

BioStar 1.92

관리자 설명서

01 BioStar 시스템에 관하여	1
1.1 논리적 구성.....	4
1.2 출입 통제 기능.....	6
1.2.1 사용자 인증.....	6
1.2.2 사용자 관리.....	7
1.2.3 출입그룹 관리.....	7
1.2.4 장치 관리.....	7
1.2.5 출입문 및 리프트 관리	7
1.2.6 구역 관리.....	8
1.2.7 근태 관리.....	8
1.2.8 IP 카메라 및 NVR 서버 관리	8
1.3 1.x 장치와 2.x 장치의 기능 차이.....	9
02 BioStar 설치하기	11
2.1 시스템 요구사항	11
2.2 BioStar 서버와 클라이언트를 한번에 설치하기	12
2.3 BioStar 서버 설치하기	13
2.3.1 MySQL 서버 설정하기.....	16
2.3.2 BioStar 서버 설정하기	16
2.4 BioStar 클라이언트 설치하기	18
2.4.1 처음으로 BioStar 에 접속하기	19
2.5 BioStar 의 화면 구성.....	21
2.6 BioStar 인터페이스 변경하기.....	21
2.6.1 테마 변경하기.....	21
2.6.2 도구 표시줄 변경하기	21
2.6.3 이벤트 보기 변경하기	22
2.6.4 서체 변경하기.....	22
2.7 BioAdmin 에서 BioStar 로 데이터베이스 옮기기.....	23
03 BioStar 설정하기	24
3.1 관리자 계정 만들기.....	24
3.1.1 관리자 권한	24
3.1.2 관리자 계정을 추가하고 설정하기	25
3.1.2.1 관리자 계정 추가하기	25
3.1.2.2 관리자 계정의 권한이나 비밀번호 변경하기.....	26

3.1.2.3	임의의 관리자 권한 추가하기	27
3.2	장치 설정하기	28
3.2.1	장치 추가하기	28
3.2.2	슬레이브 장치를 검색하고 추가하기	30
3.2.3	RF 장치 추가하기	31
3.2.4	무선 랜으로 장치 연결하기	32
3.2.5	BioStation 설정하기	34
3.2.6	BioEntry Plus 및 BioEntry W 설정하기	35
3.2.6.1	커맨드 카드 발급하기	36
3.2.7	BioLite Net 설정하기	36
3.2.8	Xpass 및 Xpass S2 설정하기	37
3.2.8.1	커맨드 카드 발급하기	38
3.2.9	X-Station 설정하기	38
3.2.10	BioStation T2 설정하기	39
3.2.11	FaceStation 설정하기	40
3.2.12	BioStation 2 설정하기	41
3.2.13	BioStation A2 설정하기	42
3.2.14	BioStation L2 설정하기	44
3.2.15	BioEntry W2 설정하기	45
3.2.16	위갠드 형식 변경하기	46
3.2.16.1	26 비트 표준 위갠드 형식 설정하기	47
3.2.16.2	패스 스루 Wiegand 형식 설정하기	47
3.2.16.3	사용자 지정 위갠드 형식 설정하기	48
3.3	출입문 설정하기	49
3.3.1	출입문 추가하기	49
3.3.2	출입문에 장치 연결하기	49
3.3.3	출입문 설정하기	50
3.3.4	출입문 그룹 만들기	51
3.4	리프트 설정하기	51
3.4.1	리프트 추가하기	51
3.4.2	리프트에 출입 장치 연결하기	51
3.4.3	리프트 설정하기	52
3.4.4	리프트에 사용자 추가하기	52
3.4.5	장치에 설정 정보 전송하기	53
3.5	구역 설정하기	54
3.5.1	사용할 구역을 결정하기	54
3.5.2	구역을 추가하고 설정하기	55
3.5.2.1	구역 추가하기	55
3.5.2.2	구역에 장치 추가하기	55
3.5.2.3	구역의 입력 설정하기	57

3.5.2.4	경보 동작과 출력 설정하기	58
3.5.2.5	경비 개시와 경비 해제 설정하기	58
3.5.2.6	외부 I/O 연동 설정하기	60
3.5.2.7	출입통제 그룹 선택하기	61
3.5.2.8	구역 이벤트 보기	61
3.6 사용자 설정하기	61	
3.6.1	사용자 계정 만들기	61
3.6.2	지문 등록하기	63
3.6.2.1	지문 스캔하기	63
3.6.2.2	지문 등록하기	64
3.6.2.3	커맨드 카드를 이용하여 사용자 등록하기	65
3.6.3	얼굴 이미지 캡처하기	66
3.6.4	출입 카드 발급하기	67
3.6.4.1	EM4100 카드 발급하기	67
3.6.4.2	HID 근접식 카드 발급하기	68
3.6.4.3	FeliCa 카드 발급하기	69
3.6.4.4	MiFARE, DESFire, iCLASS CSN 카드 발급하기	69
3.6.4.5	MIFARE, DESFire, iCLASS 템플릿 카드 발급하기	70
3.6.4.6	MiFARE, DESFire, iCLASS 사이트 키 변경하기	71
3.6.4.7	MiFARE 레이아웃 편집하기	72
3.6.4.8	DESFire 레이아웃 편집하기	73
3.6.4.9	iCLASS 레이아웃 편집하기	74
3.6.4.10	USB 기반 리더로부터 카드 정보 읽기	75
3.6.5	사용자 데이터 전송하기	75
3.6.5.1	사용자 정보를 장치에 전송하기	75
3.6.5.2	모든 사용자 정보 동기화하기	76
3.6.5.3	장치에서 사용자 정보 가져오기	76
3.6.5.4	장치에서 사용자 정보 병합하여 가져오기	77
3.6.6	사용자 데이터 암호화하기	78
3.7 출입시간 설정하기	80	
3.7.1	출입시간 만들기	80
3.7.2	휴일군 만들기	81
3.8 출입그룹 설정하기	82	
3.8.1	출입그룹 추가하기	82
3.8.2	출입그룹에 사용자 추가하기	82
3.8.3	사용자에게 출입그룹 할당하기	83
3.8.4	출입그룹을 장치에 전송하기	84
3.8.5	장치별 출입 그룹 확인하기	84
3.9 근태관리 설정하기	86	
3.9.1	시간구분 추가하기	86
3.9.2	일일규칙 추가하기	87

3.9.3	근무규칙 추가하기.....	88
3.9.4	사용자에게 근무규칙 적용하기.....	90
3.9.5	휴일규칙 추가하기.....	92
3.9.6	개인휴가 추가하기.....	93
3.9.7	사용자 지정 휴가 추가하기.....	94
3.9.8	근태 사용 단말기 설정.....	94
3.10	경보 설정하기.....	96
3.10.1	경보와 경보음 설정하기.....	96
3.10.1.1	경보 동작 설정하기.....	96
3.10.1.2	임의의 경보음 추가하기.....	96
3.10.2	메일 통지 설정하기.....	97
3.10.3	슬레이브 장치 설정하기.....	99
3.10.3.1	슬레이브 장치에 내보내는 출력 설정하기.....	99
3.10.3.2	슬레이브 장치에서 받아들이는 입력 신호 설정하기.....	100
3.11	카메라 설정.....	101
3.11.1	NVR 서버 추가하기.....	102
3.11.2	IP 카메라 추가하기.....	104
3.11.3	IP 카메라 설정하기.....	106
04 BioStar 관리하기.....		107
4.1 실시간으로 이벤트 감시하기.....		107
4.1.1	실시간으로 소집구역 감시하기.....	109
4.1.2	카메라를 통해 실시간으로 감시하기.....	110
4.2 이벤트 기록 보기.....		110
4.2.1	이벤트 로그 업로드 하기.....	111
4.2.2	사용자, 출입문, 구역 창에서 이벤트 로그 보기.....	111
4.2.3	모니터링 창에서 이벤트 로그 보기.....	112
4.2.4	액세스 로그 보기.....	113
4.3 비주얼 맵으로 출입문 감시하기.....		114
4.3.1	비주얼 맵 추가하기.....	114
4.3.2	비주얼 맵에서 출입문 감시하기.....	116
4.4 출입문, 경보, 장치를 원격으로 제어하기.....		118
4.4.1	출입문을 열거나 닫기.....	118
4.4.2	경보 해제하기.....	118
4.4.3	장치를 잠그거나 잠금 해제하기.....	119
4.4.3.1	연결된 장치를 잠그거나 잠금 해제하기.....	119
4.4.3.2	장치 자동 잠금 설정하기.....	119
4.4.3.3	장치 잠금 초기화하기.....	120

4.5 사용자 관리하기	121
4.5.1 사용자 삭제하기	121
4.5.1.1 커맨드 카드를 이용하여 개별 사용자 삭제하기	121
4.5.1.2 커맨드 카드를 이용하여 모든 사용자 삭제하기	122
4.5.2 사용자를 다른 부서로 이동하기	122
4.5.3 사용자 정의 항목 설정하기	123
4.5.3.1 새로운 정보 항목 추가하기	123
4.5.3.2 기존 정보 항목 편집하기	123
4.5.4 사용자 데이터 내보내기	124
4.5.5 사용자 데이터 가져오기	125
4.6 근태 관리하기	126
4.6.1 근태 상황 확인하기	126
4.6.2 근태 보고서 생성하기	127
4.6.3 근태 보고서 수정하기	129
4.6.4 근태 보고서 인쇄 및 내보내기	130
4.7 장치 관리하기	132
4.7.1 장치 제거하기	132
4.7.2 장치의 펌웨어 업그레이드하기	132
4.7.3 장치 펌웨어 다운그레이드하기	133
4.8 지문 암호화 사용하기	133
4.9 지문 템플릿 형식 변경하기	134
05 사용자 설정	135
5.1 장치 설정 변경하기	135
5.1.1 BioStation 설정 변경하기	135
5.1.1.1 동작모드 탭	136
5.1.1.2 지문 탭	138
5.1.1.3 네트워크 탭	139
5.1.1.4 출입그룹 탭	140
5.1.1.5 입력 탭	140
5.1.1.6 출력 탭	141
5.1.1.7 인증 거부 리스트 탭	143
5.1.1.8 화면/음성 탭	143
5.1.1.9 근태 탭	145
5.1.1.10 위젯 탭	146
5.1.2 BioEntry Plus 및 BioEntry W 설정 변경하기	146
5.1.2.1 동작모드 탭	146
5.1.2.2 지문 탭	148
5.1.2.3 네트워크 탭	150
5.1.2.4 출입그룹 탭	151

5.1.2.5	입력 탭	151
5.1.2.6	출력 탭	152
5.1.2.7	인증 거부 리스트 탭	154
5.1.2.8	커맨드카드 탭	155
5.1.2.9	화면/음성 탭	155
5.1.2.10	위갠드 탭	156
5.1.3	BioLite Net 설정 변경하기	157
5.1.3.1	동작모드 탭	157
5.1.3.2	지문 탭	158
5.1.3.3	네트워크 탭	159
5.1.3.4	출입그룹 탭	160
5.1.3.5	입력 탭	161
5.1.3.6	출력 탭	162
5.1.3.7	인증 거부 리스트 탭	163
5.1.3.8	화면/음성 탭	163
5.1.3.9	근태 탭	164
5.1.3.10	위갠드 탭	165
5.1.4	Xpass 설정 변경하기	166
5.1.4.1	동작모드 탭	166
5.1.4.2	네트워크 탭	167
5.1.4.3	출입그룹 탭	168
5.1.4.4	입력 탭	168
5.1.4.5	출력 탭	169
5.1.4.6	인증거부리스트	170
5.1.4.7	커맨드카드 탭	170
5.1.4.8	화면/음성 탭	171
5.1.4.9	위갠드 탭	172
5.1.5	Xpass S2 설정 변경하기	172
5.1.5.1	동작모드 탭	172
5.1.5.2	네트워크 탭	173
5.1.5.3	출입그룹 탭	174
5.1.5.4	입력 탭	174
5.1.5.5	출력 탭	175
5.1.5.6	커맨드카드 탭	176
5.1.5.7	화면/음성 탭	177
5.1.5.8	위갠드 탭	178
5.1.6	X-Station 설정 변경하기	178
5.1.6.1	동작모드 탭	178
5.1.6.2	카메라 탭	180
5.1.6.3	네트워크 탭	180
5.1.6.4	출입그룹 탭	181
5.1.6.5	인터폰 탭	182
5.1.6.6	입력 탭	183
5.1.6.7	출력 탭	184

5.1.6.8	인증 거부 리스트 탭.....	185
5.1.6.9	화면/음성 탭.....	185
5.1.6.10	근태 탭.....	186
5.1.6.11	위갠드 탭.....	187
5.1.7	BioStation T2 설정 변경하기.....	188
5.1.7.1	동작모드 탭.....	188
5.1.7.2	지문 탭.....	190
5.1.7.3	카메라 탭.....	191
5.1.7.4	네트워크 탭.....	191
5.1.7.5	출입그룹 탭.....	193
5.1.7.6	인터폰 탭.....	193
5.1.7.7	입력 탭.....	194
5.1.7.8	출력 탭.....	195
5.1.7.9	인증 거부 리스트 탭.....	196
5.1.7.10	화면/음성 탭.....	196
5.1.7.11	근태 탭.....	198
5.1.7.12	위갠드 탭.....	199
5.1.8	FaceStation 설정 변경하기.....	199
5.1.8.1	동작모드 탭.....	199
5.1.8.2	얼굴 탭.....	201
5.1.8.3	카메라 탭.....	202
5.1.8.4	네트워크 탭.....	202
5.1.8.5	출입그룹 탭.....	203
5.1.8.6	인터폰 탭.....	204
5.1.8.7	입력 탭.....	204
5.1.8.8	출력 탭.....	205
5.1.8.9	화면/음성 탭.....	207
5.1.8.10	근태 탭.....	208
5.1.8.11	위갠드 탭.....	209
5.1.9	BioStation 2 설정 변경하기.....	209
5.1.9.1	동작모드 탭.....	209
5.1.9.2	지문 탭.....	212
5.1.9.3	네트워크 탭.....	213
5.1.9.4	출입그룹 탭.....	214
5.1.9.5	인터폰 탭.....	214
5.1.9.6	입력 탭.....	214
5.1.9.7	인증 거부 리스트 탭.....	215
5.1.9.8	화면/음성 탭.....	216
5.1.9.9	근태 탭.....	217
5.1.9.10	위갠드 탭.....	218
5.1.10	BioStation A2 설정 변경하기.....	218
5.1.10.1	동작모드 탭.....	218
5.1.10.2	지문 탭.....	221
5.1.10.3	카메라 탭.....	222

5.1.10.4	네트워크 탭	222
5.1.10.5	출입그룹 탭	223
5.1.10.6	입력 탭	223
5.1.10.7	인증 거부 리스트 탭	224
5.1.10.8	화면/음성 탭	224
5.1.10.9	근태 탭	225
5.1.10.10	위갠드 탭	226
5.1.11	BioStation L2 설정 변경하기	227
5.1.11.1	동작모드 탭	227
5.1.11.2	지문 탭	229
5.1.11.3	네트워크 탭	230
5.1.11.4	출입그룹 탭	231
5.1.11.5	입력 탭	231
5.1.11.6	인증 거부 리스트 탭	232
5.1.11.7	화면/음성 탭	232
5.1.11.8	근태 탭	233
5.1.11.9	위갠드 탭	234
5.1.12	BioEntry W2 설정 변경하기	235
5.1.12.1	동작모드 탭	235
5.1.12.2	지문 탭	237
5.1.12.3	네트워크 탭	238
5.1.12.4	출입그룹 탭	238
5.1.12.5	입력 탭	239
5.1.12.6	인증 거부 리스트 탭	240
5.1.12.7	화면/음성 탭	240
5.1.12.8	근태 탭	241
5.1.12.9	위갠드 탭	241
5.2	출입문 설정 변경하기	242
5.2.1	추가정보 탭	242
5.2.2	알람 탭	244
5.3	구역 설정 변경하기	245
5.3.1	이중출입 방지 구역 설정하기	245
5.3.1.1	추가정보 탭	245
5.3.1.2	알람 탭	246
5.3.1.3	출입통제그룹 탭	247
5.3.2	인증 제한 구역 설정하기	247
5.3.2.1	추가정보 탭	247
5.3.2.2	알람 탭	248
5.3.2.3	출입통제그룹 탭	248
5.3.3	경보 구역 설정하기	248
5.3.3.1	추가정보 탭	249
5.3.3.2	알람 탭	249
5.3.3.3	출입통제그룹	250

5.3.4	화재 경보 구역 설정하기	250
5.3.4.1	추가정보 탭	250
5.3.4.2	알람 탭	251
5.3.5	출입 구역 설정하기	252
5.3.5.1	추가정보 탭	252
5.3.6	소집 구역 설정하기	252
5.3.6.1	추가정보 탭	253
5.3.6.2	출입통제그룹 탭	253
5.3.7	Interlock 구역 설정하기	254
5.3.7.1	추가정보 탭	254
5.4	사용자 설정 변경하기	254
5.4.1	추가정보 탭	255
5.4.2	지문 탭	256
5.4.3	얼굴 탭	257
5.4.4	카드 탭	257
5.4.5	근태 탭	258
06	기술 지원	259
07	오픈 라이선스 공지	260
	용어집	263

보증과 면책

슈프리마의 보증 정책

슈프리마는 구매자에게, 제품을 배송한 날로부터 1년(보증 기간) 동안 아래에 제시된 범위 내에서 규격서에 명시된 제품의 성능을 보증합니다. 구매자가 보증서에서 보장하고 있는 결함에 대하여 보증 기간 안에 서면으로 슈프리마에게 알린다면, 슈프리마는 구매자가 운임(국외의 경우, 보험료 포함)을 지급하여 보증 기간 안에 반송한 결함 제품을 수리하거나 교체하여 다시 배송할 것을 약속합니다. 이러한 수리나 교체는 제품 보증 약속을 위반하지 않으려는 슈프리마의 작은 노력입니다. 그러나 다음과 같은 제품은 보증 대상에서 제외된다는 것을 알아두셔야 합니다: (1) 강한 외부의 물리적 충격, 과전류, 오용, 남용, 부주의로 인해 문제가 발생한 제품; (2) 공급자가 서면으로 승인하지 않았음에도 부적절하게 수리, 개조, 변형한 제품; (3) 슈프리마가 제공한 설명서의 내용을 위반하여 설치하거나 사용한 제품.

제품의 결함을 발견한 이후로 적어도 30일 이내에 그리고 제품을 배송한 날로부터 1년 이내에 슈프리마가 제공하는 반품 승인서(Return Material Authorization Report)를 이용하여 서면으로 슈프리마에게 알려야 합니다. 반품 승인서에는 결함 제품에 대한 자세한 정보, 모델 번호, 송장 번호, 일련 번호를 포함해야 합니다. 슈프리마가 발행한 반품 승인 번호를 포함하지 않는 제품은 인정되지 않을 것이며, 또한 모든 결함은 재현할 수 있는 것이어야 합니다.

이 제품은 여기에서 명시된 사항을 제외하고는, 제품의 보증, 상업성, 특정 목적에 맞는 이용가능성 등과 관련하여 어떠한 명시적, 묵시적 보증 없이 있는 그대로 제공됩니다.

면책 조항

이 설명서에 있는 정보는 슈프리마 제품과 관련하여 제공하는 것입니다. 슈프리마가 보장하는 판매 합의사항과 조건에 포함된 제품에 한해서만 사용 권리가 인정됩니다. 이 설명서에서 다루고 있는 그 이외의 지적 재산권에 대한 라이선스 권리는 인정되지 않습니다.

슈프리마는 슈프리마 제품의 판매 또는 사용과 관련하여, 특정 목적을 위한 제품의 적합성과 상업성, 그리고 특허, 저작권, 기타 지적 재산권의 침해에 대해서는 어떠한 보증이나 책임을 지지 않습니다.

