수 있습니다.

예약 전송이 적용되면 작업 박스에 **상태: 가져오기 예약없음**으로 표시됩니다.



9.2.4. 모든 로그를 다시 가져오기

모든 로그를 다시 가져오기 버튼을 누를 경우 장치선택을 위한 창이 뜨고, 여기에서 선택한 장치의 모든 로그정보를 가져옵니다. 단, 기존에 BioAdmin 에 일부 로그정보는 있을 경우에는 기존의 로그정보는 그대로 유지하며, 기존에 없던 로그정보를 새로이 가져옵니다.

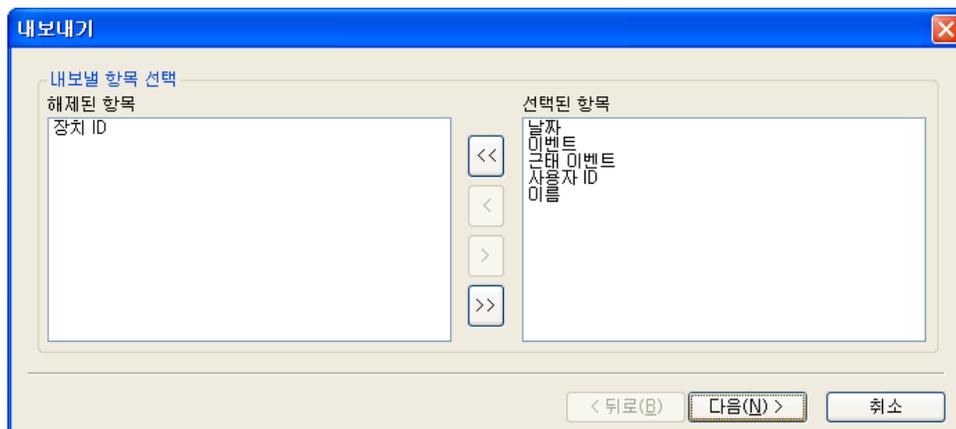


9.2.5. 파일로 내보내기

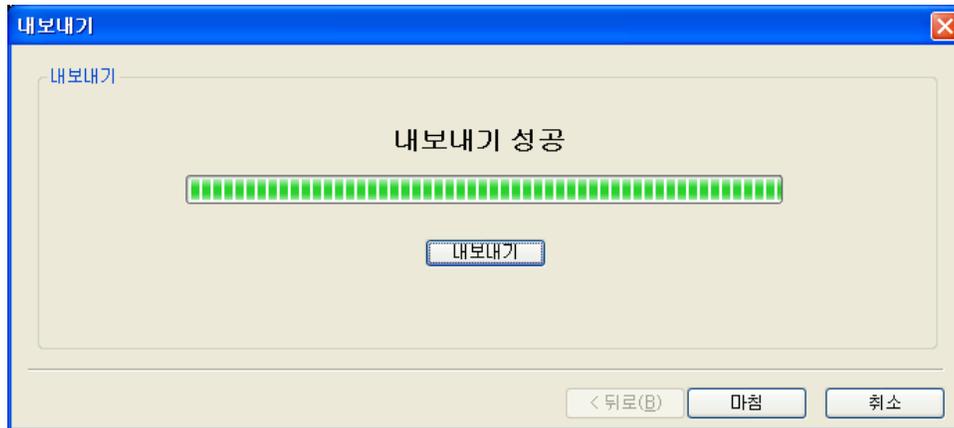
파일로 내보내기 버튼을 이용하여 로그 데이터를 CSV 파일 포맷으로 내보낼 수 있습니다.

구체적인 동작은 다음과 같습니다:

- 내보낼 로그 데이터 열을 선택합니다.
- 파일로 내보내기 버튼을 누릅니다.
- 해제된 항목 리스트에서 선택된 항목 리스트로 대상 필드를 이동하여 내보낼 필드들을 선택합니다.



- 필드들을 선택한 후에 다음 버튼을 누릅니다.
- 내보낼 파일을 선택합니다.
- 파일을 선택한 후 다음 버튼을 누릅니다.
- 내보내기 버튼을 누릅니다.



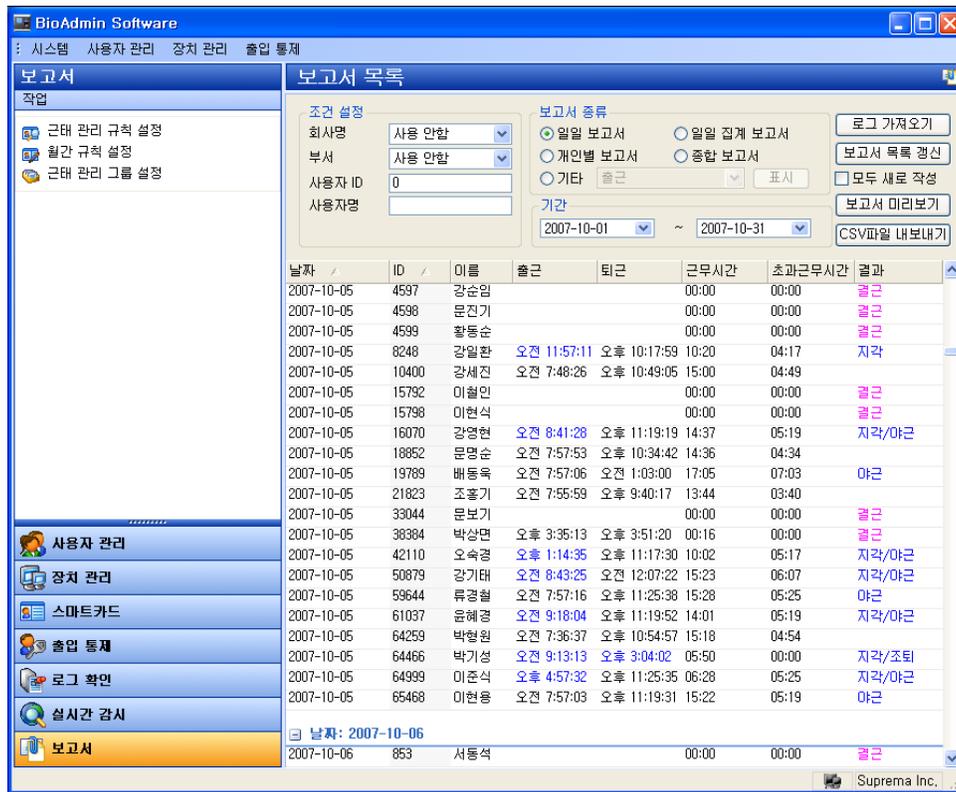
9.2.6. 로그 정보 삭제

로그 정보 삭제 버튼은 호스트 PC의 로그 데이터베이스에서 선택한 로그 데이터를 제거합니다. 장치의 로그 데이터는 이 명령으로 제거되지 않습니다.

10. 보고서

보고서 메뉴는 다음과 같은 동작들을 포함합니다..

- 근태관리규칙을 설정
- 장치로부터 로그를 가져와 근태 보고서를 작성
- 작성된 보고서를 파일로 내보내기
- 작성된 보고서를 출력.



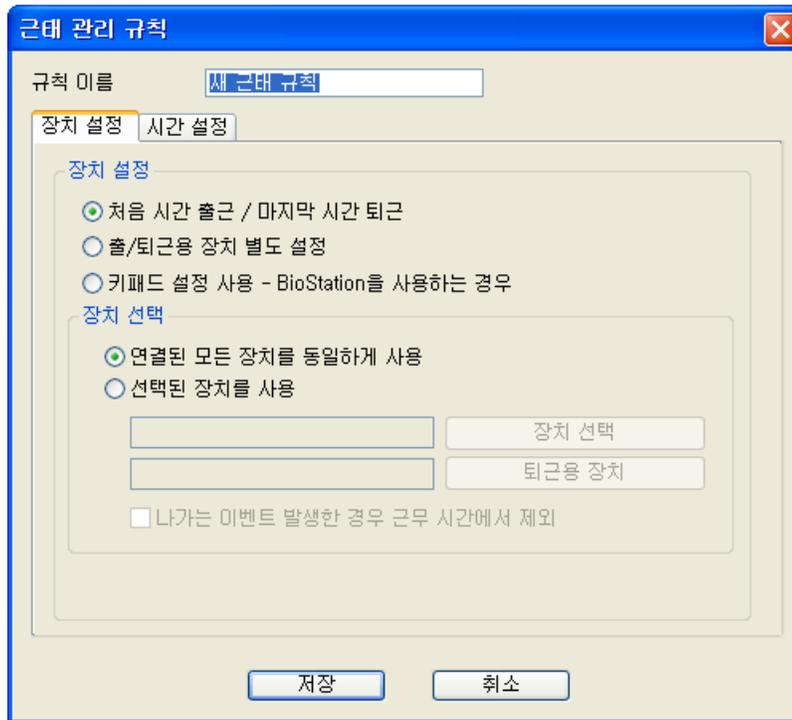
10.1. 보고서 목록 페이지의 구성

보고서 목록 페이지는 2가지 구성요소로 이루어져 있습니다.:

- 보고서 목록 페이지
보고서 목록은 보고서 조건 설정, 보고서 종류, 기간을 설정하는 메뉴와 보고서 작성을 위해 필요한 기초 정보를 보여줍니다.
- 작업 박스
작업 박스에는 근태 관리 규칙 설정을 위한 버튼이 있습니다.