의료, 인명 구조, 생명 유지와 관련된 상황이나 또는 제품의 오작동으로 인해 사람이 다치거나 목숨을 잃을 수 있는 상황에서는 슈프리마의 제품을 사용해서는 안됩니다. 만약 구매자가 앞에 예로 든 상황에서 제품을 사용하다가 사고가 발생한다면, 설사 제품의 설계나 생산 과정에서 부족한 점이 발견되어 이를 중요한 과실로 주장한다 하더라도 슈프리마의 직원, 자회사, 지사, 제휴사, 배포사는 책임을 지지 않으며, 변호사 선임비를 포함하여 이와 관련한 모든 직간접적인 비용이나 지출에 대해서도 변제하지 않습니다.

슈프리마는 제품의 안정성, 기능, 디자인을 개선하기 위해 적절한 공지 없이 어느 때이건 제품의 규격과 명세서를 변경할 수도 있습니다. 설계자들은 "구현될 예정"이나 "정의되지 않음"으로 표시된 기능이나 설명은 항상 변동될 수 있다는 점을 염두에 두어야 합니다. 슈프리마는 멀지 않은 미래에 이러한 것들을 구현하거나 정의할 것이며, 호환성의 문제를 포함하여 이로 인해 발생할 수 있는 어떠한 문제점에 대해서도 책임을 지지 않습니다.

제품을 주문하기 전에 가장 최신의 규격서를 얻고자 한다면 슈프리마, 슈프리마의 판매 대행사, 지역 배포사에 문의하십시오.

저작권 공지

이 문서의 저작권은 슈프리마가 가집니다. 다른 제품 이름, 상표, 등록된 상표에 대한 권리는 각각 그것을 소유한 개인이나 단체가 가집니다.

01

BioStar 시스템에 관하여

BioStar 는 네트워크 연결과 바이오인식 보안 기술을 기반으로 하는 슈프리마의 차세대 출입 통제 시스템입니다. 다양한 수준의 사용자 인증 서비스를 제공하기 위해서 대부분의 시스템 장치에서는 지문 스캐너와 카드 리더가 통합되어 있습니다. 각각의 출입문에 설치될 슈프리마의 바이오인식 장치는 카드 리더나 지문 인식기의 역할을 할 뿐만 아니라 지능적인 출입문 통제기의 역할을 수행합니다.

BioStar 표준 버전을 사용하려면 USB 동글을 이용하여 사용권을 획득해야 합니다. USB 동글이 없다면, BioStar 는 기능에 제한이 있는 무료 버전으로 동작합니다. USB 동글이 있다면, 아래의 표에서 볼 수 있듯이 BioStar 에서 더욱 확장된 성능과 다양한 기능들을 사용할 수 있습니다.

구분	표준 버전	무료 버전
최대 출입문 개수	512	20
최대 클라이언트 개수	32	2
구역 기능 지원	예	아니오
이메일 통지	예	아니오
서버 인증	예	아니오
근무 일정 편성	일간 순환, 주간 순환	주간 순환
IO 보드	예	아니오
비주얼 맵	예	아니오

1. BioStar 시스템에 관하여

BioStar1.92 은 다음의 장치들을 지원합니다.



BioStation A2: 슈프리마의 최신 지문 인식 기술과 하드웨어 플랫폼을 기반으로 개발한 지문 인식 장치입니다. 초당 15 만명까지 처리할 수 있는 인증 속도, 위조 지문 감지(LFD) 기능, 얼굴 검출, PoE, 근태 관리와 같은 출입 통제와 근태 관리에 관한 모든 기능을 지원합니다.



BioStation 2: 슈프리마의 업그레이드된 바이오인식 기술과 고성능 CPU 를 이용한 초고속 매칭 및 강력한 인증 성능은 물론, 대용량 데이터도 초고속 전송할 수 있습니다. 고급스러운 외관 설계와 IP65 등급의 방수/방진 구조를 갖추고 있어 다양한 환경에 설치가 가능한 제품입니다.



BioStation L2: 출입 통제와 근태 관리 기능을 모두 제공하는 지문 인식 장치입니다. 최대 1,000,000 개의 템플릿을 저장할 수 있으며, 초당 10 만명까지 처리할 수 있는 속도, 위조 지문 감지(LFD) 기능, 근태 관리 기능을 제공합니다.



BioEntry W2: 슈프리마의 최신 하드웨어와 소프트웨어가 공존하는 근태 관리 및 출입 통제 장치입니다. 이 장치는 쿼드 코어 CPU 와 2 GB 메모리를 비롯하여 OP5 센서, 최신 지문 인식 알고리즘이 탑재되었으며, 1 초에 150,000 개의 지문을 매칭할 수 있습니다. 위조 지문 감지 (LFD) 기능과 근태 관리 기능도 탑재되어 뛰어난 성능을 제공합니다. 옥외 설치가 가능한 IK08 등급 파손 방지 구조와 IP67 방수방진 구조를 갖고 있으며, 장치의 가로 크기가 50 mm 로 작기 때문에 다양한 환경에 설치할 수 있습니다. 또한, 이중 주파수 RFID 기술을 활용한 멀티 카드 스캔이 가능하여 시스템 설계에 유연성을 제공합니다.



Secure I/O 2: 초슬림 디자인을 갖춘 1 개 외부 도어 릴레이 제어와 입출력 확장을 위한 분리형 컨트롤러입니다. 슈프리마 IP 출입통제 단말기와 암호화된 통신으로 사용되어 보안성을 강화할 수 있으며, 사용 환경에 맞춰 최적화된 솔루션을 제공합니다.



BioStation (V1.5 또는 그 이상): 숫자 키와 2.5 인치 LCD 모니터를 포함하고 있는 다기능 단말기입니다. 때문에 관리자가 직접 이 단말기를 이용하여 사용자를 등록하거나 관리할 수 있습니다. 무선 랜이나 이더넷을 이용하여 네트워크에 연결할 수 있으며, 쉽게 데이터를 전송할 수 있도록 USB 인터페이스를 지원합니다. 또한 BioStation MiFARE(BSM) 모델은 스마트 카드를 이용한 출입 통제 기능을 지원합니다.



BioStation T2: 네트워크 기반의 다기능 출입 통제 장치입니다. 5 인치 터치스크린, 카메라, 지문 스캐너, 카드 리더를 이용하여 다양한 인증 방식을 지원합니다. 뿐만 아니라 인터폰 기능을 지원하여 상대방과 화상으로 통화할 수 있습니다.

1. BioStar 시스템에 관하여



FaceStation: LCD 터치스크린, 얼굴 인식 및 비디오폰용 카메라를 포함하고 있는 네트워크 기반의 다기능 출입 통제 장치입니다. 다양한 인터페이스를 지원하여 여러 방법으로 컴퓨터나 네트워크에 연결할 수 있습니다. 또한 위젯 및 입출력 포트를 이용하여 다양한 출입 통제 시스템을 구성할 수 있습니다.



BioEntry Plus (버전 1.2 이상): 지문이나 카드를 인식할 수 있는 네트워크 기반의 출입 통제 장치입니다. 커맨드 카드를 이용하여 장치에서 직접 몇 가지 기능을 수행할 수 있으며, BioStar 소프트웨어를 이용하여 장치를 전체적으로 관리할 수도 있습니다. 내부 릴레이를 통하여 출입문 잠금 장치와 연결할 수 있으며, Secure I/O 를 함께 사용하면 높은 수준의 보안을 유지할 수 있으며 확장된 기능을 사용할 수 있습니다.



BioEntry W: BioEntry W 는 IP65 국제방진방수 규격을 준수하며 파손에 강한 외장을 채택한 것을 제외하면 BioEntry Plus 와 기능이 동일합니다. 옥외 설치에 가장 적합하며 견고한 외장을 갖춰 혹독한 환경에서도 견고함을 유지합니다. 다양한 통신 기능을 갖추고 있으며 PoE 기능을 지원합니다.



BioLite Net (버전 1.0 이상): 출입통제와 근태관리기능을 모두 제공하는 네트워크 기반의 옥외형 지문인식기입니다. IP65 등급의 방수, 방진 구조를 채택하여 옥외 설치가 가능하며 TCP/IP 및 RS485 를 통한 네트워크 연결이 가능합니다. BioStar 소프트웨어와 연동하여 분산형 출입보안 시스템을 구성할 수 있는 초소형, 초슬림의 지문인식기입니다.



Xpass (버전 1.0 이상): 네트워크 기반의 출입 통제 장치로 RF 카드와 함께 사용할 수 있습니다. 지문 인식 기능을 제외하고 BioEntry Plus 와 동일한 기능을 제공합니다. 전원 공급 이더넷(PoE: Power over Ethernet) 기능을 갖춰 CAT5 또는 CAT6 을 사용하여 설치하면 이더넷을 통해 전원 공급이 가능할 뿐 아니라 방수 기능을 갖춰 옥외에서 사용할 수 있습니다.



Xpass S2: Xpass 와 동일한 기능을 가진 얇은 형태의 출입 제어 장치로서 FeliCa 및 ISO 15693 카드를 지원합니다. Lift I/O 장치를 RS485 슬레이브로 연결하여 여러 층의 출입을 제어할 수 있습니다.



X-Station: 3.5 인치 LCD 터치스크린을 갖춘 스마트 IP 장치로 사용이 매우 간단하며 사용자 ID 와 출입 카드를 지원합니다. 내장된 카메라로 얼굴 검출을 할 수 있으며 1GB 의 내장 플래쉬 메모리와 256MB 의 RAM 으로 최대 20 만 명의 사용자를 저장할 수 있습니다.

1. BioStar 시스템에 관하여



BioMini/BioMini Plus: 지문 스캐너로서 사용자를 간편하게 등록할 수 있습니다. BioStar 서버에 연결된 컴퓨터의 USB 포트에 연결하여 장치 드라이버만 설치하여 사용할 수 있습니다.



Secure I/O: Secure I/O 를 사용하면 실외에 설치된 장치의 보안 수준을 향상할 수 있으며 시스템의 기능을 확장할 수 있습니다. Secure I/O 를 통해 출입문을 제어함으로써 외부 침입자가 실외에 설치된 인증 장치를 무력화하더라도 실내로의 출입을 막을 수 있습니다. 보안 수준을 높이기 위하여, 출입문과 출입문에 설치된 장치들 간의 통신을 암호화할 수 있습니다. 4 개의 입력 포트와 2 개의 출력 릴레이를 가지고 있어 하나의 장치로 여러 개의 출입 지점을 제어할 수 있습니다.



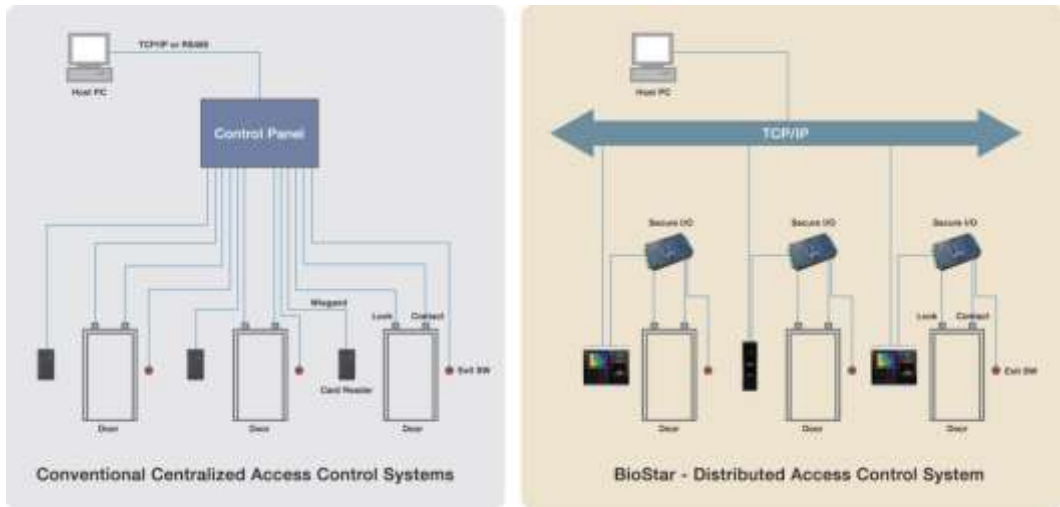
Lift I/O: 0~9의 장치 ID 를 지원하며, 12 개의 출력 포트를 지원합니다. 각 출력은 엘리베이터 버튼에 연결되어 각 층의 출입을 제어할 수 있습니다(12 개의 입력 포트는 현재 지원되지 않습니다.). 최대 10 대까지 RS485 슬레이브로 Xpass 및 Xpass S2 에 연결 가능하며, BioEntry Plus, Xpass, Xpass S2 는 최대 120 개 층을 제어할 수 있습니다.

1.1 논리적 구성

BioStar 는 지능분산형 시스템입니다. 슈프리마의 출입 통제 장치는 전통적인 출입 통제 시스템에서 사용되었던 복잡한 연결선과 중앙집중식 제어 방식을 사용하지 않습니다. 또한 장치들을 TCP/IP 나 무선 랜으로 네트워크에 연결하거나 시리얼 통신을 이용하여 직접 연결할 수 있습니다. 무엇보다 각 개별 장치들이 사용자 정보, 출입 규칙, 기타 데이터를 저장하기 때문에 사용자를 인증하는 데 걸리는 시간이 짧고 네트워크 연결이 끊어지더라도 안정적으로 동작합니다.

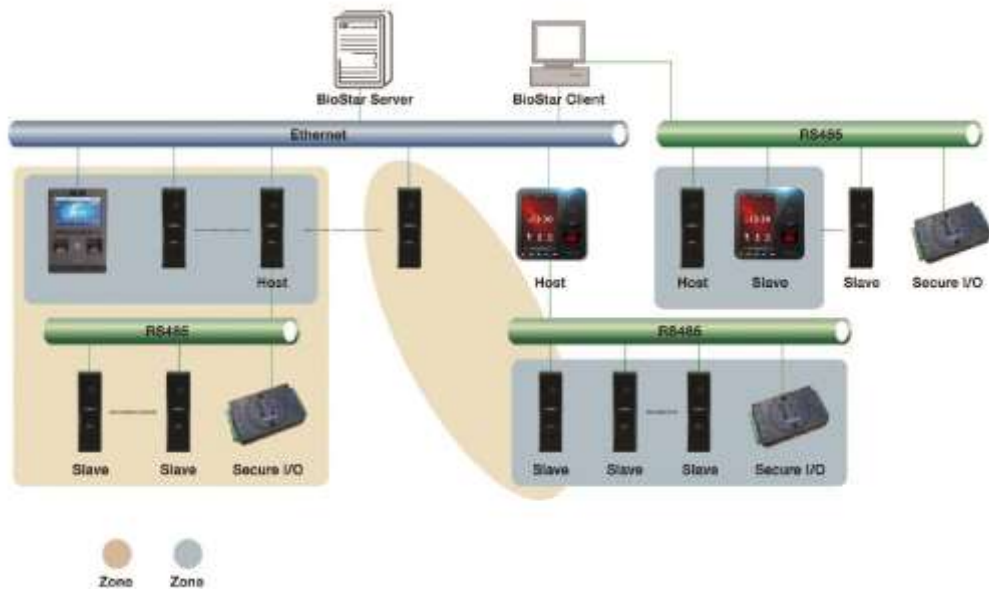
다음의 그림에서 확인할 수 있듯이, BioStar 시스템은 별다른 출입 제어장치(Control Panel)가 필요하지 않습니다. 단말기(BioStation, BioEntry Plus, BioEntry W, BioLite Net)는 제어기와 리더의 역할을 동시에 수행합니다. 이러한 특징은 다른 출입 통제 시스템에 비해서 아주 뚜렷한 이점을 제공합니다. 슈프리마의 지능분산형 접근법은 전통적인 중앙집중식 출입 통제 시스템에 비하여 더 적은 하드웨어와 더 적은 연결선을 사용합니다.

1. BioStar 시스템에 관하여



BioStar 는 서버와 클라이언트 프로그램으로 구성되어 있으며, 한 서버 프로그램에 최대 32 개의 클라이언트 프로그램이 동시에 연결될 수 있습니다. (무료 버전에서는 최대 2 개의 클라이언트 프로그램이 서버 프로그램에 연결될 수 있습니다.) 시스템 구성 방법은 일반적으로 이더넷, 무선 랜, RS485 를 이용하여 하나의 서버에 다수의 출입 통제 장치들을 연결합니다. BioStar 는 MS SQL Server 또는 MySQL 데이터베이스를 사용합니다. BioStar 시스템에서는 최대 512 개의 출입문과 512 개의 장치를 연결할 수 있습니다. (무료 버전에서는 최대 20 개의 출입문과 장치를 연결할 수 있습니다.)

네트워크로 연결된 장치를 여러 개의 그룹으로 묶어서 아래의 그림과 같이 다양한 이중출입방지 구역(anti-passback zone)이나 경보 구역(alarm zone)을 구성할 수 있습니다.



1. BioStar 시스템에 관하여

1.2 출입 통제 기능

BioStar 시스템은 전통적인 출입 통제 시스템에 비해 더 진보하여 바이오인식 기능과 출입 카드 설정 기능을 지원합니다.

1.2.1 사용자 인증

슈프리마의 출입 통제 장치는 지문 인증 컨테스트(FVC2004, FVC2006)에서 2 회 연속 1 위를 수상한 최첨단 지문 인식 알고리즘을 포함하고 있으므로 보다 높은 보안 수준의 출입 통제 기능을 제공합니다. 다음과 같은 다양한 방식으로 사용자를 인증할 수 있습니다.

- **지문 또는 카드:** 지문을 입력하거나 출입 카드를 사용하여 인증합니다.
- **지문 + 카드:** 지문을 입력하고 출입 카드를 사용하여 인증합니다.
- **사용자 ID + 지문:** 사용자 ID 를 입력하고 지문을 입력하여 인증합니다. 사용자 ID 는 사용자를 확인하기 위해 필요하고 지문을 입력하면 출입을 승인 받을 수 있습니다.
- **사용자 ID + 비밀번호:** 사용자 ID 와 비밀번호를 입력하여 인증합니다. 사용자 ID 는 사용자를 확인하기 위해 필요하고 비밀번호를 입력하면 출입을 승인 받을 수 있습니다.
- **사용자 ID + 카드 + 지문:** 사용자 ID, 출입 카드, 지문을 모두 입력하여 인증합니다.
- **지문:** 지문만 입력하여 인증합니다.
- **카드:** 출입 카드만 사용하여 인증합니다.

[FaceStation 전용]

- **얼굴:** 얼굴 정보만으로 인증을 수행합니다.
- **얼굴 + 비밀번호:** 얼굴 정보 및 비밀번호로 인증을 수행합니다.
- **얼굴 + 카드:** 얼굴 정보 및 출입 카드로 인증을 수행합니다.
- **얼굴 + 카드 또는 비밀번호:** 얼굴 정보 입력 후 출입 카드나 비밀번호를 입력하여 인증을 수행합니다.
- **얼굴 + 카드 + 비밀번호:** 얼굴 정보, 출입 카드, 비밀 번호를 모두 입력하여 인증을 수행합니다.
- **사용자 ID + 얼굴:** 사용자 ID 및 얼굴 정보로 인증을 수행합니다.
- **사용자 ID + 얼굴 또는 비밀번호:** 사용자 ID 입력 후 얼굴 정보나 비밀번호를 입력하여 인증을 수행합니다.
- **사용자 ID + 얼굴 + 비밀번호:** 사용자 ID, 얼굴 정보, 비밀번호를 모두 입력하여 인증을 수행합니다.

[BioStation A2, X-Station, BioStation T2, FaceStation]

- **얼굴 검출:** 사용자 인증이 된 경우 얼굴을 캡처해야 합니다.

BioStar는 한 사람마다 2 개의 지문, 그리고 한 지문마다 2 개의 템플릿(총 4 개의 템플릿)을 저장합니다. 그리고 하나의 지문을 험박 지문으로 등록해 두면, 험박에 의하여 출입 허가를 받아야 할 때 험박 지문으로 인증을 하면 경보를 작동시키거나 경고 메일을 발송할 수 있습니다. 각 지문의 두 번째 템플릿은 지문을 잘못 인식할 수 있는 확률(본인 거부율)을 감소시킵니다. 지문 등록에 관한 자세한 내용은 3.6.2 를 참조하십시오.

1. BioStar 시스템에 관하여

BioStar 를 이용하면 EM4100 카드와 HID 카드를 읽을 수 있을 뿐 아니라 MiFARE(MIFARE) 및 iCLASS(iCLASS) 출입 카드를 읽거나, 발급하거나, 포맷을 변경할 수 있습니다. 출입 카드에 관한 자세한 내용은 3.6.4 를 참조하십시오.

BioStation A2, X-Station, BioStation T2 및 FaceStation 은 내장된 카메라로 얼굴 이미지를 검출 및 저장하여 향상된 출입 통제를 가능하게 해줍니다. 얼굴 검출에 관한 자세한 내용은 3.6.3 을 참조하십시오.

1.2.2 사용자 관리

BioStar 를 이용하면 자동 모드나 수동 모드로 사용자를 관리할 수 있습니다. 수동 모드는 사용자 데이터 일부분을 특정 장치에만 등록하거나 또는 BioStar 데이터베이스가 너무 커서 단말기에 저장할 수 없어 일부만 저장할 때 사용할 수 있습니다. 자동 모드는 개별 장치마다 사용자 데이터를 다르게 저장할 필요가 없을 때 사용할 수 있습니다.

BioStar 는 사용자와 관련된 모든 이벤트를 기록하며 이 데이터를 CSV 형식의 파일로 저장할 수 있습니다. BioStar 는 데이터베이스 소프트웨어나 하드웨어 구성이 뒷받침된다면 무한히 많은 사용자 데이터를 기록할 수 있습니다. 사용자 관리에 관한 자세한 내용은 4.5 를 참조하십시오.

1.2.3 출입그룹 관리

BioStar 에서 출입시간과 출입문을 묶어서 출입그룹을 만들 수 있습니다. 이 기능을 이용하면, 출입시간과 사용하는 출입문에 따라 각 사용자의 출입을 통제할 수 있습니다.

BioStar에서는 7개의 일간 일정과 2개의 휴일 일정으로 구성되는 출입시간을 최대 128개까지 만들 수 있습니다. 하나의 출입시간에 포함되어 있는 각각의 하루는 최대 5 개의 시간 구역(time period)으로 나눠서 구성할 수 있습니다.

BioStar 는 최대 128 개의 출입그룹을 지원하며 이 데이터는 연결된 모든 장치에 전달됩니다. 출입그룹에 관한 자세한 내용은 3.8 을 참조하십시오.

1.2.4 장치 관리

관리자는 BioStar 소프트웨어를 이용하여 다양한 장치 설정을 조절할 수 있습니다. 인증 모드뿐만 아니라 입력 릴레이, 출력 릴레이, 동작, 소리 등 다양한 설정을 조절할 수 있습니다. 또한, BioStation A2, BioStation 2, BioStation L2, BioStation, X-Station, BioStation T2 및 FaceStation 의 경우 화면과 음성을, BioEntry Plus 를 비롯한 나머지 단말기의 경우 LED 와 Buzzer 를 조절할 수 있습니다.

BioStar 는 출입문 잠금 장치와 경보 사이렌 등과 같은 슬레이브 장치를 제어할 수 있는 환경설정 옵션을 제공합니다. 또한 위갠드 인터페이스를 이용하여 연결하면 타사의 제품과도 통신할 수 있습니다. 장치 관리에 관한 자세한 내용은 3.2 와 4.7 을 참조하십시오.

1.2.5 출입문 및 리프트 관리

BioStar 는 출입문 릴레이, 경보 릴레이, 출입문 센서, 문열림 스위치와 같은 장치들을 종합적으로 관리할 수 있습니다. 하나의 출입문에 최대 2 개의 출입 통제 장치를 연결하여 출입을 제어할 수 있으며, 2 개의 출입 통제 장치를 연결하여 사용할 때에는 이중 출입방지 기능을 적용할 수 있습니다. BioStar 는 BioEntry Plus, Xpass, Xpass S2 와 슬레이브로 연결된 Lift I/O 장치로 엘리베이터(리프트)를 제어할 수 있습니다.

1. BioStar 시스템에 관하여

BioStar 는 강제로 열리거나 오랫동안 열린 채로 방치된 출입문에 대해 경고하도록 설정할 수 있습니다. 이러한 경고 기능에는 개별 장치에서 경고음을 울리거나, 외부의 경보 사이렌에 신호를 보내거나, BioStar 의 사용자 인터페이스에 경고를 표시하거나, 통지 이메일을 보내는 것이 포함됩니다. 이외에도 관리자(administrator)나 운영자(operator)는 BioStar 를 이용하여 원격으로 출입문을 여닫거나 경보를 초기화할 수 있습니다. 출입문 관리에 관한 자세한 내용은 3.3, 4.3, 4.4 를 참조하십시오. 엘리베이터(리프트) 관리에 관한 자세한 내용은 3.4 를 참조하십시오.

1.2.6 구역 관리

BioStar 를 이용하면 관리자는 다양한 구역을 설정하여 관리할 수 있습니다. (무료 버전은 이 기능을 지원하지 않습니다.) 구역은 이더넷이나 RS485 로 연결된 장치들을 하나의 그룹으로 묶어서 설정합니다. 하나의 구역은 1 개의 호스트 장치(마스터 장치)와 65 개의 슬레이브 장치(슬레이브 장치)로 구성됩니다. 하나의 개별 장치는 최대 4 개의 구역에 동시에 포함될 수 있습니다.

BioStar 는 이중출입 방지 구역(anti-passback zone)이나 인증 제한 구역 등과 같이 좀더 향상된 출입 통제 기능을 제공하기 위하여 구역 설정을 지원합니다. 구역 설정 기능을 이용하여 경보 구역이나 화재 경보 구역을 적용할 수도 있습니다. 뿐만 아니라 하나의 구역 안에 있는 모든 장치들의 시간, 이벤트 기록, 사용자 데이터를 동일하게 유지할 수 있습니다. 구역 관리에 관한 자세한 내용은 3.5 를 참조하십시오.

1.2.7 근태 관리

BioStar(V1.2 또는 그 이상)는 근태관리 기능을 지원합니다. 관리자는 시간대별 요율, 일일 근무 일정, 근무 일정 편성, 휴일 규칙을 설정할 수 있습니다. BioStar 가 제공하는 근태관리 기능을 이용하면 모든 근로자의 출석, 결석, 지각, 조퇴, 외근, 출장을 집계하여 보고서를 생성할 수 있을 뿐만 아니라 이를 토대로 급여를 계산할 수도 있습니다.

관리자는 BioStar 를 이용하여 슈프리마 출입통제 단말기(BioStation A2, BioStation 2, BioStation L2, BioEntry W2, BioStation, X-Station, BioStation T2 및 FaceStation)의 근태 기능을 설정할 수 있으며, 이를 통해 근태 이벤트를 어떻게 기록할 것인가를 결정할 수 있습니다. 표준 버전에서 사용할 수 있는 I/O 보드를 이용하면 근무자의 출결 상태를 실시간으로 쉽게 확인할 수 있습니다. 근태 관리 기능에 관한 자세한 내용은 3.9 과 4.6 을 참조하십시오.

1.2.8 IP 카메라 및 NVR 서버 관리

BioStar(V1.5 또는 그 이상)는 IP(인터넷 프로토콜) 카메라와 NVR(네트워크 비디오 레코더) 서버를 지원하여 관리자가 원하는 지역을 실시간으로 감시할 수 있으며 특정 이벤트가 발생하면 해당 IP 카메라에서 전송되는 정지 영상을 확인할 수 있습니다. BioStar 시스템은 NVR 서버와 연동하여 날짜별로 정렬된 이벤트 로그와 함께 정지 영상이나 동영상을 제공합니다. BioStar 인터페이스를 통해 관리자가 NVR 추가할 수 있으며 IP 카메라를 추가 및 설정할 수 있습니다. IP 카메라와 NVR 서버에 관해서 자세한 정보는 3.11 과 4.1 을 참조하십시오.

1. BioStar 시스템에 관하여

1.3 1.x 장치와 2.x 장치의 기능 차이

슈프리마 장치는 BioStar 1 을 지원하는 장치와 BioStar 2 를 지원하는 장치의 설계 구조 및 동작 방식이 다릅니다. 이 때문에 BioStar 2 를 지원하는 장치를 BioStar 1 과 연결하여 사용할 수 없었습니다. 하지만, BioStar 2 만 지원하는 장치 중 BioStation 2, BioStation A2, BioStation L2, BioEntry W2 는 BioStar 1 과 사용할 수 있도록 추가되었습니다.

아래는 BioStation 2, BioStation A2, BioStation L2, BioEntry W2 를 BioStar 1 과 연결하여 사용할 때 발생하는 제약 사항입니다. 시스템을 구성하기 전에 반드시 확인하십시오.

2.x 장치 호환 정보

- **BioStar 1.91:** BioStation 2, BioStation A2, BioStation L2
- **BioStar 1.92:** BioStation 2, BioStation A2, BioStation L2, BioEntry W2

펌웨어 호환 정보

- BioStation 2: 1.2.1 버전 이상
- BioStation A2: 1.1.0 버전 이상
- BioStation L2: 1.0.1 버전 이상
- BioEntry W2: 1.0.0 버전 이상

사용자

- 사용자 가져오기: 부서 정보, PIN 을 가져올 수 없습니다.
- 카드: BioStar 2 에서 발급할 수 있는 보안 크리덴셜 카드를 발급할 수 없습니다. 또한, 카드를 1 장만 사용할 수 있습니다.
- 지문 스캔 및 카드 읽기: 사용자의 지문을 스캔하거나 카드를 발급할 때 마스터 장치를 사용해야 합니다. 슬레이브로 연결된 2.x 장치는 지문을 스캔하거나 카드를 읽을 수 없습니다.

출입문

- 출입문: 1.x 장치와 2.x 장치를 함께 사용하여 출입문을 구성할 수 없습니다. 즉, 서로 다른 버전의 장치로 입실/퇴실 장치를 설정할 수 없습니다.
- 구역: 1.x 장치와 2.x 장치를 함께 사용하여 구역을 구성할 수 없습니다. 서로 다른 버전의 장치로 구역을 구성할 수 없습니다.

출입통제

- Full Access / No Access: 2.x 장치는 장치에 설정된 Full Access/No Access 보다 사용자의 출입통제 정보를 우선으로 사용합니다. 장치에 설정된 출입통제 정보가 없다면 기본으로 등록된 사용자의 인증 정보만으로 출입이 가능하며, 사용자의 출입을 구체적으로 제어하려면 반드시 출입통제 정보를 설정해야 합니다.

1. BioStar 시스템에 관하여

장치

- 장치 트리: 2.x 장치는 항상 BioStar Server의 하위 목록에 표시됩니다. 1.x 장치는 서버 모드를 사용할 경우 BioStar Server의 하위 목록에 표시되며, 다이렉트 모드를 사용할 경우 장치의 하위 목록에 표시됩니다.
- 네트워크 탭: 설정할 수 있는 RS485 모드가 1.x 장치와 다릅니다. 2.x 장치의 RS485 모드는 기본값, 호스트, 슬레이브를 설정할 수 있으며, 기본값으로 설정한 경우 1개의 장치로 1개의 출입문을 구성할 수 있습니다. 또한, RS485 모드가 기본값으로 설정된 장치를 호스트 장치에 RS485 케이블로 연결하면 BioStar에서 슬레이브 장치로 등록할 수도 있습니다.
- 입력/출력 탭: 2.x 장치는 입력 탭만 사용합니다.
- Wiegand 탭: Wiegand 모드는 확장 모드만 지원합니다.
- MIFARE 카드 CSN: 2.x 장치는 MIFARE 카드 CSN을 읽는 방식이 1.x 장치와 다릅니다. 1.x 장치의 Byte Order가 MSB로 설정되어 있다면 2.x 장치는 LSB로 설정하십시오. 1.x 장치의 Byte Order가 LSB로 설정되어 있다면 2.x 장치는 MSB로 설정하십시오.

모니터링

- 경비 개시/해제: 2.x 장치로 구성된 출입문이나 구역은 경비 개시/해제를 사용할 수 없습니다.
- 로그 업로드: 2.x 장치는 USB를 이용하여 로그를 업로드 할 수 없습니다.

BioStar 설치하기

BioStar 프로그램을 설치하기에 앞서 몇 가지만 준비한다면, BioStar 를 설치하는 과정은 매우 간단합니다. 먼저 다음 사항을 확인하시기 바랍니다.

- 2.1 에 제시되어 있는 시스템 요구사항을 확인하십시오.
- BioStar 서버를 설치할 컴퓨터를 선택하십시오. BioStar 서버를 항상 사용하려면, 24x7 시간 동안 운영 가능한 컴퓨터에 설치해야 합니다. BioStar 서버는 연결된 장치로부터 실시간으로 기록(log) 데이터를 전달받아 저장합니다.
- 사용할 데이터베이스의 종류를 선택하십시오. BioStar 는 Oracle, MySQL 과 MS SQL(MS SQL 의 간소화 버전인 MS SQL Sever Express 포함)을 모두 지원합니다. 어떤 데이터베이스를 선택하든, 데이터베이스에 접속하여 새로운 테이블을 만들 수 있는 권한을 가지고 있어야 합니다.

BioStar 설치 CD 에는 BioStar 설치 프로그램이 포함되어 있습니다. BioStar 설치 프로그램을 이용하면 별다른 설정없이 BioStar 서버와 클라이언트 프로그램을 동시에 설치할 수 있습니다(2.2 참조). 데이터베이스 옵션을 직접 설정해야 하거나, BioStar 서버와 클라이언트 프로그램을 각각 다른 컴퓨터에 설치할 때에는 BioStar 설치 프로그램을 실행한 다음 원하는 프로그램만 선택하여 설치하십시오(2.3 참조).

2.1 시스템 요구사항

BioStar 는 다음의 운영체제를 지원합니다.

- Windows 8 (32 비트 및 64 비트 시스템)
- Windows 7 (32 비트 및 64 비트 시스템)
- Windows Server 2008 R2
- Windows Vista
- Windows XP, Service Pack 1 이상
- Windows Server 2003
- Windows 2000, Service Pack 4 이상

2. BioStar 설치하기

최소 시스템 요구사항은 다음과 같습니다.

- CPU: 1.5GHz 이상의 듀얼 코어 프로세서
- 메모리: 2GB
- 하드디스크: 5GB

권장 시스템 요구 사항은 다음과 같습니다.

- CPU: 2GHz 이상의 쿼드 코어 프로세서
- 메모리: 4GB
- 하드디스크: 10GB

2.2 BioStar 서버와 클라이언트를 한번에 설치하기

BioStar 서버와 클라이언트를 같은 컴퓨터에 설치하고 또한 기본 설정으로 MS SQL Server Express 데이터베이스를 사용하려 한다면, BioStar 설치 프로그램을 실행하십시오.

주의: 이전 버전의 BioStar 클라이언트 또는 BioStar 서버를 컴퓨터에 설치하였다면 BioStar 설치 프로그램을 실행하기 전에 반드시 이전 버전을 삭제하십시오.

주의: BioStar 2 가 설치된 컴퓨터에 BioStar 1 을 설치하지 마십시오. 프로그램 성능에 문제가 발생할 수 있습니다.

BioStar 설치 프로그램은 다음의 구성 요소를 설치합니다.

- BioStar 서버 프로그램
- 보조 프로그램: Open SSL, Microsoft Visual C++ Redistributable
- MS SQL Sever Express
- BioStar 클라이언트 프로그램
- BADB Con(데이터베이스 변환 프로그램)

BioStar 설치 프로그램을 실행하기 전에 다른 모든 응용 프로그램을 종료하십시오. BioAdmin 서버가 설치되어 있는 컴퓨터에 BioStar 를 설치한다면, 설치를 시작하기 전에 BioAdmin 서버를 중지하십시오.

설치 프로그램 실행하기

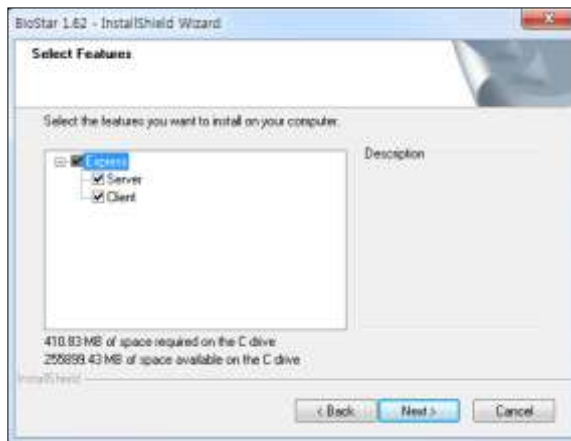
1. CD-ROM 드라이브에 BioStar 설치 CD 를 넣습니다.
2. 설치 폴더를 찾아 BioStar 1.92 Setup 을 실행합니다.
3. 화면의 지시에 따라 설치를 시작합니다.

2. BioStar 설치하기

4. 언어 선택 화면이 나타나면 **Korean** 을 선택하고 **Next** 를 클릭합니다.



5. 구성 요소 선택 창에 **Server** 프로그램과 **Client** 프로그램이 모두 선택되었는지 확인한 후, **Next** 를 클릭합니다.



6. 화면의 지시에 따라 설치를 마칩니다.

MS SQL Sever 가 이미 설치되어 있다면 MS SQL Server Express 를 설치할 것인지 지정합니다. MS SQL Server Express 를 설치하지 않겠다고 선택한다면, 2.3 의 7 단계에 설명되어 있는 대로 기존에 설치된 MS SQL Server 에 접속하기 위한 정보를 입력합니다.

2.3 BioStar 서버 설치하기

BioStar 서버만 설치하려는 경우 BioStar 설치 프로그램을 실행한 다음 설치 화면에서 클라이언트 설치 옵션의 선택 표시를 해제해야 합니다. 설치를 시작하기 전에 이 장의 맨 앞에 설명된 기본적인 준비 사항과 2.1 에 제시되어 있는 시스템 요구사항을 확인하십시오.

BioStar 설치 프로그램은 다음의 구성 요소를 설치합니다.

- BioStar 서버 프로그램
- 보조 프로그램: Open SSL, Microsoft Visual C++ Redistributable
- MS SQL Sever Express
- BioStar 클라이언트 프로그램
- BADB Conv(데이터베이스 변환 프로그램)

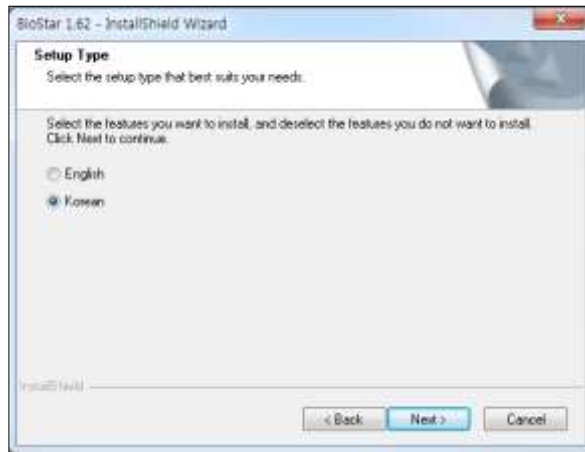
2. BioStar 설치하기

BioStar 설치 프로그램을 실행하기 전에 다른 모든 응용 프로그램을 종료하십시오. BioAdmin 서버가 설치된 컴퓨터에서 BioStar를 설치한다면, 설치를 실행하기 전에 BioAdmin 서버를 중지하십시오.