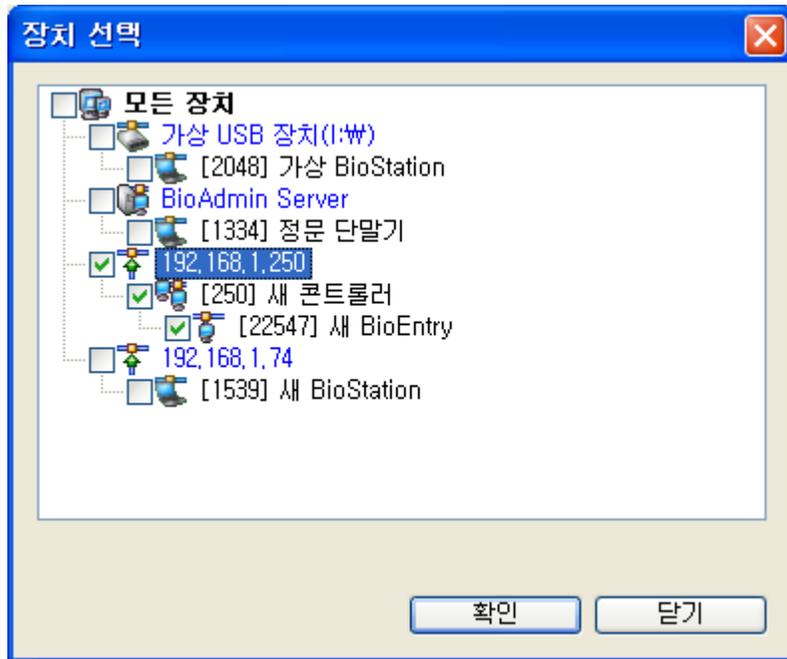
10.2. 근태관리 규칙 설정

- 근태 관리 규칙 설정 버튼을 눌러 새로운 근태규칙을 설정합니다.



- **처음시간 출근 / 마지막 시간 퇴근**을 선택할 경우 사용자가 해당일 중 처음 인증된 시간을 출근으로, 마지막 인증된 시간을 퇴근으로 적용합니다.
- **출/퇴근용 장치 별도 설정**을 선택할 경우 장치 선택 메뉴를 이용하여 출근용 장치와 및 퇴근용 장치를 별도로 지정할 수 있습니다. 그 경우 출근용 장치에 한하여 처음 시간을 출근으로 적용하며, 퇴근용 장치에 대해 마지막 시간을 퇴근으로 적용하게 됩니다. 선택되지 않은 장치에 대해 사용자가 출근 또는 퇴근으로 입력할 경우 로그 정보는 출근 또는 퇴근으로 표시되지만 보고서 작성시에는 출근 또는 퇴근이 적용되지 않습니다.
- **키 패드 설정 사용 - BioStation을 사용하는 경우**를 선택할 경우 BioStation에 설정된 근태 키를 사용하는 경우에 한하여 출근 또는 퇴근으로 보고서에 적용됩니다. 이 메뉴는 BioStation에만 적용되며 따라서 BioEntry 는 이 경우 근태용 장치로 사용할 수 없습니다.

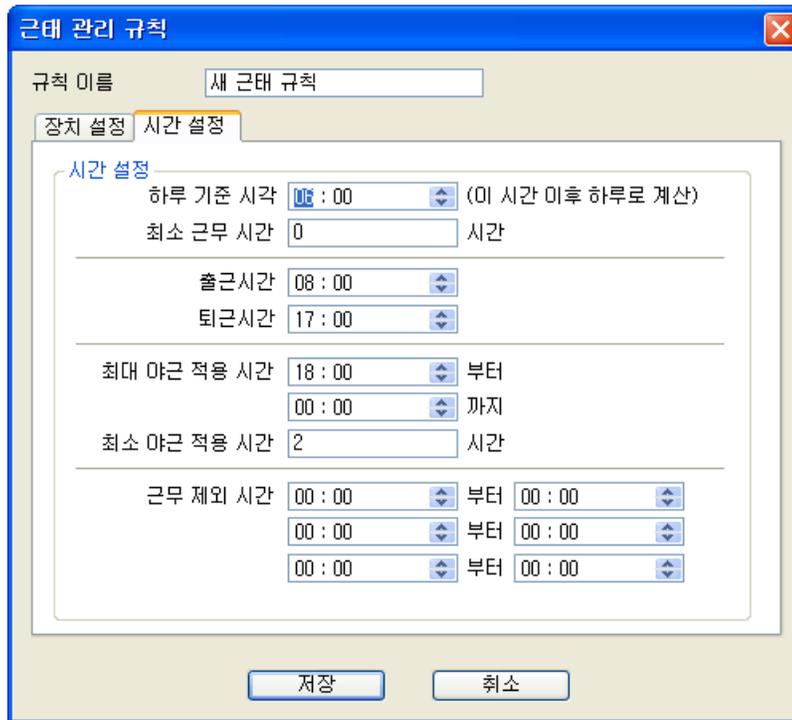
장치 선택 메뉴를 통해 근태용 장치로 사용할 장치를 선택 할 수 있습니다.



- 연결된 모든 장치를 동일하게 사용을 선택할 경우 네트워크에 연결된 모든 장치를 근태용 장치로 사용하게 됩니다. 단, 키 패드 설정 사용을 선택한 경우에는 BioEntry를 근태용 장치로 사용할 수 없습니다.
- 선택된 장치를 사용을 선택 할 경우 선택된 장치에 대해서만 근태용 장치로 사용할 수 있습니다.

10.2.2. 시간 설정

근태 관리 규칙 화면에서 시간 설정 메뉴를 선택하여 아래와 같이 근태관리기준 시간을 설정합니다.

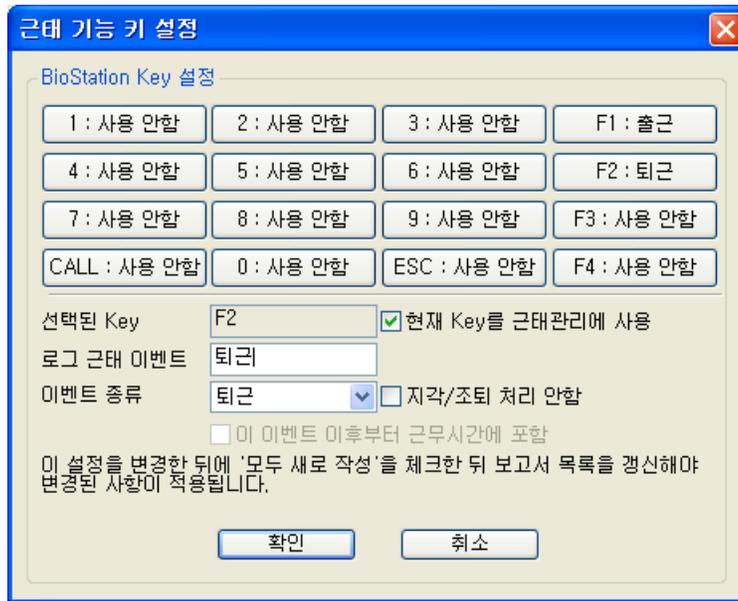


구체적인 설정방법은 다음과 같습니다.