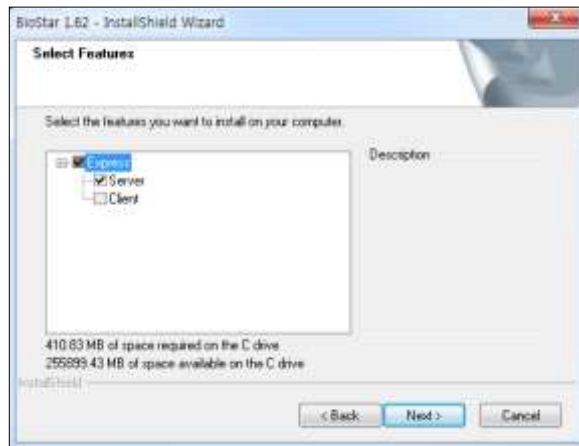
주의: 이전 버전의 BioStar 클라이언트 또는 BioStar 서버를 컴퓨터에 설치하였다면 BioStarInstaller를 실행하기 전에 반드시 이전 버전을 삭제하십시오.

BioStar 서버 설치하기

1. CD 롬 드라이브에 BioStar 설치 CD를 넣습니다.
2. 설치 폴더를 찾아 BioStar 1.92 Setup을 실행합니다.
3. 화면의 지시에 따라 설치를 시작합니다.
4. 언어 선택 화면이 나타나면 **Korean**을 선택하고 **Next**를 클릭합니다.



5. 구성 요소 선택 창에서 Client 프로그램의 선택 표시를 해제한 다음 **Next**를 클릭하여 설치를 진행합니다(기본값으로 Server와 Client가 모두 선택되어 있습니다).

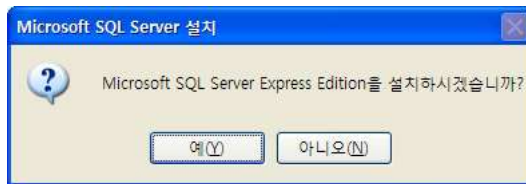


2. BioStar 설치하기

6. OpenSSL 이 설치되어 있지 않다면, OpenSSL 설치 마법사가 시작됩니다.



- 설치를 진행하려면 **Next** 를 클릭합니다.
 - 사용권 동의서를 읽은 다음, 동의한다면 **I accept the agreement.**를 선택한 후 **Next** 를 클릭합니다.
 - 설치할 폴더를 확인한 후 **Next** 를 클릭합니다. 설치할 폴더를 변경하려면 **Browse...**를 클릭한 후 폴더를 선택합니다.
 - 설치를 시작하려면 **Install** 을 클릭합니다.
 - Finish** 를 클릭합니다.
7. 설치 마법사가 MS SQL Server Express 를 설치할 것인지 묻습니다.



- 이미 설치되어 있는 MS SQL Server 나 MySQL, ORACLE 을 사용하려 한다면 **아니오**를 클릭합니다.
 - MS SQL Server Express 를 설치하려면 **예**를 클릭하고, 10 단계로 이동하십시오. 설치 마법사가 데이터베이스를 자동으로 설정합니다.
8. 데이터베이스 생성 [BioStar] 대화 상자가 나타납니다.



- 데이터베이스 영역에서, 사용하고 있는 데이터베이스(MS SQL Server/ MySQL / ORACLE)를 선택합니다.
- 계정 영역에서, 데이터베이스에 접속하기 위한 방법을 선택합니다.

2. BioStar 설치하기

- MySQL 을 사용하고 있다면 **서버 계정 사용**을 선택한 후, 데이터베이스에서 만든 ID 와 비밀번호를 입력합니다.
- MS SQL Server 를 사용하고 있다면 **서버 계정 사용**이나 **윈도우즈 계정 사용**을 선택합니다. 서버 계정 사용을 선택하면 데이터베이스에서 만든 ID 와 비밀번호를 입력해야 합니다. 윈도우즈 사용자 계정을 선택하면 ID 와 비밀번호를 입력하지 않아도 됩니다.

참고: 데이터베이스에서 새로운 테이블을 만들 수 있는 권한을 가진 ID 를 입력해야 합니다. 동일한 시스템에 여러 개의 데이터베이스를 설치하는 것을 방지하기 위하여 데이터베이스의 기본 이름은 항상 “BioStar”입니다. 하지만 DBSetup.exe 를 실행하여 데이터베이스의 이름을 변경할 수 있습니다. 데이터베이스 서버를 패치할 때 데이터베이스를 수동으로 선택할 수 있는 옵션이 있습니다.

c. **실행**을 클릭하여 BioStar 가 사용할 데이터베이스를 만듭니다.

d. 데이터베이스 설정이 완료되면, **종료**를 클릭합니다.

9. 설치 프로그램이 나머지 작업을 마무리하면 설치가 완료됩니다. **Finish** 를 클릭합니다.

주의: BioStar 1.3 이상은 Windows 7 에서 BioStation 을 연결할 수 있는 USB 드라이버를 포함하고 있습니다. 이 드라이버는 이전 버전의 BioStar 와 호환되지 않습니다. 이전 버전의 BioStar 를 사용하고 있다면 올바른 USB 드라이버를 설치하십시오.

2.3.1 MySQL 서버 설정하기

MySQL 데이터베이스를 사용하는 경우, MySQL 서버의 최대 허용 패킷이 16MB 이하로 설정되어 있다면 BioStar 시스템은 MySQL 데이터베이스를 활용할 수 없습니다. MySQL 서버의 최대 허용 패킷을 16MB 이상으로 설정해야 합니다.

MySQL 서버의 최대 허용 패킷을 설정하려면 MySQL 서버의 설정 파일(Windows 계열 OS 에서는 my.ini 파일, 리눅스 계열 OS 에서는 my.cnf 파일)을 편집해야 합니다. 설정 파일에 최대 허용 패킷 값이 설정되어 있지 않다면, [mysqld] 항목 아래에 max_allowed_packet=16M 을 추가합니다. 설정 파일에 최대 허용 패킷 값이 있으나 이 값이 16MB 보다 작은 경우에는 이 값을 16M 이상의 값(예를 들어, max_allowed_packet=16M)으로 변경합니다. 설정 파일을 변경하고 저장한 후 MySQL 서비스를 다시 시작하여 변경 사항을 적용합니다.

2.3.2 BioStar 서버 설정하기

BioStar 서버를 직접 설정해야 할 때도 있습니다. 예를 들어, BioStar 클라이언트 프로그램에서 BioStar 서버에 접속하는 데 문제가 있다면, 서버 설정을 수정해야 합니다. 서버 설정을 수정하거나 데이터베이스 설정을 수정하기 위해서는 BioStar 서버 프로그램을 멈춘 후 다시 시작합니다.

BioStar 서버 설정 프로그램을 시작하려면, 바탕화면에서 **BioStar Server Config** 를 클릭합니다. 또는 Windows 에서 **시작 > 모든 프로그램 > BioStar 1.92 > Server Service > BioStar Server Config** 를 클릭합니다.

서버 설정 프로그램을 이용하면 다음과 같은 사항을 감시하고 제어할 수 있습니다.

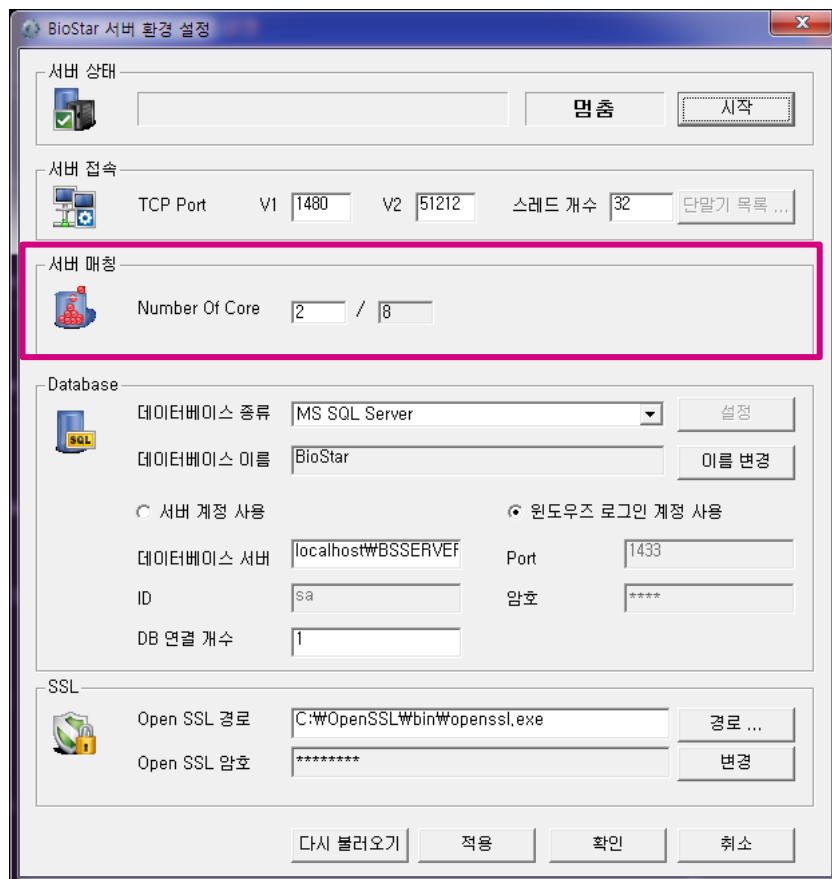
- **서버 상태:** BioStar 서버의 현재 상태(멈춤 또는 실행 중)를 확인하고 수정할 수 있습니다. **시작** 또는 **멈춤**을 클릭하여 서버를 시작하거나 멈출 수 있습니다.
- **서버 접속:** 서버와 장치들의 연결 상태를 확인하고 수정할 수 있습니다.

2. BioStar 설치하기

- **TCP Port:** 장치와 클라이언트 프로그램이 서버에 접속하기 위해서 사용할 포트 번호를 입력합니다. 다른 프로그램이 사용하지 않는 포트 번호를 입력해야 합니다. BioStar 1 을 지원하는 대부분의 장치는 **1480** 포트를 기본값으로 사용하며, BioStation A2, BioStation 2, BioStation L2, BioEntry W2 는 **51212** 포트를 기본값으로 사용합니다.
- **스레드 개수:** BioStar 서버가 만들 수 있는 최대 스레드 개수를 입력합니다. 32~512 사이의 값을 입력할 수 있습니다. 시스템 구성 환경에 따라 최적값은 달라질 수 있으나 기본값(32)을 사용하기를 권장합니다.
- **단말기 목록:** 이 버튼을 클릭하면 BioStar 서버에 연결된 장치의 목록을 볼 수 있습니다. 목록에서 장치의 IP 주소와 장치에 SSL 인증서가 발급되었는지 확인할 수 있습니다. 이 프로그램을 이용하여 직접 SSL 인증서를 발급하거나 삭제할 수 있습니다.
- **서버 매칭:** 서버 매칭 시, 사용하는 Matcher 의 기능이 개선되어 시스템의 CPU 코어 개수에 따라 성능이 향상되도록 지원됩니다. 따라서, Matcher 에서 사용하는 코어의 수가 많을수록 더 빠른 서버 매칭 속도를 기대할 수 있습니다.

BioStar Server Config 의 Server Matching 항목에서 아래와 같이 설정을 지원합니다.

- **Number of Core** 는 Matcher 가 사용할 Core 개수를 나타내며, 기본값은 2 입니다.



- **데이터베이스:** 데이터베이스의 종류를 확인하고 수정할 수 있습니다. 이 설정을 변경하는 방법에 대해 자세한 정보는 2.3 를 참조하십시오.
 - **DB 연결개수:** BioStar 서버와 데이터베이스 사이의 최대 연결 개수를 입력합니다. 대부분의 경우 기본값(1)을 사용하기를 권장합니다.

2. BioStar 설치하기

- SSL: OpenSSL 설정을 확인하고 수정할 수 있습니다. 경로를 클릭하여 OpenSSL 프로그램의 경로를 변경하거나 변경을 클릭하여 암호문(pass phrase)을 변경할 수 있습니다.

2.4 BioStar 클라이언트 설치하기

BioStar 설치 프로그램을 실행하기 전에 다른 모든 응용 프로그램을 종료하십시오.

주의: 이전 버전의 BioStar 클라이언트 또는 BioStar 서버를 컴퓨터에 설치하였다면 BioStar 설치 프로그램을 실행하기 전에 반드시 이전 버전을 삭제하십시오.

BioStar 클라이언트만 설치하려는 경우, 설치 프로그램을 실행한 다음 설치 화면에서 BioStar 서버 설치 옵션의 BioStar 1.3 이상은 Windows 7 에서 BioStation 을 선택 표시를 해제해야 합니다. 설치를 시작하기 전에 이 장의 맨 앞에 설명된 기본적인 준비 사항과 2.1 에 제시되어 있는 시스템 요구사항을 확인하십시오.

BioStar 설치 프로그램은 다음의 구성 요소를 설치합니다.

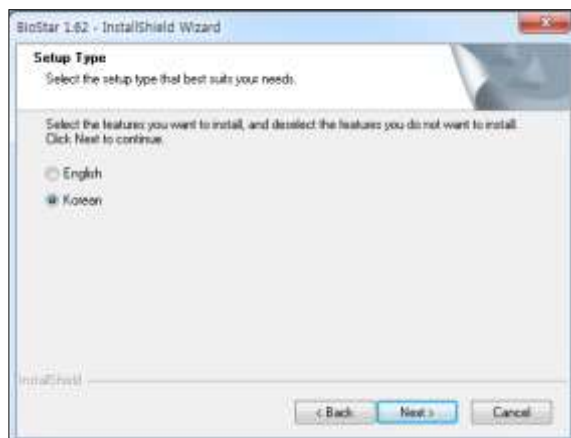
- BioStar 서버 프로그램
- 보조 프로그램: Open SSL, Microsoft Visual C++ Redistributable
- MS SQL Sever Express
- BioStar 클라이언트 프로그램
- BADB Conv(데이터베이스 변환 프로그램)

BioStar 설치 프로그램을 실행하기 전에 다른 모든 응용 프로그램을 닫으십시오. BioAdmin 서버가 설치되어 있는 컴퓨터에서 BioStar 를 설치한다면, 설치를 실행하기 전에 BioAdmin 서버를 중지하십시오.

주의: 이전 버전의 BioStar 클라이언트 또는 BioStar 서버를 컴퓨터에 설치하였다면 BioStar 설치 프로그램을 실행하기 전에 반드시 이전 버전을 삭제하십시오.

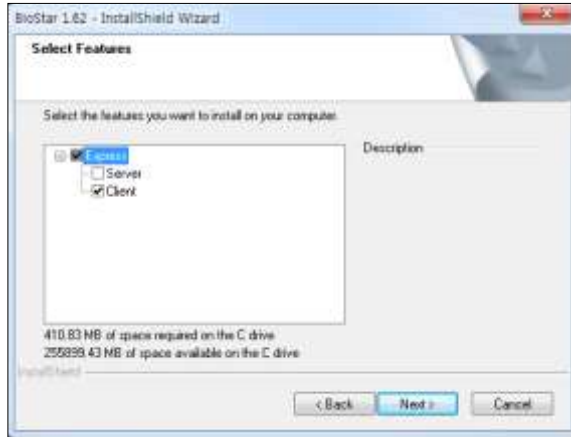
BioStar 클라이언트 설치하기

1. CD 롬 드라이브에 BioStar 설치 CD 를 넣습니다.
2. 설치 폴더를 찾아 BioStar 1.92 Setup 을 실행합니다.
3. 화면의 지시에 따라 설치를 시작합니다.
4. 언어 선택 화면이 나타나면 **Korean** 을 선택하고 **Next** 를 클릭합니다.



2. BioStar 설치하기

- 구성 요소 선택 창에서 **Server**를 선택 해제한 후 **Next**를 클릭하여 설치를 진행합니다(기본값으로 Server와 Client가 모두 선택되어 있습니다.).



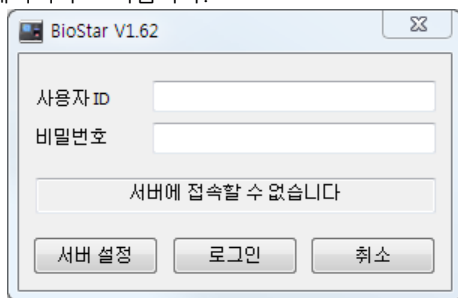
주의: BioStar 1.3 이상은 Windows 7에서 BioStation을 연결할 수 있는 USB 드라이버를 포함하고 있습니다. 이 드라이버는 이전 버전의 BioStar와 호환되지 않습니다. 이전 버전의 BioStar를 사용하고 있다면 올바른 USB 드라이버를 설치하십시오.

2.4.1 처음으로 BioStar에 접속하기

설치를 마치고 컴퓨터를 다시 시작하면, 운영체제의 시작과 동시에 BioStar 서버가 자동으로 실행됩니다. 그러나 컴퓨터를 다시 시작하지 않았다면, 먼저 BioStar 서버를 직접 실행해야 합니다(2.3.2 참조). BioStar 클라이언트 프로그램에 접속하기 위해서는 먼저 관리자 계정을 만들어야 합니다.

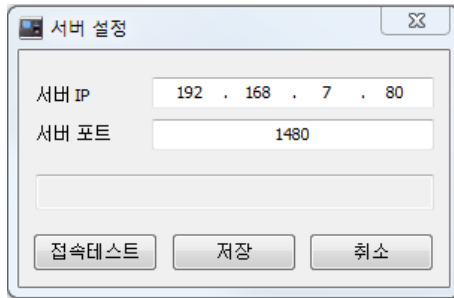
BioStar 클라이언트 최초 접속하기

- BioStar 프로그램을 실행합니다. BioStar 클라이언트가 BioStar 서버에 성공적으로 연결되었다면, 새 관리자 추가 대화 상자가 나타납니다. 이 대화 상자가 나타난다면 6 단계로 건너뛰십시오. BioStar 클라이언트가 서버에 연결되지 못했다면, 대화 상자에 "서버에 접속할 수 없습니다"라는 메시지가 표시됩니다.

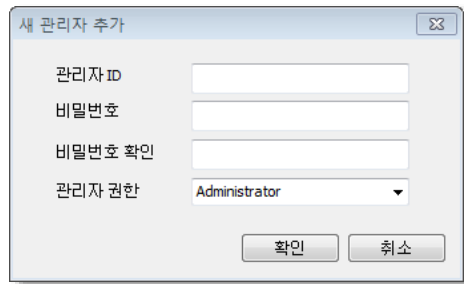


2. BioStar 설치하기

2. 서버 설정을 클릭합니다. 서버 설정 대화 상자가 나타납니다.



3. 서버 설정 대화 상자에서 BioStar 서버의 IP 주소와 포트 번호를 입력합니다.
4. 연결을 확인하기 위해서 **접속테스트**를 클릭합니다.
5. **저장**을 클릭하여 설정을 저장합니다. **새 관리자 추가** 대화 상자가 나타납니다.