- 이 시간 이후 하루로 계산에 근무일 시작의 기준 시간을 설정합니다.
- 최소 근무시간으로 해당일의 최소 근무 시간을 설정합니다. 지정된 최소 근무 시간보다 근무 시간이 적을 경우 보고서 상의 결과가 결근으로 적용됩니다. 최소 근무시간을 0으로 설정 할 경우 이 기능을 사용하지 않을 수 있습니다.
- 출근시간을 입력합니다.
- 퇴근시간을 입력합니다.
- 최대 야근 적용 시간을 입력합니다. 설정된 최대 야근 적용시간 이외의 시간에 야근을 할 경우에는 보고서상의 야근시간에 포함되지 않습니다.
- 최소 야근 적용 시간을 입력합니다. 퇴근시간 이후 설정된 최소 야근 적용시간 미만으로 추가근무 할 경우에는 보고서상에 야근이 적용되지 않습니다.
- 근무 제외 시간을 설정하면 해당시간은 향후 보고서 작성시 근무시간에서 제외 됩니다. 변경버튼을 눌러 최대 3개까지 근무 제외 시간을 적용할 수 있습니다. 드롭 다운 메뉴를 통해 각각의 근무 제외 시간이 몇 시부터 몇 시까지 설정되어 있는지를 확인할 수 있습니다.

10.2.3. 바이오 스테이션 기능 키 설정

바이오 스테이션 기능 키 설정 메뉴를 선택하여 아래와 같이 로그 정보 및 보고서 표시방법을 설정합니다.



구체적인 설정방법은 다음과 같습니다:

- 해당 키를 선택합니다.
- 선택된 키를 근태관리 키로 사용하고자 할 경우 **현재Key**를 **근태관리에 사용**을 활성화 시킵니다.
- 선택된 키에 대한 로그 표시 방법을 **로그 근태 이벤트**에 입력합니다. 실시간 감시 및 로그 확인 시 해당 키에 대해 로그 정보 이벤트에 입력된 대로 표시 됩니다.
- **이벤트 종류**를 통해 해당키가 출근, 퇴근, 들어옴, 나감 중 어떠한 이벤트로 적용될 지 여부를 선택합니다. 선택된 이벤트는 보고서 작성시 근태 결과 및 근무시간 산정의 기준이 됩니다.

바이오 스테이션 기능 키 설정을 변경한 뒤에 보고서를 갱신해야만 변경된 사항이 적용됩니다.

- 여기서 설정한 근태 이벤트는 **BioLite Net**에서 발생한 로그에도 적용됩니다.

10.3. 월간 규칙 설정

월간 근태규칙을 설정함으로써 향후 근태관리 보고서 작성의 기준이 되는 일반 근무일과 휴일을 선택 할 수 있습니다. 휴일로 설정된 날에는 지각, 조퇴, 결석 등이 적용되지 않으며, 그 근무시간은 휴일근무 시간에 더해지게 됩니다.

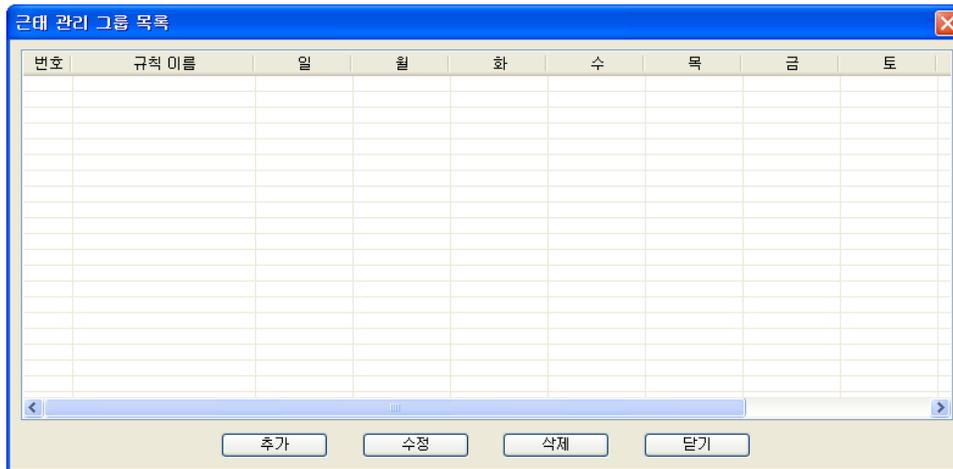
- **근태 관리 규칙 설정** 버튼을 눌러 월 규칙을 설정합니다.



- 매월 적용된 일반 근무일과 휴일을 설정한 후 저장 버튼을 눌러 변경된 내용을 저장합니다.
- 이 설정을 변경한 뒤에는 보고서 목록 윈도우의 모두 새로 작성에 체크한 뒤 보고서 목록을 갱신해야 변경된 사항이 적용됩니다.

10.4. 근태 관리 그룹 설정

위에서 설정한 사항을 사용하여 근태 관리 규칙을 그룹화 하여 관리할 수 있습니다.



추가를 눌러 새로운 근태 규칙 그룹을 생성하고 각각 세부 규칙을 설정해 줍니다.

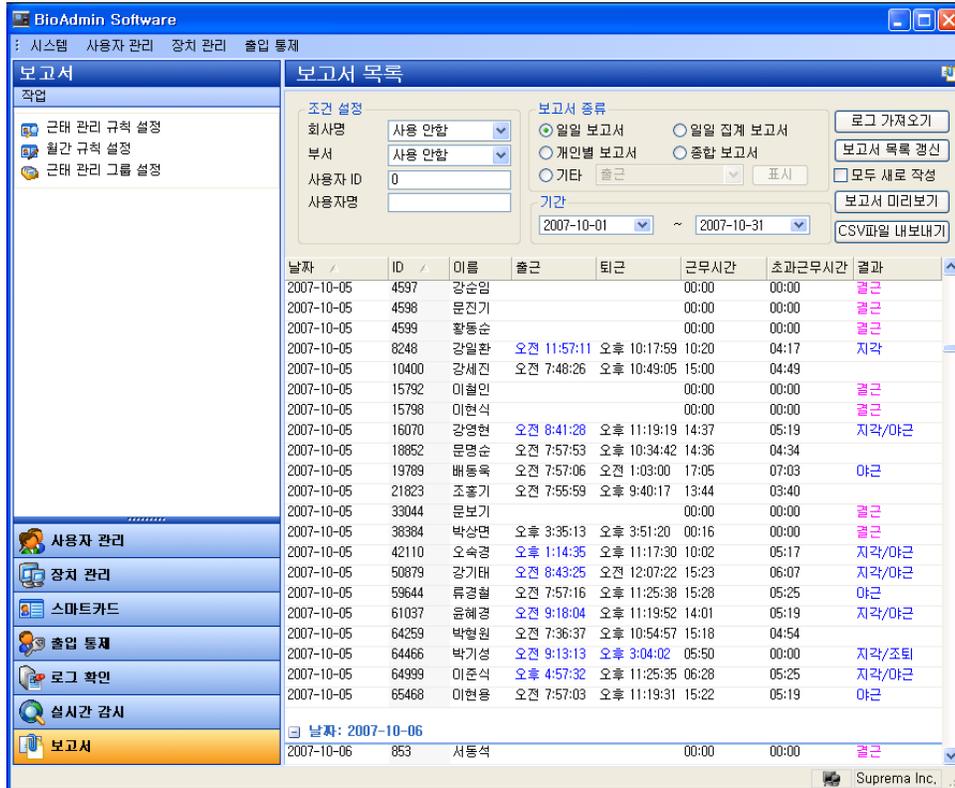
- 이 규칙을 기본 규칙으로 사용

기본으로 사용을 활성화 시킴으로써 선택된 근태 관리 규칙을 기본 규칙으로 적용합니다. 특정 사용자에게 대해 근태 관리 규칙이 설정되지 않았을 경우 동 사용자에게 대해서는 기본 규칙이 적용됩니다.

10.5. 보고서 작성 방법

- 로그 가져오기 버튼을 눌러 최근 로그정보를 가져옵니다. 이는 최근 출입정보에 근거하여 보고서를 작성하기 위한 과정으로서, 로그 가져오기를 완료하여도 보고서 목록에 로그가 표시되지는 않습니다.