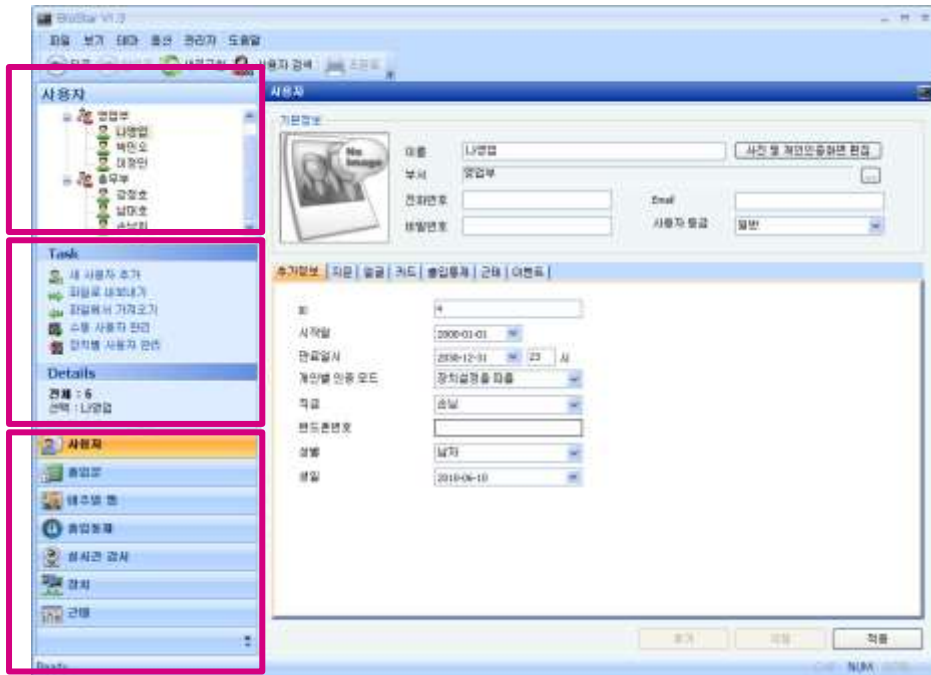


6. 관리자 ID 와 비밀번호를 입력하고, 비밀번호를 한번 더 입력한 뒤, 관리자 권한 목록 상자에서 관리자 등급을 선택합니다.
7. **확인**을 클릭합니다. 로그인 대화 상자로 되돌아갑니다.
8. ID 와 비밀번호를 입력한 후 **로그인**을 클릭합니다.

2. BioStar 설치하기

2.5 BioStar의 화면 구성

BioStar는 여러 인터페이스 요소로 구성되어 있습니다. 각 요소에 대해서는 표준 명칭을 사용하고 있으므로 설명서를 읽기에 앞서 각 요소의 이름을 확인하십시오.



이 설명서에서 메인 창, 대화 상자, 탭, 영역은 그것의 제목 표시줄에 표시된 이름을 사용하여 부릅니다. 예를 들어 사용자 창, Customize 대화 상자, 추가정보 탭, 기본정보 영역 등으로 부릅니다.

2.6 BioStar 인터페이스 변경하기

기본 설정만 이용해도 조작하는 데 문제가 없으므로 특별히 인터페이스 설정을 바꿀 필요는 없습니다. 그러나 BioStar는 개인의 취향에 맞게 인터페이스의 모습을 바꿀 수 있는 기능을 제공합니다.

2.6.1 테마 변경하기

BioStar는 마이크로소프트 오피스 스타일을 기반으로 하는 2개의 테마를 기본으로 제공합니다.

- Office 2003
- Office 2007

테마를 변경하려면, 메뉴 표시줄에서 **테마**를 클릭한 후 원하는 테마를 선택합니다.

2.6.2 도구 표시줄 변경하기

BioStar 인터페이스의 왼쪽 상단에는 표준 도구 표시줄이 있습니다. 이 도구 표시줄에 있는 버튼은 웹 브라우저에 있는 버튼과 비슷하며 앞으로, 뒤로, 새로 고침, 사용자 검색, 인쇄 버튼으로 구성되어 있습니다.

2. BioStar 설치하기

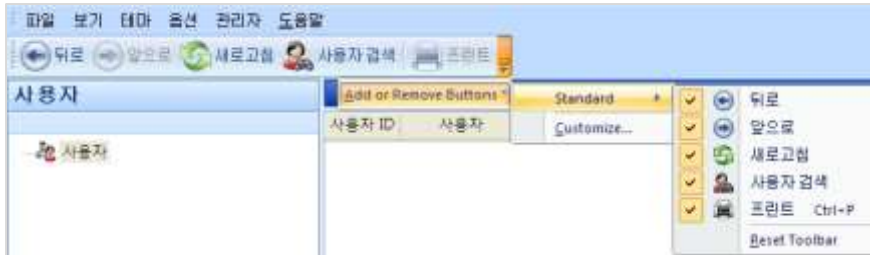
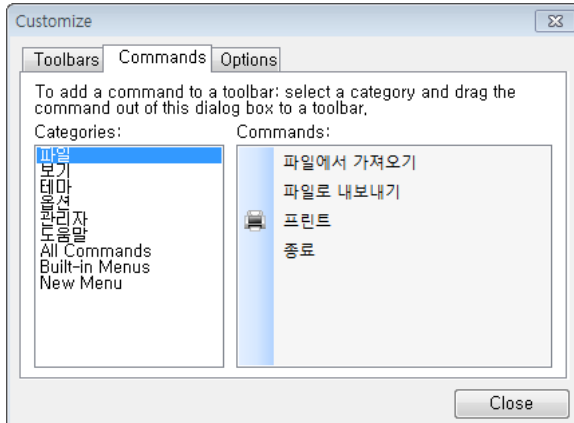


그림 2.1

도구 표시줄 변경하기

1. 도구 표시줄의 오른쪽에 있는 아래 화살표를 클릭합니다.
2. **Add or Remove Buttons > Customize** 를 클릭합니다. **Customize** 대화 상자가 나타납니다.
3. **Commands** 탭을 클릭합니다.
4. **Categories** 목록에 있는 **All Commands** 를 클릭하면 사용할 수 있는 버튼이 표시됩니다.



5. **Commands** 목록에 있는 명령어를 클릭한 채로 도구 표시줄로 가져다 놓습니다. 도구 표시줄에 새로운 버튼이 추가됩니다.

2.6.3 이벤트 보기 변경하기

사용자 또는 출입문이나 구역별로 이벤트 탭에 이벤트가 표시되는 기간을 바꿀 수 있습니다. 기본값으로 1 일, 3 일, 7 일 중에서 선택할 수 있으며, 선택한 기간 동안 자세한 이벤트 내용이 사용자 인터페이스에 표시됩니다.

이벤트 보기 변경하기

1. 메뉴 표시줄에서 **보기 > 이벤트**를 클릭합니다.
2. 이벤트 보기를 바꿀 대상(**사용자** 또는 **출입문/구역**)을 클릭합니다.
3. 기본값으로 사용할 이벤트 표시 기간(**1 일, 3 일, 7 일**)을 클릭합니다.

2.6.4 서체 변경하기

BioStar 는 다양한 언어를 지원하기 위해 시스템에 설치된 서체를 사용할 수 있습니다.

서체를 변경한 뒤 반드시 BioStar 를 재시작하십시오.

2. BioStar 설치하기

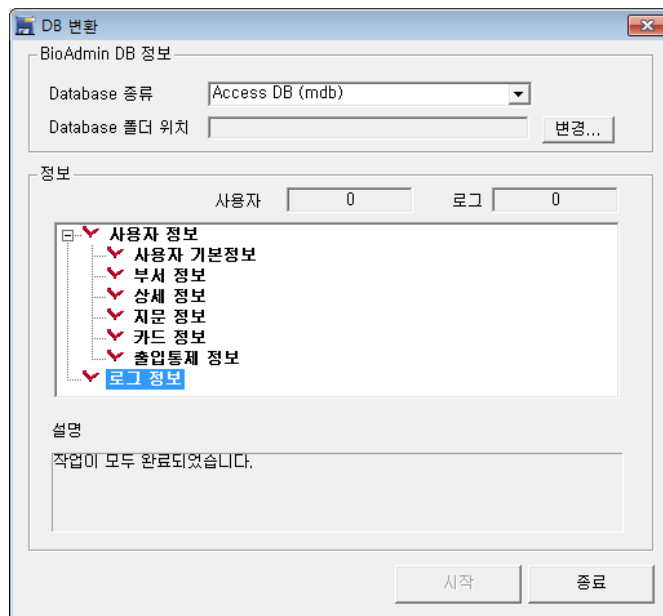
2.7 BioAdmin 에서 BioStar 로 데이터베이스 옮기기

BioStar 설치 프로그램은 **BADBConv** 라는 데이터베이스 변환 도구를 포함하고 있습니다. 이 도구를 이용하면 기존의 BioAdmin 데이터베이스를 BioStar 데이터베이스로 변환해서 사용할 수 있습니다.

데이터베이스를 변환할 때, BioStar 데이터베이스에 동일한 정보가 있으면 BioAdmin 데이터베이스의 정보로 교체됩니다. 예를 들어, BioAdmin 에서 등록했던 사용자를 BioStar 에 다시 등록했다면, 이 사용자 정보가 데이터베이스를 전환하는 과정에서 BioAdmin 에 등록됐던 정보로 교체됩니다. 따라서 데이터베이스를 변환한 다음에 새로운 사용자를 등록하는 것이 좋습니다.

BioAdmin 에서 BioStar 로 데이터베이스 정보를 옮기기

1. 변환 프로그램인 **BADBConv.exe** 를 실행합니다. Windows 에서 **시작 > 모든 프로그램 > BioStar 1.92 > Server Service > BADBConv** 를 클릭합니다.
2. 동일한 사용자가 있으면 BioAdmin 에 등록된 사용자로 덮어쓴다는 경고 대화 상자를 확인한 후 계속 진행하려면 **예** 를 클릭합니다.
3. 기본적으로 BioAdmin 이 설치되어 있으면 Database 종류와 위치 정보를 보여줍니다. 또한 Access DB 일 경우는 파일만 있으면 BioAdmin 이 설치되어 있지 않은 PC 에서 변환할 수 있으며, 이 경우 Database 폴더 위치 변경을 누르고 Access DB(mdb)파일이 있는 폴더를 선택하면 됩니다. BioAdminData.mdb 파일은 반드시 있어야 하며, BioAdminUserImage.mdb 파일과 Log 폴더는 사용자 이미지 정보와 로그정보를 갱신할 경우 포함되어 있어야 합니다.
4. 데이터베이스 변환을 시작하려면 **시작** 을 클릭합니다. 작업이 완료되면 BADBConv 대화 상자에서 **예** 를 클릭합니다.



5. **종료** 를 클릭하여 변환 프로그램을 닫습니다.

BioStar 설정하기

이 장에서는 관리자 계정, 장치, 출입문, 구역, 부서, 사용자, 출입그룹을 BioStar 에 추가하는 방법에 관해서 설명합니다. 이 관리자 설명서는 장치를 설치하는 방법, 출입문과 장치를 연결하는 방법, 장치를 네트워크에 연결하는 방법에 대해서는 설명하지 않습니다. 장치를 설치하거나 출입 통제 시스템을 구성하는 방법에 관한 정보는 출입 통제 장치에 동봉된 설명서를 참조하십시오.

3.1 관리자 계정 만들기

사용자를 추가하려면, 먼저 시스템을 관리할 관리자나 운영자 계정을 만들어야 합니다. 계정의 등급에 따라 시스템을 사용할 수 있는 권한이 달라지므로 계정의 권한에 대해서도 숙지하시기 바랍니다.

3.1.1 관리자 권한

BioStar 는 여러 관리자가 시스템을 관리, 운영, 또는 감독할 수 있도록 여러 종류의 관리자 권한을 지원합니다. 각 관리자 권한은 시스템 메뉴(사용자, 출입문, 비주얼 맵, 출입통제, 모니터링, 장치, 근태)에 대한 접근 권한이 다양합니다. BioStar 시스템은 아래와 같이 미리 설정된 3개의 관리자 권한을 포함하고 있으며 임의의 관리자 권한을 생성할 수 있도록 지원합니다.

- 관리자
- 운영자
- 감독자
- 임의의 관리자 권한

관리자(administrator)는 장치, 사용자, 출입문, 구역, 출입그룹을 추가하거나 설정을 변경할 수 있습니다. 또한 관리자는 근태 관리와 관련된 시간대 효율, 일일 일정, 근무 일정 편성, 휴일 규칙, 휴가 일정을 설정할 수 있으며 근태 결과 보고서를 생성, 수정, 확인할 수 있습니다. 뿐만 아니라 관리자는 새로운 관리자 권한을 추가하여 메뉴에 대한 접근 권한을 설정할 수 있습니다.

운영자(operator)는 네트워크에 연결된 다른 컴퓨터에서 BioStar 시스템에 접속하여 BioStar 시스템을 감시하고 관리할 수 있습니다. 운영자는 관리자 계정(관리자, 운영자, 감독자, 임의의 관리자 권한)을 만들거나 삭제할 수 있는 권한을 제외하고, 관리자와 동일한 권한을 가집니다. 즉, 관리자와 마찬가지로 장치, 사용자, 출입문, 구역, 출입그룹을 추가하거나 설정을 변경할 수 있습니다. 또한, 근태 관리와

3. BioStar 설정하기

관련된 시간대 요율, 일일 일정, 근무 일정 편성, 휴일 규칙, 휴가 일정을 설정할 수 있으며 근태 결과 보고서를 생성, 수정, 확인할 수 있습니다.

감독자(manager)는 모든 메뉴에서 정보를 열람할 수 있는 접근 권한만 가집니다. 메뉴에서 어떤 것도 생성, 수정, 삭제할 수 없습니다. 조직의 필요에 따라 모든 정보를 열람할 수만 있는 접근 권한도 관리 목적으로 유용하게 사용할 수 있습니다.

임의의 관리자 권한은 7 개의 각 메뉴에 대해 완전한 또는 제한적인 접근 권한을 가집니다. 각 메뉴에 대해 3 개의 접근 권한(모든 권한, 수정, 읽기) 중 하나를 부여할 수 있습니다. 조직의 필요에 따라 임의의 관리자 권한을 추가하여 BioStar 시스템을 좀더 효율적으로 관리할 수 있습니다.

일반적으로 시스템의 모든 기능을 통제할 수 있는 관리자(administrator)는 1 명으로 충분하며, 조직의 규모가 큰 경우에는 더 많은 관리자가 필요할 수도 있습니다. 관리자 아래에 몇 명의 운영자(operator)를 두면, 이들이 원격으로 출입문을 열고 닫거나, 사용자를 추가하거나, 지문을 등록하거나, 출입 카드를 발급하거나, 출입 그룹을 등록하거나, 출입 시간을 설정하거나, 경보 이벤트를 설정하는 등 관리자와 함께 다양한 역할을 수행할 수 있습니다.

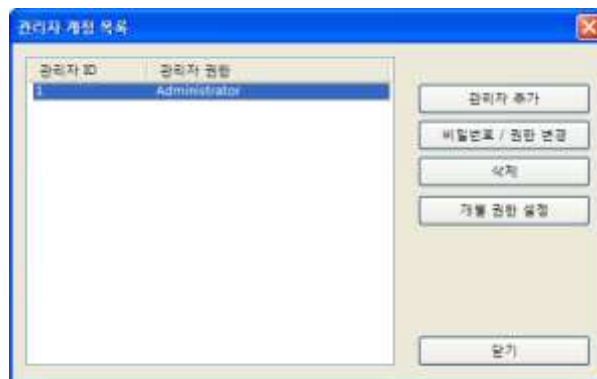
3.1.2 관리자 계정을 추가하고 설정하기

BioStar 소프트웨어를 설치하면 기본적으로 하나의 관리자 계정이 생성됩니다(소프트웨어 설치에 관해서는 2.3 참조). 이 관리자 계정 하나만 사용하면서 시스템을 관리할 다른 사용자에게 운영자 권한을 부여할 수도 있고, 또는 여러 개의 관리자 계정을 둘 수도 있습니다.

3.1.2.1 관리자 계정 추가하기

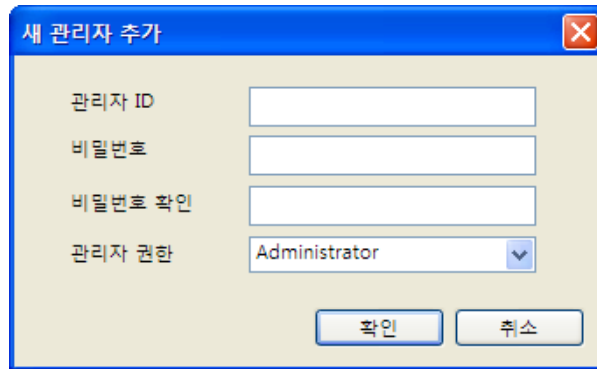
관리자 계정 추가하기

1. 메뉴 표시줄에서 관리자 > 관리자계정을 클릭합니다. 관리자 계정 목록 대화 상자가 나타납니다.



2. 관리자 추가를 클릭합니다. 새 관리자 추가 대화 상자가 나타납니다.

3. BioStar 설정하기



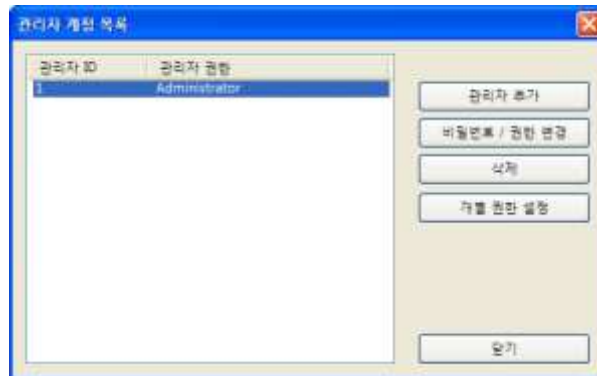
3. 관리자 ID와 비밀번호, 비밀번호 확인을 입력합니다.
4. 관리자 권한 목록 상자에서 원하는 권한을 선택합니다.
 - **Administrator**: 모든 권한
 - **Operator**: 관리자와 운영자 계정을 만들고 삭제할 수 있는 권한을 제외한 모든 권한
 - **Manager**: 모든 정보를 읽을 수 있는 권한
5. 확인을 클릭합니다.

3.1.2.2 관리자 계정의 권한이나 비밀번호 변경하기

실수로 관리자 권한을 잘못 선택하여 이를 수정해야 하거나 또는 비밀번호를 바꾸거나 초기화해야 할 때가 있습니다. 이런 경우에는 관리자 메뉴를 이용하여 해결할 수 있습니다.

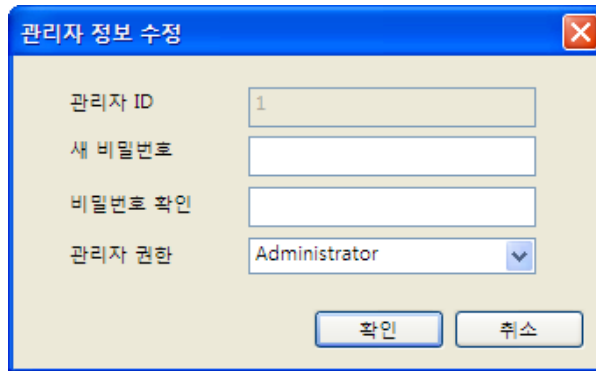
관리자 권한 또는 비밀번호 변경하기

1. 메뉴 표시줄에서 관리자 > 관리자계정을 클릭합니다. 관리자 계정 목록 대화 상자가 나타납니다.
2. 대화 상자의 왼쪽에 있는 목록에서 관리자 계정을 클릭합니다.



3. 비밀번호 / 권한 변경을 클릭합니다. 관리자 정보 수정대화 상자가 나타납니다.

3. BioStar 설정하기



The image shows a dialog box titled "관리자 정보 수정" (Administrator Information Modification). It contains four input fields: "관리자 ID" (Administrator ID) with the value "1", "새 비밀번호" (New Password), "비밀번호 확인" (Confirm Password), and "관리자 권한" (Administrator Privilege) set to "Administrator". There are "확인" (Confirm) and "취소" (Cancel) buttons at the bottom.

4. 필요한 사항을 수정합니다.
5. **확인**을 클릭하여 수정 사항을 저장합니다.

3.1.2.3 임의의 관리자 권한 추가하기

각 메뉴에 대해 개별적으로 접근 권한을 부여할 필요가 있다면 임의의 관리자 권한을 추가하여 이러한 필요를 충족할 수 있습니다. 새로운 임의의 관리자 권한을 이용하여 7 개의 각 메뉴(사용자, 출입문, 비주얼 맵, 출입통제, 모니터링, 장치, 근태)에 대해 전체 또는 제한적인 접근 권한(모든 권한, 수정, 읽기)을 부여할 수 있습니다.

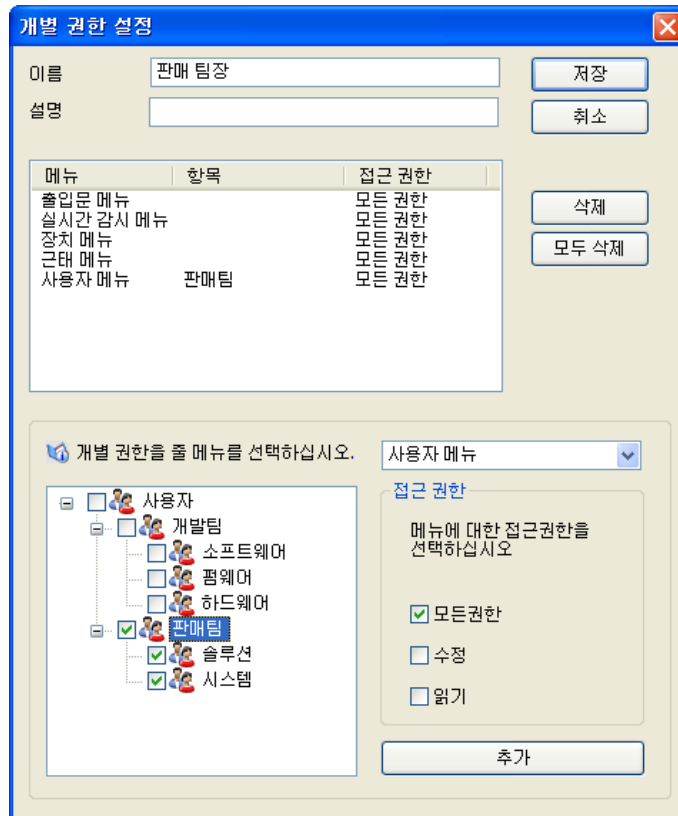
임의의 관리자 권한은 개별 사용자와 장치에 대한 접근 권한을 설정할 수 있습니다. 임의의 관리자 권한은 선택된 사용자와 장치에 대해서만 접근 권한(모든 권한, 수정, 읽기)을 가지며, 선택되지 않은 사용자와 장치는 보거나 수정할 수 없습니다. 임의의 관리자 권한을 추가하는 단계에서, 사용자 메뉴에서 접근 권한을 부여할 사용자를 선택할 수 있습니다. 다만, 개별 사용자를 직접 선택할 수는 없으며 사용자가 속해 있는 최상위 부서와 차상위 부서만 선택할 수 있습니다. 그리고 장치 메뉴에서 접근 권한을 부여할 장치를 선택할 수 있습니다. 슬레이브 장치는 선택할 수 없으며, 슬레이브 장치에 대한 접근 권한은 호스트 장치의 설정에 따릅니다.

사용자 메뉴와 장치 메뉴에서 선택되지 않은 사용자와 장치는 모든 메뉴(사용자, 출입문, 비주얼 맵, 출입통제, 모니터링, 장치, 근태)에 나타나지 않습니다. 뿐만 아니라 출입문이나 구역에 선택되지 않은 장치가 하나라도 포함되어 있으면, 해당 출입문이나 구역은 표시되지 않습니다.

새로운 관리자 권한 추가하기

1. 메뉴 표시줄에서 관리자 > 관리자계정을 클릭합니다. 관리자 계정 목록 대화 상자가 나타납니다.
2. **개별 권한 설정**을 클릭합니다.
3. 개별 권한 목록 대화 상자에서 **개별 권한 추가**를 클릭합니다. 개별 권한 설정 대화 상자가 나타납니다.

3. BioStar 설정하기



4. 이름 필드에 권한 이름을 입력합니다.
5. 설명 필드에 보충 설명을 입력합니다.
6. 아래 목록 상자에서 접근 권한을 부여할 메뉴를 선택합니다.
7. 사용자 메뉴나 장치 메뉴를 선택한 경우, 사용자나 장치 목록에서 접근 권한을 허가할 사용자나 장치를 선택합니다.
8. 접근 권한 옵션에서 허가할 접근 권한(모든 권한, 수정, 읽기)을 선택합니다.
9. 추가를 클릭하여 선택한 사항을 적용합니다.
10. 6~9 단계를 반복하여 각 메뉴에 적용되는 접근 권한을 설정합니다.
11. 모든 설정을 마쳤으면 저장을 클릭합니다.

3.2 장치 설정하기

이 절에서는 BioStar 의 장치 마법사를 이용하여 새로운 장치를 검색하고 추가하는 방법에 관해서 설명합니다. 뿐만 아니라 BioStar 시스템에서 장치를 설정하는 기본적인 방법에 관해서 설명합니다. 장치 설정에 관한 자세한 내용은 3.10.3 과 5.1 을 참조하십시오.

3.2.1 장치 추가하기

BioStar 는 사용자가 쉽게 장치를 검색하고 추가할 수 있도록 편리한 마법사를 포함하고 있습니다. 장치를 검색하기 전에 먼저 장치가 올바르게 연결되어 있는지 확인해야 합니다. 만약 한번에 여러 장치를 추가하려 한다면, 장치를 추가하기에 앞서 미리 각 장치의 위치, ID, IP 주소를 적어두면 편리합니다.

3. BioStar 설정하기

장치 추가하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 작업 창에서 **장치 추가**를 클릭합니다.
3. 장치 검색/추가 대화 상자가 나타나면, 검색 방법을 선택합니다.
 - **LAN**: 이더넷이나 무선 랜으로 연결된 장치를 검색합니다.
 - **Serial**: 클라이언트 컴퓨터에 RS485 나 RS232 로 연결된 장치를 검색하거나 또는 클라이언트 컴퓨터에 연결된 장치에 RS485 로 다시 연결된 슬레이브 장치를 검색할 수 있습니다. (3.2.2 참조).
 - **USB 장치**: USB 로 연결된 장치를 검색합니다.

주의: BioStar 1.3 이상은 Windows 7 에서 BioStation 을 연결할 수 있는 USB 드라이버를 포함하고 있습니다. 이 드라이버는 이전 버전의 BioStar 와 호환되지 않습니다. 이전 버전의 BioStar 를 사용하고 있다면 올바른 USB 드라이버를 설치하십시오.

- **가상 단말기**: USB 드라이브에 추가한 가상 장치를 검색합니다.
4. 다음을 클릭합니다.
 5. USB 장치나 가상 단말기를 선택했다면 7 단계로 건너뛰십시오. **LAN** 이나 **Serial** 을 선택했다면 고급 검색 기준을 설정해야 합니다.
 - **LAN** 을 선택한 경우: 어떤 프로토콜을 사용하여 검색할지 선택합니다. TCP 를 선택하면, IP 주소 범위(직접 입력)와 검색하려는 장치의 종류에 따른 검색 포트번호 (BioStation / X-Station / BioStation T2 / FaceStation: 1470, BioEntry Plus / BioEntry W / BioLite Net / Xpass / Xpass S2: 1471, BioStation 2 / BioStation A2 / BioStation L2 / BioEntry W2: 51212, Custom-직접 입력)를 입력해야 합니다. UDP 를 선택하면, 같은 서브넷에 있는 장치를 별다른 설정없이 검색할 수 있습니다.
 - **Serial** 을 선택한 경우: COM 포트(**COM1~COM8** 또는 **모든 포트**)를 선택한 후 통신속도를 선택합니다. RS485 네트워크 연결 시, PC의 COM 포트 하나당 최대 31 대의 장치를 연결할 수 있습니다. RS485 배선이 길어지는 경우, 신호 약화를 방지하기 위해 장치의 Dip Switch 를 켜서 종단저항을 걸면, 신호가 정상으로 전달됩니다. 배선이 아주 짧은 경우, 저항을 걸면 오히려 신호가 제대로 전달되지 않습니다. 따라서, 배선의 길이 및 신호의 상태를 고려하여, 종단 저항 선택 스위치의 On/Off 를 선택합니다.

참고: 1.x 장치와 2.x 장치는 RS485 모드 설정이 다릅니다. 1.x 장치는 **사용 안함, 호스트, 슬레이브, PC 연결 모드**를 사용할 수 있으며, 2.x 장치는 **기본값, 호스트, 슬레이브**를 사용할 수 있습니다.

2.x 장치의 RS485 모드가 **기본값**으로 설정되어 있으면 1 개의 장치로 1 개의 출입문을 구성할 수 있습니다. Anti-passback 구역과 같이 2 개의 장치로 1 개의 출입문을 구성하려면 RS485 모드를 **호스트나 슬레이브**로 변경해야 합니다.

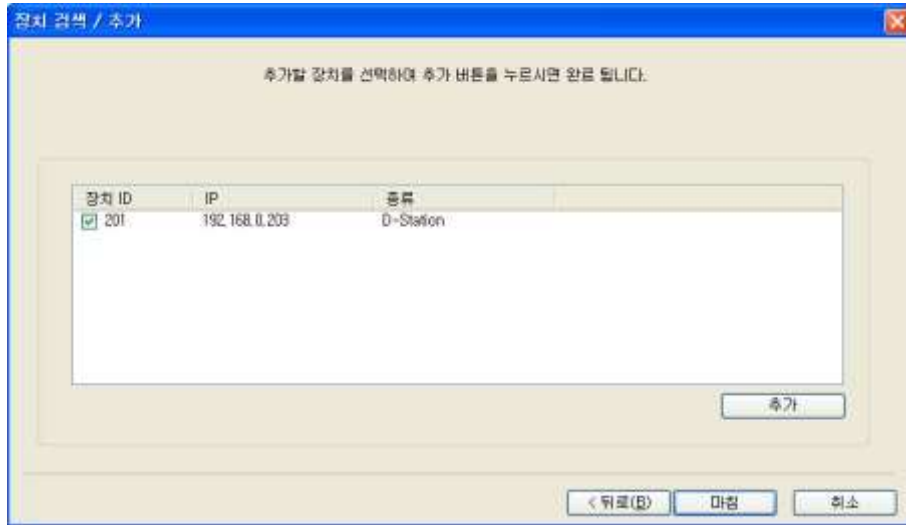
또한, RS485 모드가 **기본값**으로 설정된 장치를 호스트 장치에 RS485 케이블로 연결하면 BioStar 에서 슬레이브 장치로 검색이 가능합니다.

6. 다음을 클릭합니다.
7. 검색이 완료되면 왼쪽의 목록에서 검색된 장치를 확인한 후 다음을 클릭합니다.

참고: 장치 목록에서 장치를 클릭하면 오른쪽의 네트워크 환경 변경 영역에서 장치의 네트워크 설정을 변경할 수 있습니다. 그러나, 네트워크 설정을 변경하면 장치가 목록에서 사라지게 되어 장치를 다시 검색해야 합니다. 그러므로 이 단계에서 설정을 변경하는 것은 권장하지 않습니다.

8. 장치 ID 를 선택한 후 오른쪽 아래에 있는 추가를 클릭합니다.

3. BioStar 설정하기



9. 확인 메시지에서 **확인**을 클릭하여 닫은 다음에 **마침**을 클릭하여 마법사를 종료합니다.

참고: 그룹을 생성하여 그룹별로 장치를 관리할 수 있습니다. 장치 트리에서 그룹을 추가하고자 하는 위치를 마우스 오른쪽 버튼으로 클릭한 후 그룹 추가를 클릭합니다. 그룹에 추가할 장치를 끌어다 놓습니다. 그룹은 하위 4개 수준까지 추가할 수 있습니다. 호스트와 슬레이브 장치는 이동 시 함께 움직입니다.

3.2.2 슬레이브 장치를 검색하고 추가하기

BioStar 는 RS485 네트워크를 이용하여 호스트 장치와 슬레이브 장치를 연결하는 기능을 제공합니다. 이 기능을 이용하면, 오직 호스트 장치만 LAN 을 통하여 컴퓨터에 연결될 수 있습니다. 그런 다음에 RS485 를 이용하여 슬레이브 장치들을 호스트 장치에 연결하면 쉽게 네트워크를 확장할 수 있습니다. 이 기능을 이용하면 BioEntry Plus, Xpass 및 Xpass S2 를 Lift I/O 과 연결하여 엘리베이터 출입을 제어할 수 있습니다.

슬레이브 장치가 네트워크 구성에 포함되어 있다면, 이러한 슬레이브 장치들을 검색해서 시스템에 추가해야 합니다. 먼저 호스트 장치를 설정한 후, 슬레이브 장치를 추가합니다.

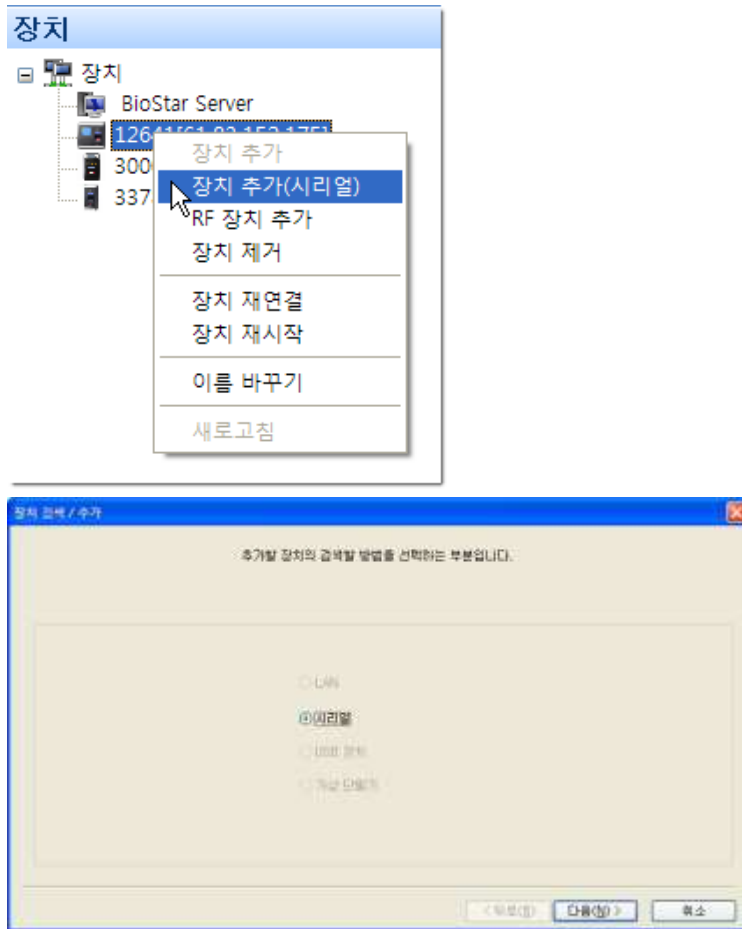
호스트 장치 설정하기

1. 3.2.1의 설명을 따라 호스트 장치를 검색하여 추가합니다.
2. 단축 메뉴 창에서 **장치**를 클릭합니다.
3. 탐색 창에서 호스트 장치를 클릭합니다.
4. 장치 창에서 네트워크 탭을 클릭합니다.
5. 모드 상자의 아래 화살표를 클릭하여 목록에서 **호스트**를 선택합니다.
6. **적용**을 클릭하여 수정 사항을 저장합니다.

슬레이브 장치 추가하기

1. 탐색 창에서 호스트 장치를 오른(오른쪽 마우스 버튼으로) 클릭한 후 **장치 추가(시리얼)**을 클릭합니다. **장치 검색 / 추가** 대화 상자가 나타납니다.

3. BioStar 설정하기



2. 다음을 클릭하여 검색을 시작합니다.
3. BioStar 가 검색을 완료하면 다음을 클릭합니다.
4. 장치 ID 를 선택합니다.
5. 추가를 클릭하여 장치를 추가합니다.
6. 확인 메시지에서 확인을 클릭하여 닫은 다음에 마침을 클릭하여 마법사를 종료합니다.
7. 탐색 창에서 슬레이브 장치를 클릭합니다.
8. 장치 창에서 네트워크 탭을 클릭합니다.
9. 모드 상자의 아래 화살표를 클릭하여 목록에서 슬레이브를 선택합니다.
10. 적용을 클릭하여 수정 사항을 저장합니다.

3.2.3 RF 장치 추가하기

기존에 사용하고 있는 RF 장치를 슈프리마의 출입통제 단말기(BioStation, BioEntry Plus, BioEntry W 및 BioLite Net)에 연결하여 BioStar 시스템에서 독립된 장치로 활용할 수 있습니다. 이렇게 독립된 장치로 연결된 RF 장치를 출입문과 연결할 수 있으며, 또한 구역에 포함할 수도 있습니다.

RF 장치 추가하기

1. RF 장치를 슈프리마의 출입통제 단말기에 연결합니다.
2. 슈프리마 단말기가 BioStar 시스템에 추가되어 있는지 확인합니다(3.2.1 참조).

3. BioStar 설정하기

3. 단축 메뉴 창에서 **장치**를 클릭합니다.
4. 탐색 창에서 RF 장치를 연결한 슈프리마의 출입통제 단말기의 이름을 클릭합니다.
5. 오른쪽의 장치 창에서 위갠드 탭을 클릭한 후 다음과 같이 설정합니다.
6. Wiegand 모드 목록 상자에서 **확장모드**를 선택합니다.
7. Wiegand 입력 목록 상자에서 **Wiegand(카드)**를 선택한 후, 장치 창의 아래에 있는 **적용**을 클릭하여 설정을 저장합니다.
8. 탐색 창에서 RF 장치가 연결된 단말기의 이름을 마우스 오른쪽 버튼으로 클릭한 후 **RF 장치 추가**를 클릭합니다.

참고: RF 장치 사용법에 관한 자세한 내용은 RF 장치의 설명서를 참조하십시오. RF 장치가 슈프리마의 출입통제 장치와 성공적으로 연동하려면 위갠드 형식을 올바르게 설정해야 합니다.

3.2.4 무선 랜으로 장치 연결하기

슈프리마 장치 중에서 BioStation A2, BioStation 2, BioStation 일부 모델(BSTW-OC, BSTW-TC, BSRW-OC, BSRW-TC), BioStation T2, FaceStation 은 무선 랜 통신이 지원됩니다.