- 조건설정 메뉴에서 보고서를 작성하고자 하는 회사, 부서, 사용자를 선택합니다.
- 보고서 종류 메뉴에서 일일 보고서 또는 개인별 보고서를 선택합니다.
- 기간 메뉴에서 보고서 작성의 시작일과 종료일을 선택합니다.
- 보고서 목록갱신 버튼을 누릅니다.



- 보고서 미리 보기 버튼을 누릅니다.

미리보기

9 / 31

2006-08-09

2006-08-01~2006-08-31

일일 근태 결과 보고서

ID	부서	직책	이름	출근	퇴근	근무시간	대근	결핵	출근이벤트	퇴근이벤트
1211	M&S	과장	장인하			00:00	00:00	결근		
3786	M&S	과장	전영복	오후 4:37:24	오후 9:37:23	04:59	03:37	지각		
4405	생산	사원	기보원	오후 5:12:29		00:00	00:00	지각		
8248	경영기획	과장	왕길환			00:00	00:00			
10400	R&D	연구원	왕세경	오후 4:49:42	오후 7:55:41	03:05	01:55	지각		
15792	M&S	사원	이필연			00:00	00:00	결근		
15799	M&S	사원	이준식			00:00	00:00			
16070	R&D	연구원	왕영관	오후 6:32:16	오후 7:53:28	01:21	00:00	결근		
19852	R&D	선임연구원	최영순	오후 5:29:51	오후 9:54:37	04:24	03:54	지각		
19799	R&D	선임연구원	비동욱			00:00	00:00			
21823	경영기획	사원	조흥기	오후 4:42:11	오후 10:46:09	06:03	04:46	지각		
33044	R&D	전임연구원	류보기	오후 4:54:49	오전 3:29:27	10:34	09:29	지각/이근		
38984	생산	디리	박상연	오후 4:44:05	오후 9:06:37	04:22	03:06	지각		
42110	R&D	전임연구원	오숙경	오후 5:25:35	오후 8:39:59	03:14	02:39	지각		
50979	생산	디리	장기태	오후 4:28:38		00:00	00:00	지각		
59644	M&S	디리	류경필	오후 6:45:59	오후 10:26:49	03:40	00:00	지각		
61037	경영기획	디리	윤재경			00:00	00:00			
64259	M&S	과장	박형철	오후 4:33:19	오후 8:05:00	03:31	02:05	지각		
64466	경영기획	사원	박기성	오후 5:32:39	오후 7:49:15	02:16	01:49	결근		
64999	M&S	부장	이준식			00:00	00:00			
65469	경영기획	사원	이정훈			00:00	00:00			

2006년 8월 25일 월요일 오전 11:51:01

Page 9 of 31

-  을 눌러 각종 형태의 파일로 저장합니다.
-  을 눌러 작성된 보고서를 출력합니다.

10.6. 보고서 자료 수정

근태 미 입력 시 또는 기타 필요에 따라 관리자가 사용자의 출입/근태 기록을 추가 및 수정할 수 있습니다.

- 일일 보고서 또는 개인별 보고서 화면에서 특정 보고자료를 더블클릭 아래와 같이 자료 수정을 위한 화면이 표시됩니다.

자료 수정

기준날짜 2007-06-29 이름 서동석
 사용자 ID 853 결과 결근

이벤트 날짜	이벤트 시간	이벤트	해당 장치
2007-06-29	오전 8:07:53	Start	[3143] 새 BioSt...
2007-06-29	오후 12:07:53		[3143] 새 BioSt...
2007-06-29	오후 2:07:53	Start Break	[3143] 새 BioSt...
2007-06-29	오후 3:07:53	End Break	[3143] 새 BioSt...
2007-06-29	오후 7:07:53	End	[3143] 새 BioSt...

이벤트 속성

날짜 당일 시간 오후 7:07:53
 이벤트 End 장치 [3143] 새 BioStation

이벤트 추가 이벤트 수정 이벤트 삭제

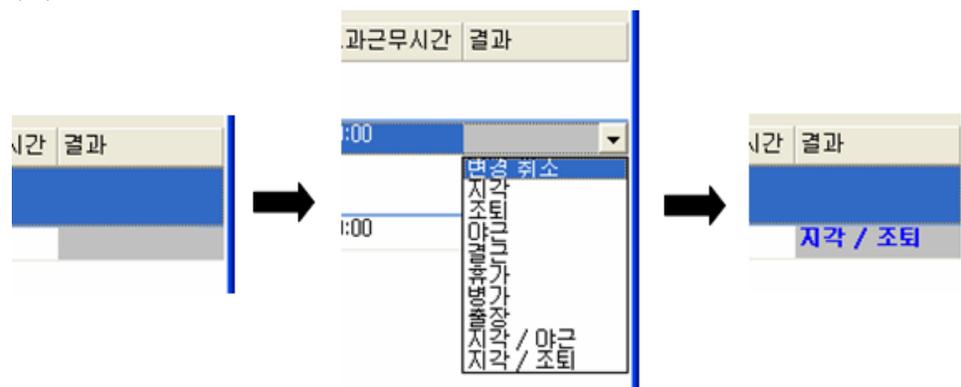
이 설정을 변경한 뒤에 '모두 새로 작성'을 체크하게 되면 수정한 내용이 초기화 됩니다.

적용 닫기

- 이벤트 속성 입력란에 추가 또는 변경코자 하는 값을 입력한 후 이벤트 추가 또는 이벤트 수정 버튼을 누릅니다.
- 적용 버튼을 눌러 추가 또는 변경된 내용으로 보고서에 반영시킵니다. 이렇게 관리자에 의해 변경된 결과는 '결과' 난이 회색으로 표시됩니다.

날짜	ID	부서	직책	이름	출근	퇴근	근무시간	초과근무시간	결과
날짜: 2007-06-29									
2007-06-29	853			서동석	오전 8:07:53	오후 7:07:53	09:00	00:00	결근
날짜: 2007-06-30									
2007-06-30	853			서동석			00:00	00:00	결근

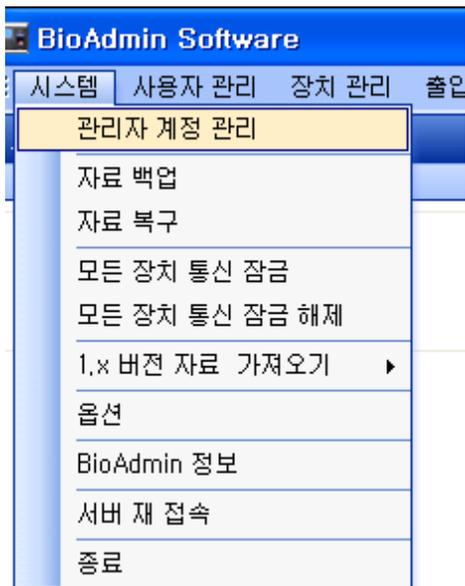
- 보고서에서 바로 결과를 수정할 수 있습니다. 보고서의 '결과' 부분을 한 번 클릭하면 그림과 같이 표시할 결과를 선택할 수 있는 리스트가 표시가 됩니다. 이렇게 수정된 결과는 굵은 글씨로 표시가 되며 변경 여부를 쉽게 확인할 수 있습니다.



Note: 보고서 자료를 수정한 뒤에 “모두 새로 작성”을 체크하지 않고 보고서 목록을 갱신해야 변경된 내용이 보고서에 반영됩니다. 만약 “모두 새로 작성”을 체크하면 자료를 수정하기 전 상태로 복구됩니다.

11. 메뉴 바의 기능들

11.1. 시스템



11.1.1. 관리자 계정 관리

BioAdmin 로그인 시의 관리자를 추가하거나, 기존 관리자의 권한 및 패스워드를 변경합니다.

11.1.2. 자료 백업

옵션 메뉴상의 자동 백업 이외에, 수동으로 백업 파일을 만듭니다. 백업 파일은 서버가 설치된 경로에 날짜_일련번호의 형태로 저장됩니다.

11.1.3. 자료 복구

서버/클라이언트 형태로 BioAdmin 소프트웨어가 변경된 이후 자료 복구는 서버가 설치된 PC에 생성된 백업 파일을 복사하는 것으로 가능합니다.