무선 랜으로 장치 연결하기

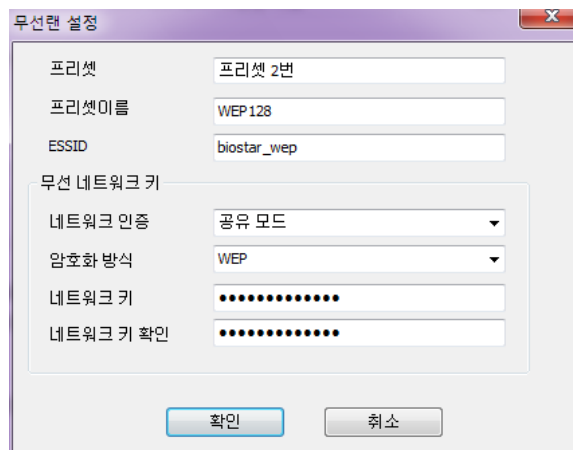
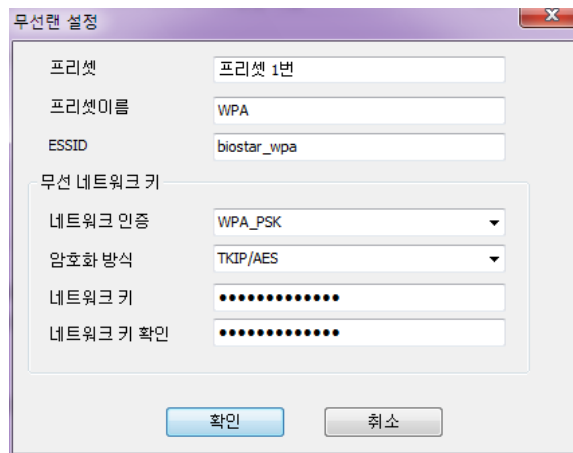
1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 장치 이름을 클릭합니다.
3. 장치 창에서 네트워크 탭을 클릭합니다.
4. 네트워크 종류 목록 상자에서 **무선 랜 사용**을 선택합니다.
5. 무선 랜 환경에 따라 무선 랜 영역 목록 상자에서 **프리셋 1~4 번**을 클릭한 후, **옆에 있는 설정 변경**을 클릭합니다. 프리셋 1 번 또는 2 번을 사용할 경우, 다음과 같이 무선 랜 설정 대화 상자가 나타납니다.

[BioStation 무선 랜 지원 모델]

3. BioStar 설정하기



[BioStation A2, BioStation 2, BioStation T2, FaceStation]



6. 선택 사항: BioStar 에서 정의한 프리셋 1 번 또는 2 번 무선 랜 설정을 사용하지 않고, 프리셋 3 번 또는 4 번을 사용한다면, 다음 옵션을 설정합니다.
 - **프리셋 이름:** 사용 가능한 무선 공유기(AP 장비)의 이름을 입력합니다.
 - **ESSID:** 무선 공유기의 고유 ID 를 입력합니다.
 - **네트워크 인증:** 네트워크 인증 모드(개방 모드, 공유 모드, WPA-PSK)를 선택합니다. 장치와 무선 공유기는 동일한 인증 모드를 사용해야 합니다.
 - **암호화 방식:** 암호화 수준을 선택합니다.
 - **네트워크 키:** 네트워크 키를 입력합니다. 기본적으로 프리셋 1 번 biostation_wpa 와 biostar_wpa 의 네트워크 키는 ‘_suprema_wpa_’, 프리셋 2 번 biostation_wep, biostar_wep 의 네트워크 키는 ‘_suprema_wep_’로 설정되어 있습니다.

3. BioStar 설정하기

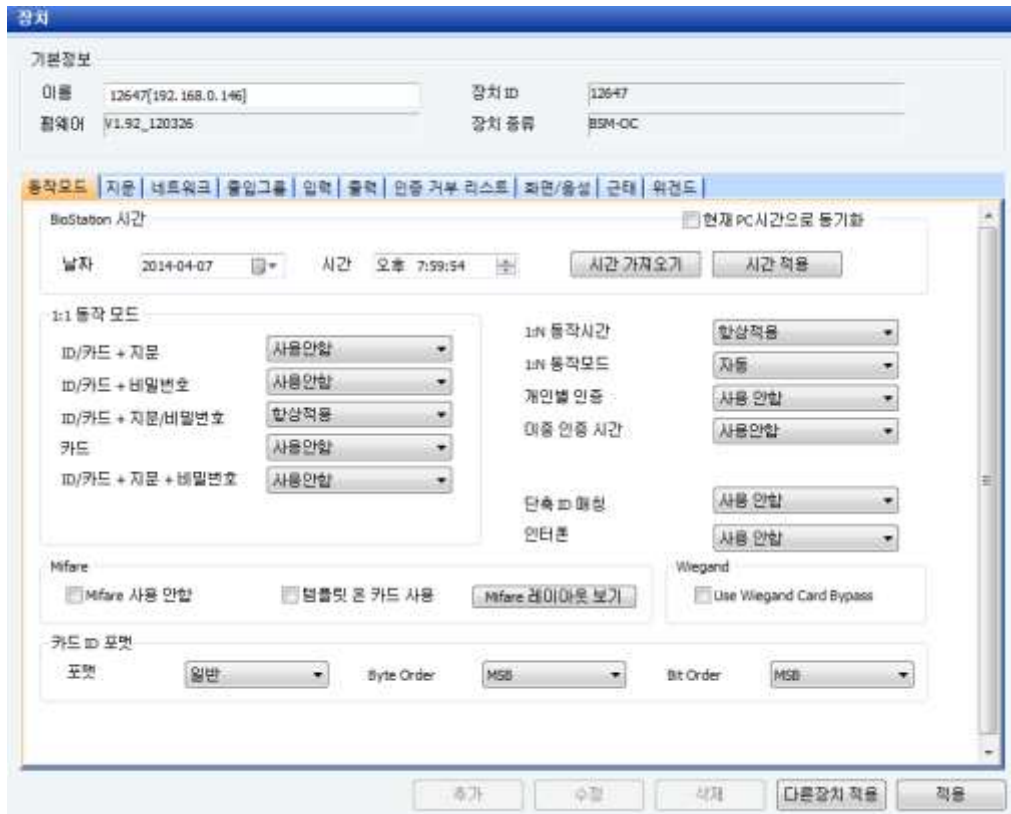
- **네트워크 키 확인:** 네트워크 키를 한번 더 입력합니다.
7. **확인**을 클릭합니다.

3.2.5 BioStation 설정하기

이 절에서는 BioStar 프로그램을 이용하여 BioStation 을 설정하는 방법에 관해서 설명합니다. 자세한 정보는 장치와 함께 제공되는 사용자가이드를 참고하십시오.

BioStation 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 BioStation 의 장치 이름을 두 번 클릭합니다. 장치 창이 나타납니다.



3. 각 탭에서 장치의 정보를 설정합니다. 장치 설정에 관한 자세한 내용은 5.1.1 을 참조하십시오.
 - **동작모드:** 장치의 시간을 설정하거나, 호스트 PC 에서 시간을 가져오도록 설정하거나, 동작모드의 세부사항을 설정할 수 있습니다.
 - **지문:** 지문 인식과 관련된 보안 등급, 품질, 서버 매칭, 인증 제한 시간 옵션을 설정할 수 있습니다.
 - **네트워크:** 이더넷이나 시리얼 연결 옵션을 설정할 수 있습니다.
 - **출입그룹:** 개별 장치에 적용될 출입 제한이나 기본 출입그룹 옵션을 설정할 수 있습니다.
 - **입력:** 장치로 들어오는 입력을 추가하거나, 수정하거나, 삭제할 수 있습니다.
 - **출력:** 장치에서 내보내는 출력을 추가하거나, 수정하거나, 삭제할 수 있습니다.
 - **인증 거부 리스트:** 카드를 분실했거나 퇴사한 사용자가 있을 때 인증 거부 기능을 사용하여 특정 카드의 인증을 거부하도록 설정할 수 있습니다. 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있으며, 사용자 ID 또는 카드 ID 를 등록하면 해당 카드를 가진 사람이 인증을 시도할 때 장치에서 인증이 거부됩니다.

3. BioStar 설정하기

- **화면/음성:** 화면이나 소리 설정을 조절할 수 있으며 배경 화면이나 소리를 추가할 수 있습니다.
 - **근태:** 근태와 관련된 기능을 설정할 수 있습니다.
 - **Wiegand:** 위갠드 형식을 설정할 수 있습니다. 위갠드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.
4. **적용**을 클릭하여 변경 사항을 저장합니다.
 5. 장치의 설정을 다른 장치에도 적용하려면, **다른 장치 적용**을 클릭한 후 장치 트리 대화 상자에서 장치를 선택한 다음, **확인**을 클릭합니다.

3.2.6 BioEntry Plus 및 BioEntry W 설정하기

BioEntry Plus 및 BioEntry W 장치 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 BioEntry Plus 의 장치 이름을 두 번 클릭합니다. 장치 창이 나타납니다.

The screenshot shows the '장치' (Device) configuration window for BioEntry Plus. It includes a '기본정보' (Basic Information) section with fields for Name, Device ID, Firmware, and Device Type. Below this is a '동작모드' (Operation Mode) section with tabs for '지문' (Fingerprint), '네트워크' (Network), '출입그룹' (Access Groups), '입력' (Input), '출력' (Output), '인증 거부 리스트' (Authentication Denial List), '커맨드카드' (Command Card), '화면/음성' (Screen/Audio), '근태' (Attendance), and '위갠드' (Wiegand). The '동작모드' tab is selected, showing 'BioEntry Plus 시간' (BioEntry Plus Time) settings, '동작 모드' (Operation Mode) options, 'Mifare/CLASS' settings, 'Wiegand' settings, and '카드 ID 포맷' (Card ID Format) options. Buttons for '추가' (Add), '수정' (Modify), '삭제' (Delete), '다른장치 적용' (Apply to other devices), and '적용' (Apply) are at the bottom.

3. 각 탭에서 장치의 정보를 설정합니다. 장치 설정에 관한 자세한 내용은 5.1.2 를 참조하십시오.
 - **동작모드:** 장치의 시간을 설정하거나, 호스트 PC 에서 시간을 가져오도록 설정하거나, 동작모드의 세부사항을 설정하거나, 지문 인식 옵션을 설정할 수 있습니다.
 - **지문:** 지문 인식과 관련된 보안 등급, 품질, 서버 매칭, 인증 제한 시간 옵션을 설정할 수 있습니다.
 - **네트워크:** 이더넷이나 시리얼 연결 옵션을 설정할 수 있습니다.
 - **출입그룹:** 출입 제한이나 출입그룹을 설정할 수 있습니다.
 - **입력:** 장치로 들어오는 입력을 추가하거나 수정할 수 있습니다.
 - **출력:** 장치에서 내보내는 출력을 추가하거나 수정할 수 있습니다.

3. BioStar 설정하기

- **인증 거부 리스트:** 카드를 분실했거나 퇴사한 사용자가 있을 때 인증 거부 기능을 사용하여 특정 카드의 인증을 거부하도록 설정할 수 있습니다. 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있으며, 사용자 ID 또는 카드 ID 를 등록하면 해당 카드를 가진 사람이 인증을 시도할 때 장치에서 인증이 거부됩니다.
 - **커맨드카드:** BioEntry Plus 및 BioEntry W 장치를 제어할 때 필요한 커맨드 카드를 발급할 수 있습니다. 커맨드 카드 발급에 관한 자세한 내용은 3.2.6.1 을 참조하십시오.
 - **화면/음성:** 이벤트 별 LED 나 Buzzer 설정을 할 수 있습니다.
 - **Wiegand:** 위갠드 형식을 설정할 수 있습니다. 위갠드 형식에 관한 자세한 사항은 3.2.16 을 참조하십시오.
4. **적용**을 클릭하여 변경 사항을 저장합니다.
 5. 동일한 설정을 다른 장치에 적용하려면, **다른 장치 적용**을 클릭한 후 장치 트리 대화 상자에서 설정을 적용할 다른 장치를 선택한 후, **확인**을 클릭합니다.

3.2.6.1 커맨드 카드 발급하기

커맨드 카드를 이용하면 BioEntry Plus 및 BioEntry W 장치에서 직접 사용자를 등록하거나 삭제할 수 있습니다. 커맨드 카드를 이용해 사용자를 등록하는 방법에 관한 자세한 내용은 3.6.2.3 을 참조하십시오. 커맨드 카드를 이용해 개별 또는 모든 사용자를 삭제하는 방법에 관한 자세한 내용은 4.5.1.1 과 4.5.1.2 를 참조하십시오.

커맨드 카드 발급하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 BioEntry Plus 또는 BioEntry W 장치의 이름을 클릭합니다.
3. 장치 창에서 커맨드카드 탭을 클릭합니다.
4. **카드 읽기**를 클릭합니다.
5. 장치에 커맨드 카드를 댁니다.
6. 커맨드 종류 목록 상자에서 카드에 입력할 커맨드 종류를 선택합니다.
7. 관리자로부터 인증을 받은 후에 카드를 사용할 수 있게 하려면, 관리자 인증 필요 체크 상자를 선택합니다.
8. **추가**를 클릭합니다.

3.2.7 BioLite Net 설정하기

BioLite Net 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 BioLite Net 의 장치 이름을 두 번 클릭합니다. 장치 창이 나타납니다.
3. 각 탭에서 장치의 정보를 설정합니다. 장치 설정에 관한 자세한 내용은 5.1.3 를 참조하십시오.
 - **동작모드:** 장치의 시간을 설정하거나, 호스트 PC 에서 시간을 가져오도록 설정하거나, 동작모드의 세부사항을 설정하거나, 지문 인식 옵션을 설정할 수 있습니다.
 - **지문:** 지문 인식과 관련된 보안 등급, 품질, 서버 매칭, 인증 제한 시간 옵션을 설정할 수 있습니다.
 - **네트워크:** 이더넷이나 시리얼 연결 옵션을 설정할 수 있습니다.

3. BioStar 설정하기

- **출입그룹:** 출입 제한이나 출입그룹을 설정할 수 있습니다.
 - **입력:** 장치로 들어오는 입력을 추가하거나 수정할 수 있습니다.
 - **출력:** 장치에서 내보내는 출력을 추가하거나 수정할 수 있습니다.
 - **인증 거부 리스트:** 카드를 분실했거나 퇴사한 사용자가 있을 때 인증 거부 기능을 사용하여 특정 카드의 인증을 거부하도록 설정할 수 있습니다. 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있으며, 사용자 ID 또는 카드 ID 를 등록하면 해당 카드를 가진 사람이 인증을 시도할 때 장치에서 인증이 거부됩니다.
 - **화면/음성:** 이벤트 별 LED 나 Buzzer 설정을 할 수 있으며, 언어 및 구성 파일을 변경할 수 있습니다.
 - **T&A:** 근태관리 기능을 설정할 수 있습니다.
 - **Wiegand:** 위갠드 형식을 설정할 수 있습니다. 위갠드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.
4. **적용**을 클릭하여 변경 사항을 저장합니다.
 5. 동일한 설정을 다른 장치에 적용하려면, **다른 장치 적용**을 클릭한 후 장치 트리 대화 상자에서 설정을 적용할 다른 장치를 선택한 다음, **확인**을 클릭합니다.

3.2.8 Xpass 및 Xpass S2 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 Xpass 의 장치 이름을 두 번 클릭합니다. 장치 창이 나타납니다.
 - **인증 거부 리스트:** 카드를 분실했거나 퇴사한 사용자가 있을 때 인증 거부 기능을 사용하여 특정 카드의 인증을 거부하도록 설정할 수 있습니다. 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있으며, 사용자 ID 또는 카드 ID 를 등록하면 해당 카드를 가진 사람이 인증을 시도할 때 장치에서 인증이 거부됩니다.
 - **T&A:** 근태 관리 기능을 설정할 수 있습니다.
 - **Wiegand:** 위갠드 형식을 설정할 수 있습니다. 위갠드 형식에 관한 자세한 내용은 3.2.15 를 참조하십시오.
3. 각 탭에서 장치의 정보를 설정합니다. 장치 설정에 관한 자세한 내용은 5.1.4(Xpass) 또는 5.1.5 (Xpass S2)를 참조하십시오.
 - **동작모드:** 장치의 시간을 설정하거나, 호스트 PC 에서 시간을 가져오도록 설정하거나, 동작 모드의 세부사항을 설정할 수 있습니다. Xpass S2 는 Mifare 템플릿 카드를 지원하지 않습니다.
 - **네트워크:** 이더넷이나 시리얼 연결 옵션을 설정할 수 있습니다.
 - **출입그룹:** 출입 제한이나 출입그룹을 설정할 수 있습니다.
 - **입력:** 장치로 들어오는 입력을 추가하거나 수정할 수 있습니다.
 - **출력:** 장치에서 내보내는 출력을 추가하거나 수정할 수 있습니다.
 - **커맨드카드:** Xpass 및 Xpass S2 장치를 제어할 때 필요한 커맨드 카드를 발급할 수 있습니다. 커맨드 카드 발급에 관한 자세한 내용은 3.2.8.1 을 참조하십시오.
 - **화면/음성:** 이벤트 별 LED 나 Buzzer 를 설정할 수 있습니다.
 - **Wiegand:** 위갠드 형식을 설정할 수 있습니다. 위갠드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.
4. 장치 설정을 완료하면, **적용**을 클릭하여 변경 사항을 저장합니다.
5. 동일한 설정을 다른 장치에 적용하려면, **다른 장치 적용**을 클릭한 후 장치 트리 대화 상자에서 설정을 적용할 다른 장치를 선택한 다음, **확인**을 클릭합니다.

3. BioStar 설정하기

3.2.8.1 커맨드 카드 발급하기

커맨드 카드를 이용하면 Xpass 및 Xpass S2 에서 직접 사용자를 등록하거나 삭제할 수 있습니다. 커맨드 카드를 이용해 사용자를 등록하는 방법에 관한 자세한 내용은 3.6.2.3 을 참조하십시오. 커맨드 카드를 이용해 개별 또는 모든 사용자를 삭제하는 방법에 관한 자세한 내용은 4.5.1.1 과 4.5.1.2 를 참조하십시오.

커맨드 카드 발급하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 Xpass 장치의 이름을 클릭합니다.
3. 장치 창에서 커맨드카드 탭을 클릭합니다.

카드ID	커맨드

커맨드 종류: 0 - 0

커맨드 종류: 등록 카드

관리자 인증 필요

Buttons: 삭제, 모두 삭제, 카드 읽기, 추가

4. **카드 읽기**를 클릭합니다.
5. 장치에 커맨드 카드를 겁니다.
6. 커맨드 종류 목록 상자에서 카드에 입력할 커맨드 종류를 선택합니다.
7. 관리자로부터 인증을 받은 후에 카드를 사용할 수 있게 하려면, 관리자 인증 필요 체크 상자를 선택합니다.
8. **추가**를 클릭합니다.

3.2.9 X-Station 설정하기

X-Station 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 장치 이름을 두 번 클릭합니다. 장치 창이 나타납니다.
3. 각 탭에서 장치의 정보를 설정합니다. 장치 설정에 관한 자세한 내용은 5.1.6 을 참조하십시오.
 - **동작모드**: 장치의 시간을 설정하거나, 호스트 PC 에서 시간을 가져오도록 설정하거나, 동작모드의 세부사항을 설정할 수 있습니다.