자료를 복구하기 위해서는 먼저 생성된 백업 파일이 있어야 가능하며, 날짜_일련번호의 형식으로 생성된 폴더 내에 있는 파일을 서버가 설치된 경로에 복사하는 것으로 백업 당시의 상태로 모든 데이터를 되돌릴 수 있습니다. 이 과정은 모든

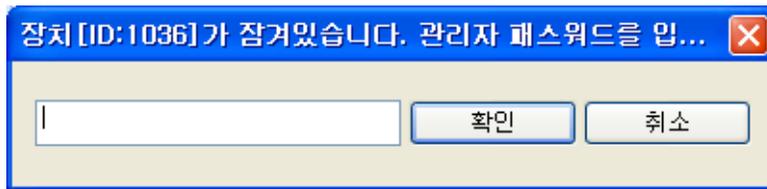
관리자 정보 및 사용자 정보, 규칙 및 로그 정보를 모두 해당 시점으로 복원하게 되며, 복원 시점 이후의 데이터는 사라집니다.

11.1.4. 모든 장치 잠금

BioAdmin 소프트웨어를 사용하면서 연결된 모든 BioEntry 와 BioStation을 잠금/해제할 수 있습니다. 모든 장치 잠금 메뉴를 클릭하면, 연결된 모든 BioEntry 와 BioStation 은 차단되며, 차단된 후에는 잠금 해제 명령을 제외한 어떠한 외부 패킷에도 반응하지 않습니다. 단, 서버와 연결된 BioStation의 경우에는 장치 잠금을 지원하지 않습니다.

11.1.5. 모든 장치 잠금 해제

모든 리더 잠금 해제 메뉴를 클릭하여 차단된 모든 BioEntry 와 BioStation을 잠금 해제할 수 있습니다. 만약 잠금 패스워드가 설정되었다면 잠금 해제하기 위해서 패스워드를 입력해야 합니다.



11.1.6. BioAdmin 1.X 자료 가져오기



- **BioAdmin 1.X 자료 가져오기** 메뉴를 클릭하면 BioAdmin 소프트웨어 버전 1.XX을 사용하면서 생성한 예전 사용자 데이터와 로그 데이터를 가져올 수 있습니다.

Note: 이 메뉴는 BioAdmin 소프트웨어 버전 3.0의 처음 실행 시에만 사용될 수 있습니다. 이 메뉴를 실행해서 예전 데이터를 가져올 때, 기존에 있던 데이터를 삭제한 뒤에 새로 작성하기 때문입니다.

11.1.7. 옵션

선택 사항 메뉴는 다음의 기능들을 지원합니다..

- 장치 시간 설정
- 자동 잠금
- 백업
- 보안 옵션
- 지문 옵션

- Mifare 설정
- 버전 관리 - 출입 통제 기능 선택

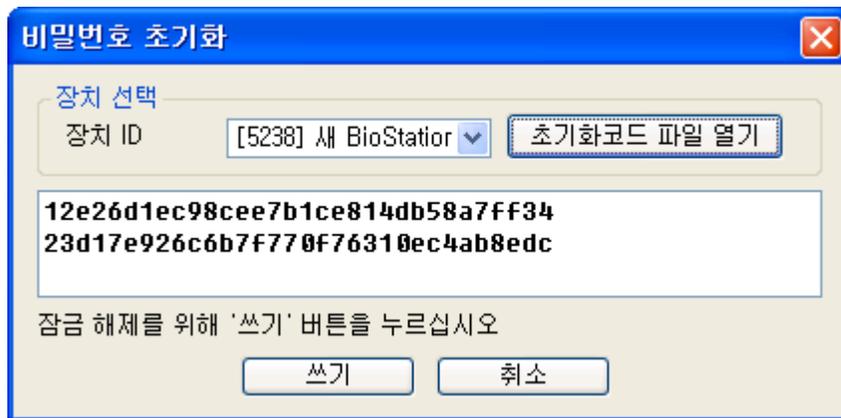
- 장치 시간 설정
선택 사항 윈도우에서 시작할 때 PC 시간으로 설정 체크 박스를 표시하여, 연결된 모든 장치들의 시간을 호스트 PC의 시간에 맞출 수 있습니다.
- 자동 잠금
보안을 강화하기 위해 BioEntry와 BioStation, BioLite Net 은 패스워드에 의해 차단할 수 있습니다. 차단된 BioEntry와 BioStation, BioLite Net 이 네트워크상에서 발견되면, BioAdmin 소프트웨어에서 리더를 잠금 해제하기 위해서는 관리 패스워드를 요구합니다. 잠금 메커니즘은 이 윈도우에서 끝날 때 모든 장치 잠금 체크 박스나 메뉴 바에 시스템 메뉴 아래 모든 장치 잠금 메뉴에 의해 설정됩니다. 설정되면 BioAdmin 소프트웨어는 프로그램 종료 시 리더를 차단합니다.
 - 잠금 패스워드 변경 버튼을 누르면 패스워드 관리 창이 나타납니다.

BioEntry와 BioStation, BioLite Net 에 대한 잠금 패스워드는 변경 버튼을 누른 후 신규 패스워드를 입력하여 변경할 수 있습니다.

Note: BioAdmin 소프트웨어는 잠금 패스워드를 저장하지 않으므로, 관리자는 잠금 메커니즘을 사용할 때는 패스워드를 반드시 기억해야 합니다.

- 차단된 리더 해제: BioEntry를 차단하였으나 패스워드를 분실하여 해제하지 못하면, 다음 과정을 수행해야 합니다. **패스워드 초기화 코드 가져오기** 버튼을 이용하여 패스워드 초기화 코드 파일을 얻어서 기술 지원 팀 (support@suprema.co.kr)에 보내기 바랍니다.

- 기술 지원 팀은 패스워드 초기화 코드에 해당하는 해제 코드 파일을 보낼 것입니다. **패스워드 초기화 코드를 이용해 패스워드 초기화** 버튼을 눌러 BioEntry와 BioStation, BioLite Net을 잠금 해제 할 수 있습니다. 그러면 리더는 해제되고 패스워드는 기본값(null)으로 변경됩니다.



- 백업 옵션

- 기본 백업 폴더: 데이터베이스에 대한 기본 백업 폴더는 선택 사항 페이지에서 정할 수 있습니다. 관련된 백업 파일들은 정해진 폴더에 저장될 것입니다. 단, 4.0 이상의 버전에서는 이 옵션에서 백업 생성 경로를 설정할 수 없으며, 서버가 설치된 경로에 백업 파일이 생성됩니다.
- 자동 백업 옵션: 자동 백업 체크 박스를 표시하면, **BioAdmin** 소프트웨어를 종료할 때마다 자동으로 백업 데이터베이스를 저장할 수 있습니다. 백업 데이터베이스의 생성은 선택한 옵션에 따라서 하루에 한번 혹은 한 달에 한번 생성되며, 프로그램이 종료되는 시점에 기존 백업 데이터베이스를 갱신합니다. 단, 4.0 이상의 버전에서는 수동 백업과 마찬가지로 서버가 설치된 경로에 자동으로 백업 파일이 생성됩니다.

Note: 자동 백업 옵션은 **BioAdmin** 소프트웨어를 종료할 때를 기준으로 데이터를 저장합니다. 따라서, **BioAdmin** 을 실행하지 않고 있거나, 혹은 **BioAdmin**을 실행하고 종료하지 않을 경우에는 데이터를 저장하지 않습니다. 또한 서버와 동일한 PC이며 **Microsoft Access** 데이터베이스를 사용하는 경우에만 지원하고 있습니다.

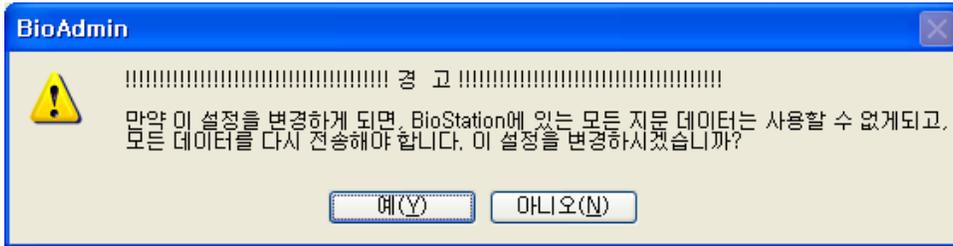
- 보안 옵션

- 바이오 정보 보호 가이드는 지문이나 홍채 인식 등의 바이오인식 시장이 급격하게 확대됨에 따라 개인의 바이오정보와 인권의 보호를 위해 2007년 9월 정보통신부와 한국정보보호진흥원에서 정한 것으로, 이를 준수하도록 보호원칙을 제시하였으며, 이에 따라 지문인식 시스템을 운영하는 것을 권장합니다
- 바이오 정보 보호 가이드 라인에 대한 자세한 정보는 한국정보보호진흥원 홈페이지 (KISA 홈페이지 <http://www.1336.or.kr>) 에서 확인할 수 있습니다.
- 바이오 정보 보호 가이드 라인은 관리자가 선택하여 시스템에 적용할 수 있으며, 이 옵션을 사용하게 되면 호스트 PC 와 **BioStation** 및 **BioEntry Plus**에 저장하는 사용자 지문 데이터를 사용자가 정의한 암호화 키를 사용하여 암호화 한 후 저장합니다. 지문에서 추출한 특징 데이터의 템플릿 자료를 암호화 함으로서 한층 강화된 보안 수준을 실현할 수 있습니다.

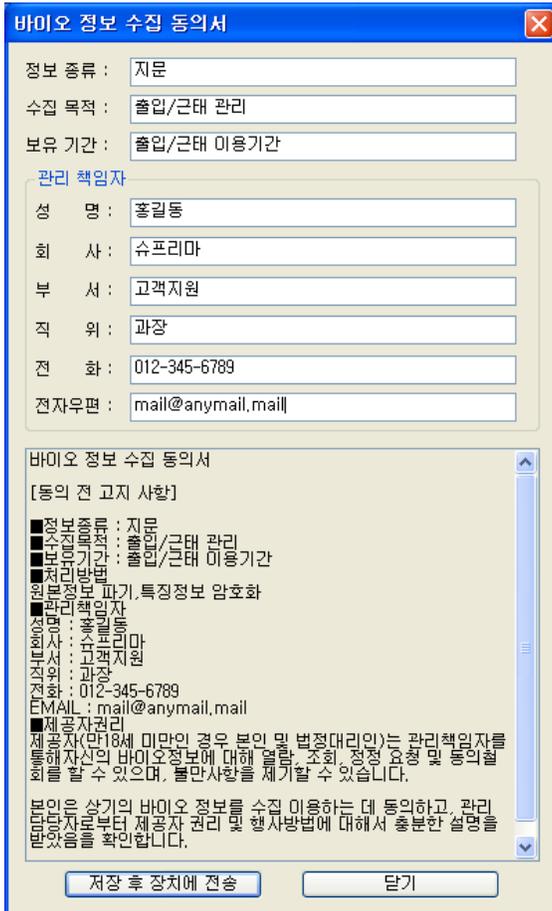
- 이 옵션을 변경할 때에는 장치에 사용자 지문 데이터가 없는 상태에서만 가능합니다. 장치 사용 중에 설정을 변경하게 된다면 BioAdmin은 저장된 사용자 지문 데이터를 모두 삭제한 뒤에 변경을 시도합니다.



- 보안옵션을 사용할 경우 바이오정보보호가이드 옵션을 체크합니다.
- 바이오정보보호가이드 옵션을 선택하면 아래와 같은 경고 창이 주 화면에 표시됩니다. 암호화 설정을 계속하고자 할 경우 예 버튼을 누릅니다.



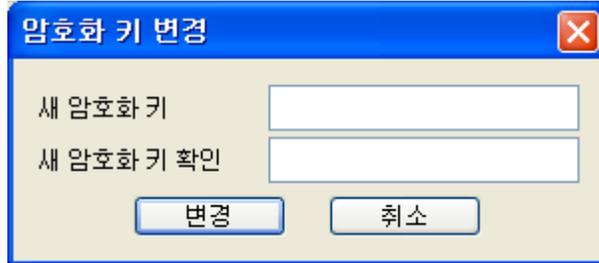
- 관리책임자 버튼을 눌러 바이오정보 관리 책임자 정보와 사용자 고지 사항에 대한 정보를 입력하고 장치로 전송합니다.



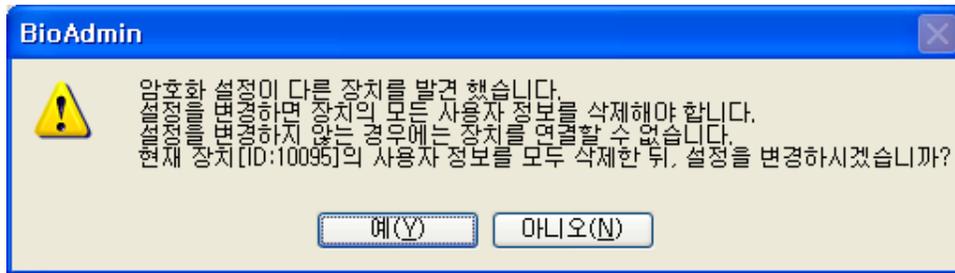
- 암호화 키 변경 버튼을 누릅니다.



- 암호화 키를 입력합니다.



- 변경버튼을 누릅니다.
- **확인** 버튼을 누릅니다.
- **취소**를 누르거나 암호화 설정을 변경하는 도중에 문제가 발생하여 사용자 지문 데이터 변환을 완료하지 못하는 경우에는 암호화 설정 전의 상태로 되돌아 갑니다.
- 암호화 키를 변경할 때마다 연결된 모든 장치에 대해 암호화 키 설정작업을 거쳐야 합니다. 새로이 장치를 추가할 때마다 암호화 키 설정 작업을 거쳐야 하며 이 때에는 **BioStation** 에 저장된 모든 사용자 지문이 삭제됩니다. 따라서, 암호화 완료 후 사용자 정보를 **BioStation**으로 전송해야 합니다.
- 암호화를 사용할 경우에는 암호화 키를 변경하는 것을 권장 합니다. 한번 변경하고 나서는 암호화 키를 반드시 기억하지 않아도 됩니다.
- 암호화 키는 **31**글자 이내로 사용해야 합니다.
- 여러 대의 **BioStation** 에 암호화 설정을 적용하는 도중 정전이나 기타 문제의 발생으로 일부 **BioStation** 에 암호화 설정이 전송되지 않았을 경우에는 **BioAdmin**을 다시 시작하면 남은 장치에 대해 암호화 설정을 전송할 수 있습니다.
- 암호화 옵션은 주의해서 사용해야 하며 만약 장치간에 서로 다른 암호화 키를 사용하게 된다면 사용자 지문 데이터를 사용하지 못하게 될 수도 있습니다.
- 호스트 **PC** 에 저장된 암호화 키와 **BioStation**에 저장된 암호화 키가 서로 다르거나, 어느 한쪽만 이 암호화 옵션을 사용할 경우에는 그러한 **BioStation** 이 네트워크에 연결 될 때마다 아래와 같은 경고 창이 표시됩니다. 이때 '아니오'를 선택한다면, **BioAdmin**은 해당 **BioStation**을 사용할 수 없도록 접속을 끊게 됩니다.

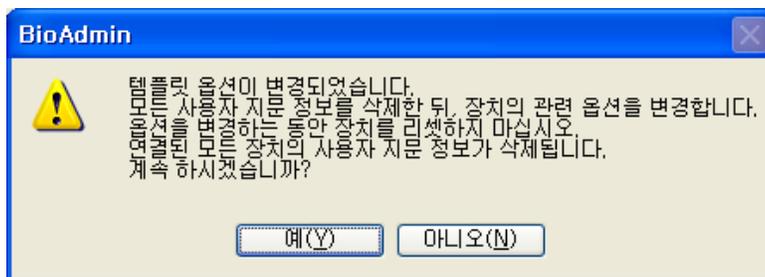
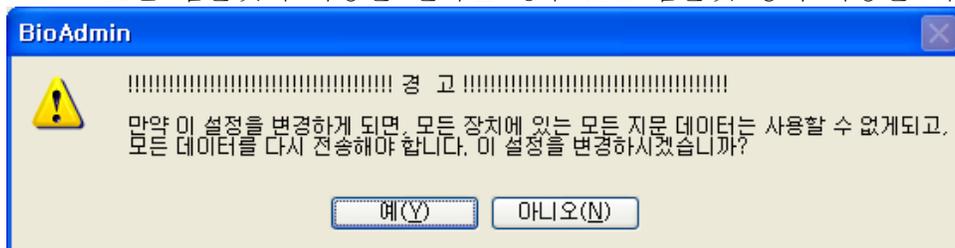


● 지문 옵션

- 지문 옵션은 슈프리마 템플릿 형식 데이터와 ISO 19794-2 표준 템플릿을 사용할 수 있도록 변경해주는 옵션입니다.
- 이 지문 옵션은 단말기에 지문 데이터가 하나도 없을 경우에만 설정이 가능합니다. 그렇기 때문에 이 옵션을 변경하면 BioAdmin은 현재 단말기 및 DB에 존재하는 모든 지문 데이터를 삭제한 뒤에 옵션을 적용하도록 되어 있습니다.



- 표준 템플릿의 사용을 원하는 경우 ISO 템플릿 형식 사용을 체크합니다.



- 2번의 경고 메시지를 나타낸 후, 이 옵션이 적용되면 BioAdmin은 먼저 사용자 DB에 있는 지문 데이터를 모두 삭제합니다.
- 이어서 BioAdmin은 연결된 모든 단말기에 있는 사용자 정보를 삭제한 뒤 ISO 템플릿 형식 옵션을 변경합니다.
- ISO 표준 템플릿 데이터를 지원하지 않는 단말기는 이 옵션을 켜고 난 뒤에는 사용할 수가 없습니다. 펌웨어를 업그레이드 하려고 하는 경우라면 이 옵션을 켜기 전에 업그레이드를 실행해 주십시오.

● Mifare 설정

Mifare 설정

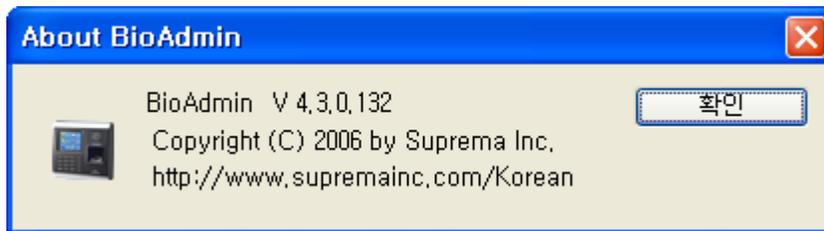
- BioEntry Smart 형식 BioStation Mifare / BioEntry Plus Mifare 형식

- BioAdmin 4.3은 BioStation Mifare와 BioEntry Plus Mifare, BioLite Net Mifare를 지원합니다.
- BioStation Mifare와 BioEntry Plus Mifare, BioLite Net Mifare에 사용되는 Mifare 카드는 BioEntry Smart의 스마트 카드와 호환되지 않기 때문에 BioAdmin을 사용하기 전에 어떤 데이터 형식을 사용할 것인지 설정을 해주어야 합니다.
- 이 옵션을 변경하더라도 장치를 사용하여 스마트 카드를 쓰고 읽는 기능은 사용 가능합니다. 단, USB Card Writer를 사용하는 경우 설정한 옵션에 따라서 읽고 쓸 수 있는 카드 형식이 결정됩니다.
-
- 버전관리
 - BioAdmin 4.2 전용 출입통제를 사용하려면 체크를 합니다.
 - 자세한 내용은 6.4 출입구역 설정을 참조하시기 바랍니다. 이 기능을 사용하려면 프로그램을 재 실행 하여야 하며, 이전 기능으로 되돌릴 수 없으니 주의하시기 바랍니다.

버전 관리

- BioAdmin V4.2 전용 출입 통제 기능 사용(BioEntry Smart/Pass 는 지원하지 않습니다.)

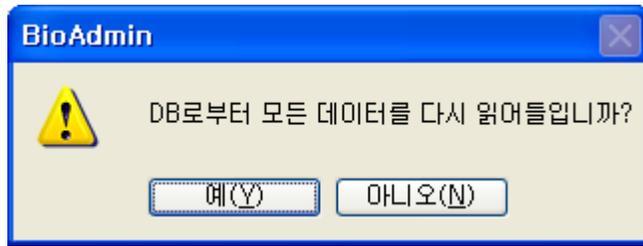
11.1.8. BioAdmin 정보



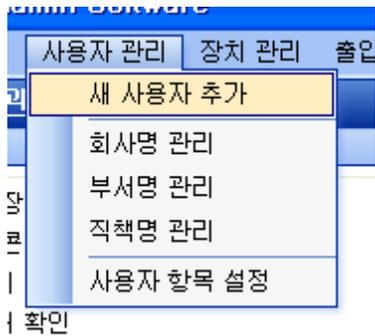
메뉴 바 상의 BioAdmin 정보는 현재 사용중인 BioAdmin에 대한 정보를 나타냅니다.

11.1.9. 서버 재 접속

통신 상의 이유 등으로 서버와 통신이 원활하지 않거나, 특정 장치와의 통신에 문제가 있다고 판단되면 이 메뉴를 통해서 서버와 접속을 재 시도할 수 있습니다. 이 경우에 서버로부터 모든 데이터를 다시 읽어올 수 있습니다.



11.2. 사용자 관리

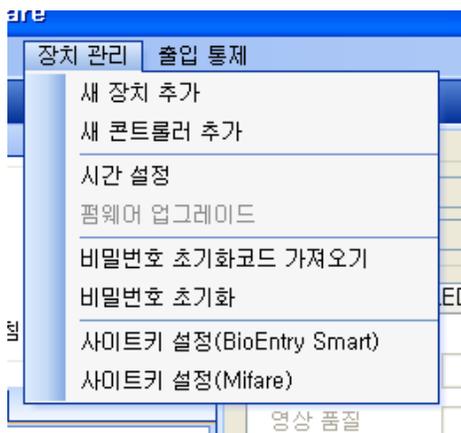


메뉴 바 상의 사용자 관리 메뉴는 다음의 기능들을 지원합니다..

- 새 사용자 추가
- 회사 명 관리
- 부서 명 관리
- 직책 명 관리
- 사용자 항목 설정

구체적인 설정방법은 제 5장 사용자 관리의 설명을 참조하십시오.

11.3. 장치 관리



메뉴 바 상의 장치 관리 메뉴는 다음의 기능들을 지원합니다..

- 새 장치 추가
- 새 컨트롤러 추가

- 시간 설정
- 펌웨어 업그레이드
- 패스워드 초기화 코드 가져오기
- 패스워드 초기화
- 사이트 키 설정

새 장치 추가, 새 컨트롤러 추가, 패스워드 초기화 코드 가져오기, 패스워드 초기화 등 에 대한 구체적인 설정방법은 제 6장 장치 관리의 설명을 참조하십시오.

11.3.1. 시간 설정

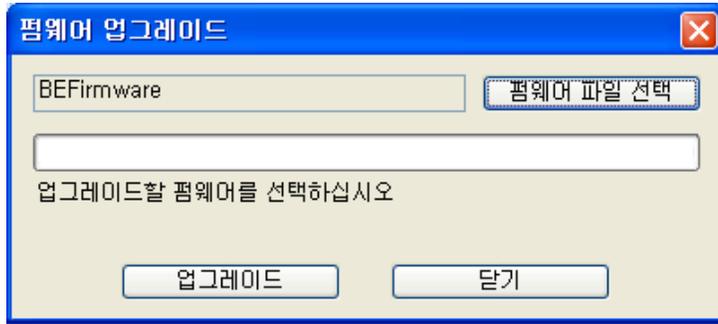


- 연결된 모든 장치의 시간을 호스트 PC의 시간에 맞출 수 있습니다. 시스템 → 옵션 → 장치 시간 설정 상의 시작할 때 PC 시간으로 설정 체크 박스를 이미 표시하였다면, 이 메뉴에서 시간을 맞추는 필요가 없습니다.

11.3.2. 펌웨어 업그레이드



- 펌웨어 업그레이드 메뉴를 선택하면, 펌웨어 업그레이드를 위한 팝업 윈도우가 나타납니다.

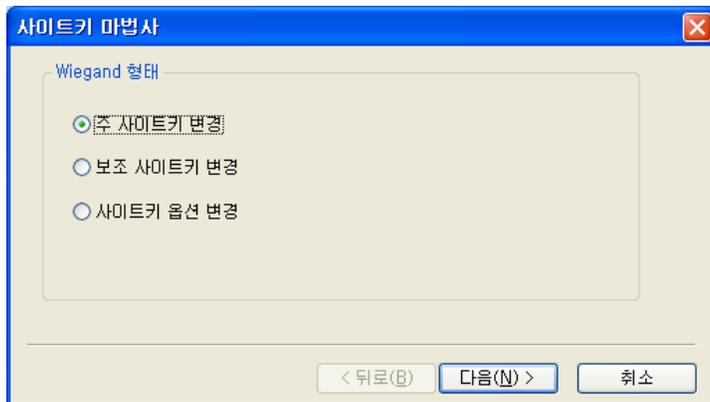


- 펌웨어 찾기 버튼을 클릭하여 펌웨어 파일을 선택합니다.
- 펌웨어 업그레이드 버튼을 클릭하여 업그레이드를 실행합니다.
- 업그레이드 과정에서 장치가 꺼지거나 리셋 되면 복구가 불가능할 수도 있습니다.
- 펌웨어 업그레이드는 한 개의 장치에 대해서 처리됩니다. 그룹이나 모든 리더를 선택할 수 없습니다.

구체적인 설정방법은 제 5장 사용자 관리 의 설명을 참조하십시오.

Note: 펌웨어 업그레이드가 완료되면 **BioEntry**와 **BioStation**은 자동으로 재 부팅 되어 네트워크에 연결됩니다. 업그레이드로 인해 **BioEntry** 또는 **BioStation** 이 재 부팅 되고 나서 약 5초 ~10초 가량은 가급적 다른 작동을 하지 않을 것을 권장합니다..

11.3.3. 사이트 키 설정(BioEntry Smart)



권한이 없는 출입을 방지하기 위해서, 스마트카드는 48 비트의 사이트 키로 암호화되어 있습니다. **BioEntry™** 리더가 스마트카드를 해독하기 위해서는, 리더에 저장된 사이트 키와 카드에 저장된 사이트 키가 일치해야 합니다. 사용자는 **BioEntry™** 리더에 두 개의 사이트 키를 저장하고 두 개의 고급 옵션을 선택할

수 있습니다. **보조 사이트 키 사용** 옵션을 선택한다면, BioEntry 가 스마트카드를 해독할 때 주 사이트 키와 보조 사이트 키를 모두 시도하게 됩니다. 이 옵션을 선택하지 않았다면, 주 사이트 키만이 사용됩니다. **자동 갱신** 옵션은 스마트카드의 키를 변경할 때 유용합니다. 이 옵션이 선택되면, 스마트카드가 보조 사이트 키로 암호화됐을 때 리더가 주 사이트 키로 다시 암호화할 수 있습니다.

Note: 사이트 키는 최대한 주의를 기울여 다루어야 합니다. 사이트 키가 노출되면 전체 시스템이 더 이상 보안되지 않습니다.

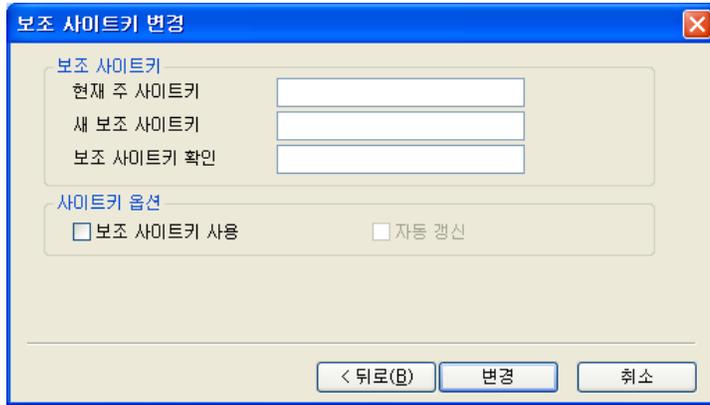
- 주 사이트 키

주 사이트 키를 변경하기 위해서는 현재와 새로운 주 사이트 키를 입력해야 합니다. **자동 갱신** 옵션 이외에, 다음과 같은 옵션들도 선택할 수 있습니다.

- **현재 주 사이트 키를 보조 사이트 키로 설정:** 주 사이트 키를 바꾸기 전에 보조 사이트 키를 현재 주 사이트 키로 변경합니다.

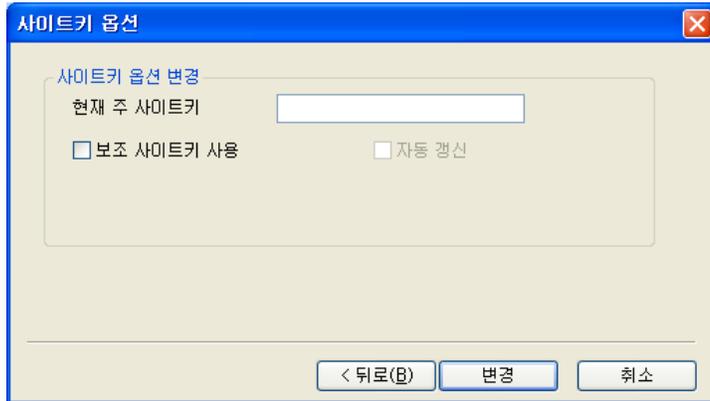
- 보조 사이트 키

보조 사이트 키를 변경하기 위해서는 현재 주 사이트 키와 새로운 보조 사이트 키를 입력해야 합니다.

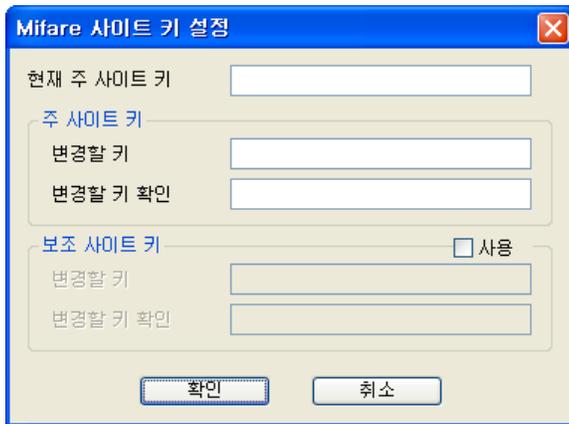


- 사이트 키 옵션

키 옵션만을 바꿀 수 있습니다. 이 경우에 현재 주 사이트 키만 입력하면 됩니다.



11.3.4. 사이트 키 설정(Mifare)

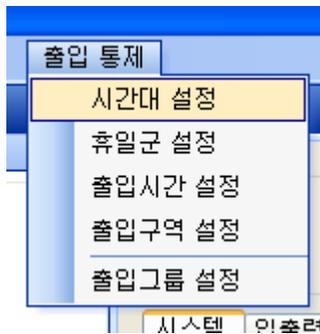


권한이 없는 출입을 방지하기 위해서, Mifare카드는 48 비트의 사이트 키로 암호

화되어 있습니다. BioStation™ / BioEntry™ Plus / BioLite Net 리더가 Mifare카드를 해독하기 위해서는, 리더에 저장된 사이트 키와 카드에 저장된 사이트 키가 일치해야 합니다. 사용자는 BioStation™ / BioEntry™ Plus / BioLite Net 리더에 두 개의 사이트 키를 저장하고 두 개의 고급 옵션을 선택할 수 있습니다. **보조 사이트 키 사용** 옵션을 선택한다면, BioStation™ / BioEntry™ Plus / BioLite Net 이 Mifare카드를 해독할 때 주 사이트 키와 보조 사이트 키를 모두 시도하게 됩니다. 이 옵션을 선택하지 않았다면, 주 사이트 키만이 사용됩니다.

Note: 사이트 키는 최대한 주의를 기울여 다루어야 합니다. 사이트 키가 노출되면 전체 시스템이 더 이상 보안되지 않습니다.

11.4. 출입 통제



메뉴 바 상의 출입통제 메뉴는 다음의 기능들을 지원합니다..

- 시간 대 설정
- 휴일 군 설정
- 출입 시간 설정
- 출입 구역 설정
- 출입 그룹 설정

BioAdmin 4.2 전용 출입통제 방식으로 전환한 경우에는 출입구역 설정이 비활성화 되어 보입니다.

구체적인 설정방법은 제 7장 출입 통제의 설명을 참조하십시오.

기술 문의

(주)슈프리마

(463-863) 경기도 성남시 분당구 정자동 파크뷰 오피스타워 16층

전화: 031-783-4502

팩스: 031-783-4503

홈페이지: <http://www.suprema.co.kr>

영업문의: sales@suprema.co.kr

기술문의: support@suprema.co.kr