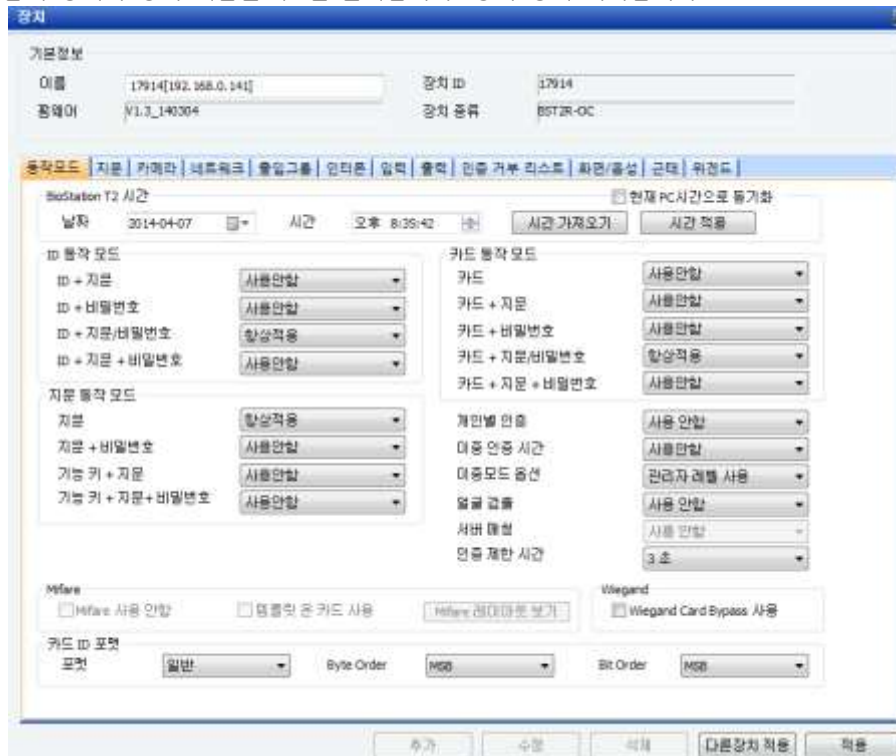
3. BioStar 설정하기

- **카메라:** 출입시간대별 발생하는 이벤트에 따라 카메라의 작동을 설정할 수 있습니다.
 - **네트워크:** 이더넷이나 시리얼 연결 옵션을 설정할 수 있습니다.
 - **출입그룹:** 개별 장치에 적용될 출입 제한이나 기본 출입그룹 옵션을 설정할 수 있습니다.
 - **입력:** 장치로 들어오는 입력을 추가하거나, 수정하거나, 삭제할 수 있습니다.
 - **출력:** 장치에서 내보내는 출력을 추가하거나, 수정하거나, 삭제할 수 있습니다.
 - **인증 거부 리스트:** 카드를 분실했거나 퇴사한 사용자가 있을 때 인증 거부 기능을 사용하여 특정 카드의 인증을 거부하도록 설정할 수 있습니다. 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있으며, 사용자 ID 또는 카드 ID 를 등록하면 해당 카드를 가진 사람이 인증을 시도할 때 장치에서 인증이 거부됩니다.
 - **화면/음성:** 화면이나 소리 설정을 조절할 수 있으며 배경 화면이나 소리를 추가할 수 있습니다.
 - **근태:** 근태와 관련된 기능을 설정할 수 있습니다.
 - **Wiegand:** 위갠드 형식을 설정할 수 있습니다. 위갠드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.
4. 장치 설정을 완료하면, **적용**을 클릭하여 변경 사항을 저장합니다.
 5. 동일한 설정을 다른 장치에 적용하려면, **다른 장치 적용**을 클릭한 후 장치 트리 대화 상자에서 설정을 적용할 다른 장치를 선택한 다음, **확인**을 클릭합니다.

3.2.10 BioStation T2 설정하기

BioStation T2 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 장치 이름을 두 번 클릭합니다. 장치 창이 나타납니다.



3. 각 탭에서 장치의 정보를 설정합니다. 장치 설정에 관한 자세한 내용은 5.1.7 을 참조하십시오.

3. BioStar 설정하기

- **동작모드:** 장치의 시간을 설정하거나, 호스트 PC 에서 시간을 가져오도록 설정하거나, 동작모드의 세부사항을 설정할 수 있습니다.
 - **지문:** 지문 인식과 관련된 보안 등급, 품질, 서버 매칭, 인증 제한 시간 옵션을 설정할 수 있습니다.
 - **카메라:** 출입시간대별 발생하는 이벤트에 따라 카메라의 작동을 설정할 수 있습니다.
 - **네트워크:** 이더넷이나 시리얼 연결 옵션을 설정할 수 있습니다.
 - **출입그룹:** 개별 장치에 적용될 출입 제한이나 기본 출입그룹 옵션을 설정할 수 있습니다.
 - **인터폰:** 장치를 인터폰으로 사용하기 위한 옵션을 설정할 수 있습니다.
 - **입력:** 장치로 들어오는 입력을 추가하거나, 수정하거나, 삭제할 수 있습니다.
 - **출력:** 장치에서 내보내는 출력을 추가하거나, 수정하거나, 삭제할 수 있습니다.
 - **인증 거부 리스트:** 카드를 분실했거나 퇴사한 사용자가 있을 때 인증 거부 기능을 사용하여 특정 카드의 인증을 거부하도록 설정할 수 있습니다. 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있으며, 사용자 ID 또는 카드 ID 를 등록하면 해당 카드를 가진 사람이 인증을 시도할 때 장치에서 인증이 거부됩니다.
 - **화면/음성:** 화면이나 소리 설정을 조절할 수 있으며 배경 화면이나 소리를 추가할 수 있습니다.
 - **근태:** 근태와 관련된 기능을 설정할 수 있습니다.
 - **Wiegand:** 위갠드 형식을 설정할 수 있습니다. 위갠드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.
4. 장치 설정을 완료하면, **적용**을 클릭하여 변경 사항을 저장합니다.
 5. 동일한 설정을 다른 장치에 적용하려면, **다른 장치 적용**을 클릭한 후 장치 트리 대화 상자에서 설정을 적용할 다른 장치를 선택한 다음, **확인**을 클릭합니다.

3.2.11 FaceStation 설정하기

FaceStation 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.

3. BioStar 설정하기

2. 탐색 창에서 장치 이름을 두 번 클릭합니다. 장치 창이 나타납니다.



3. 각 탭에서 장치의 정보를 설정합니다. 장치 설정에 관한 자세한 내용은 5.1.8 를 참조하십시오.
 - **동작모드:** 장치의 시간을 설정하거나, 호스트 PC 에서 시간을 가져오도록 설정하거나, 동작모드의 세부사항을 설정할 수 있습니다.
 - **얼굴:** 얼굴 인식과 관련된 보안 등급과 등록 품질 기준을 설정할 수 있습니다.
 - **카메라:** 출입시간대별 발생하는 이벤트에 따라 카메라의 작동을 설정할 수 있습니다.
 - **네트워크:** 이더넷이나 시리얼 연결 옵션을 설정할 수 있습니다.
 - **출입그룹:** 개별 장치에 적용될 출입 제한이나 기본 출입그룹 옵션을 설정할 수 있습니다.
 - **인터폰:** 장치를 인터폰으로 사용하기 위한 옵션을 설정할 수 있습니다.
 - **입력:** 장치로 들어오는 입력을 추가하거나, 수정하거나, 삭제할 수 있습니다.
 - **출력:** 장치에서 내보내는 출력을 추가하거나, 수정하거나, 삭제할 수 있습니다.
 - **화면/음성:** 화면이나 소리 설정을 조절할 수 있으며 배경 화면이나 소리를 추가할 수 있습니다.
 - **근태:** 근태와 관련된 기능을 설정할 수 있습니다.
 - **Wiegand:** 위갠드 형식을 설정할 수 있습니다. 위갠드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.
4. 장치 설정을 완료한 후, **적용**을 클릭하여 변경 사항을 저장합니다.
5. 동일한 설정을 다른 장치에 적용하려면, **다른 장치 적용**을 클릭한 후 장치 트리 대화 상자에서 설정을 적용할 다른 장치를 선택한 다음, **확인**을 클릭합니다.

3.2.12 BioStation 2 설정하기

이 절에서는 BioStar 프로그램을 이용하여 BioStation 2 을 설정하는 방법에 관해서 설명합니다. 자세한 정보는 장치와 함께 제공되는 사용자가이드를 참고하십시오.

BioStation 2 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.

3. BioStar 설정하기

2. 탐색 창에서 BioStation 2 의 장치 이름을 두 번 클릭합니다. 장치 창이 나타납니다.



3. 각 탭에서 장치의 정보를 설정합니다. 장치 설정에 관한 자세한 내용은 5.1.9 를 참조하십시오.
 - **동작모드:** 장치의 시간을 설정하거나, 호스트 PC 에서 시간을 가져오도록 설정하거나, 동작모드의 세부사항을 설정할 수 있습니다.
 - **지문:** 지문 인식과 관련된 보안 등급, 품질, 서버 매칭, 인증 제한 시간 옵션을 설정할 수 있습니다.
 - **네트워크:** 이더넷이나 시리얼 연결 옵션을 설정할 수 있습니다.
 - **출입그룹:** 개별 장치에 적용될 출입 제한이나 기본 출입그룹 옵션을 설정할 수 있습니다.
 - **인터폰:** 장치를 인터폰으로 사용하기 위한 옵션을 설정할 수 있습니다.
 - **입력:** 장치로 들어오는 입력/출력을 추가하거나, 수정하거나, 삭제할 수 있습니다.
 - **인증 거부 리스트:** 카드를 분실했거나 퇴사한 사용자가 있을 때 인증 거부 기능을 사용하여 특정 카드의 인증을 거부하도록 설정할 수 있습니다. 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있으며, 사용자 ID 또는 카드 ID 를 등록하면 해당 카드를 가진 사람이 인증을 시도할 때 장치에서 인증이 거부됩니다.
 - **화면/음성:** 화면이나 소리 설정을 조절할 수 있으며 배경 화면이나 소리를 추가할 수 있습니다.
 - **근태:** 근태와 관련된 기능을 설정할 수 있습니다.
 - **Wiegand:** 위캔드 형식을 설정할 수 있습니다. 위캔드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.
4. 장치 설정을 완료하면, **적용**을 클릭하여 변경 사항을 저장합니다.
5. 동일한 설정을 다른 장치에 적용하려면, **다른 장치 적용**을 클릭한 후 장치 트리 대화 상자에서 설정을 적용할 다른 장치를 선택한 다음, **확인**을 클릭합니다.

3.2.13 BioStation A2 설정하기

이 절에서는 BioStar 프로그램을 이용하여 BioStation A2 를 설정하는 방법에 관해서 설명합니다. 자세한 정보는 장치와 함께 제공되는 사용자가이드를 참고하십시오.

3. BioStar 설정하기

BioStation A2 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 BioStation A2 의 장치 이름을 두 번 클릭합니다. 장치 창이 나타납니다.



3. 각 탭에서 장치의 정보를 설정합니다. 장치 설정에 관한 자세한 내용은 5.1.10 을 참조하십시오.
 - **동작모드:** 장치의 시간을 설정하거나, 호스트 PC 에서 시간을 가져오도록 설정하거나, 동작모드의 세부사항을 설정할 수 있습니다.
 - **지문:** 지문 인식과 관련된 보안 등급, 품질, 서버 매칭, 인증 제한 시간 옵션을 설정할 수 있습니다.
 - **카메라:** 출입시간대별 발생하는 이벤트에 따라 카메라의 작동을 설정할 수 있습니다.
 - **네트워크:** 이더넷이나 시리얼 연결 옵션을 설정할 수 있습니다.
 - **출입그룹:** 개별 장치에 적용될 출입 제한이나 기본 출입그룹 옵션을 설정할 수 있습니다.
 - **인터폰:** 장치를 인터폰으로 사용하기 위한 옵션을 설정할 수 있습니다.
 - **입력:** 장치로 들어오는 입력/출력을 추가하거나, 수정하거나, 삭제할 수 있습니다.
 - **인증 거부 리스트:** 카드를 분실했거나 퇴사한 사용자가 있을 때 인증 거부 기능을 사용하여 특정 카드의 인증을 거부하도록 설정할 수 있습니다. 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있으며, 사용자 ID 또는 카드 ID 를 등록하면 해당 카드를 가진 사람이 인증을 시도할 때 장치에서 인증이 거부됩니다.
 - **화면/음성:** 화면이나 소리 설정을 조절할 수 있으며 배경 화면이나 소리를 추가할 수 있습니다.
 - **근태:** 근태와 관련된 기능을 설정할 수 있습니다.
 - **Wiegand:** 위갠드 형식을 설정할 수 있습니다. 위갠드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.
4. 장치 설정을 완료하면, **적용**을 클릭하여 변경 사항을 저장합니다.
5. 동일한 설정을 다른 장치에 적용하려면, **다른 장치 적용**을 클릭한 후 장치 트리 대화 상자에서 설정을 적용할 다른 장치를 선택한 다음, **확인**을 클릭합니다.

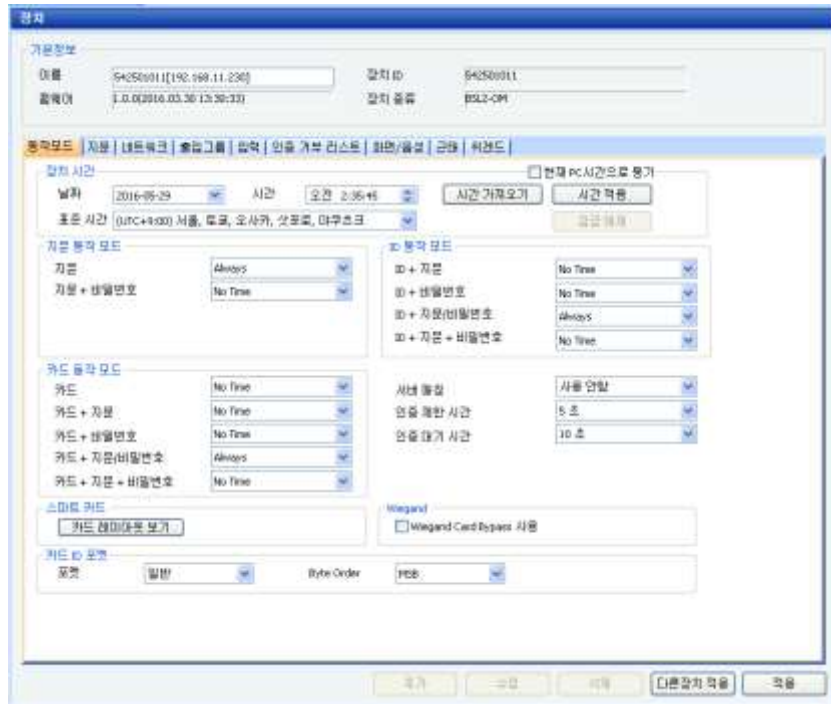
3. BioStar 설정하기

3.2.14 BioStation L2 설정하기

이 절에서는 BioStar 프로그램을 이용하여 BioStation L2 를 설정하는 방법에 관해서 설명합니다. 자세한 정보는 장치와 함께 제공되는 사용자기이드를 참고하십시오.

BioStation L2 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 BioStation L2 의 장치 이름을 두 번 클릭합니다. 장치 창이 나타납니다.



3. 각 탭에서 장치의 정보를 설정합니다. 장치 설정에 관한 자세한 내용은 5.1.11 을 참조하십시오.
 - **동작모드**: 장치의 시간을 설정하거나, 호스트 PC 에서 시간을 가져오도록 설정하거나, 동작모드의 세부사항을 설정할 수 있습니다.
 - **지문**: 지문 인식과 관련된 보안 등급, 품질, 서버 매칭, 인증 제한 시간 옵션을 설정할 수 있습니다.
 - **네트워크**: 이더넷이나 시리얼 연결 옵션을 설정할 수 있습니다.
 - **출입그룹**: 개별 장치에 적용될 출입 제한이나 기본 출입그룹 옵션을 설정할 수 있습니다.
 - **입력**: 장치로 들어오는 입력/출력을 추가하거나, 수정하거나, 삭제할 수 있습니다.
 - **인증 거부 리스트**: 카드를 분실했거나 퇴사한 사용자가 있을 때 인증 거부 기능을 사용하여 특정 카드의 인증을 거부하도록 설정할 수 있습니다. 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있으며, 사용자 ID 또는 카드 ID 를 등록하면 해당 카드를 가진 사람이 인증을 시도할 때 장치에서 인증이 거부됩니다.
 - **화면/음성**: 화면이나 소리 설정을 조절할 수 있으며 배경 화면이나 소리를 추가할 수 있습니다.
 - **근태**: 근태와 관련된 기능을 설정할 수 있습니다.
 - **Wiegand**: 위갠드 형식을 설정할 수 있습니다. 위갠드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.
4. 장치 설정을 완료하면, **적용**을 클릭하여 변경 사항을 저장합니다.
5. 동일한 설정을 다른 장치에 적용하려면, **다른 장치 적용**을 클릭한 후 장치 트리 대화 상자에서 설정을 적용할 다른 장치를 선택한 다음, **확인**을 클릭합니다.

3. BioStar 설정하기

3.2.15 BioEntry W2 설정하기

이 절에서는 BioStar 프로그램을 이용하여 BioEntry W2 를 설정하는 방법에 관해서 설명합니다. 자세한 정보는 장치와 함께 제공되는 사용자가이드를 참고하십시오.

BioEntry W2 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 BioEntry W2 의 장치 이름을 두 번 클릭합니다. 장치 창이 나타납니다.

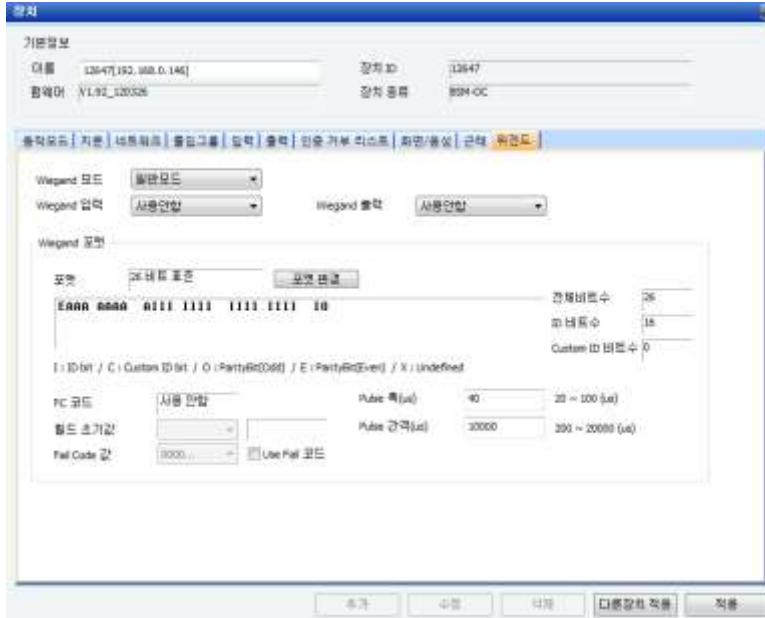


3. 각 탭에서 장치의 정보를 설정합니다. 장치 설정에 관한 자세한 내용은 5.1.12 를 참조하십시오.
 - **동작모드:** 장치의 시간을 설정하거나, 호스트 PC 에서 시간을 가져오도록 설정하거나, 동작모드의 세부사항을 설정할 수 있습니다.
 - **지문:** 지문 인식과 관련된 보안 등급, 품질, 서버 매칭, 인증 제한 시간 옵션을 설정할 수 있습니다.
 - **네트워크:** 이더넷이나 시리얼 연결 옵션을 설정할 수 있습니다.
 - **출입그룹:** 개별 장치에 적용될 출입 제한이나 기본 출입그룹 옵션을 설정할 수 있습니다.
 - **입력:** 장치로 들어오는 입력/출력을 추가하거나, 수정하거나, 삭제할 수 있습니다.
 - **인증 거부 리스트:** 카드를 분실했거나 퇴사한 사용자가 있을 때 인증 거부 기능을 사용하여 특정 카드의 인증을 거부하도록 설정할 수 있습니다. 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있으며, 사용자 ID 또는 카드 ID 를 등록하면 해당 카드를 가진 사람이 인증을 시도할 때 장치에서 인증이 거부됩니다.
 - **화면/음성:** 이벤트 별 LED 나 Buzzer 설정을 할 수 있습니다.
 - **근태:** 근태와 관련된 기능을 설정할 수 있습니다.
 - **Wiegand:** 위젯드 형식을 설정할 수 있습니다. 위젯드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.
4. 장치 설정을 완료하면, **적용**을 클릭하여 변경 사항을 저장합니다.
5. 동일한 설정을 다른 장치에 적용하려면, **다른 장치 적용**을 클릭한 후 장치 트리 대화 상자에서 설정을 적용할 다른 장치를 선택한 다음, **확인**을 클릭합니다.

3. BioStar 설정하기

3.2.16 위갠드 형식 변경하기

BioStar에서는 장치의 입력과 출력을 제어하기 위하여 위갠드 형식을 설정할 수 있습니다.



Wiegand 형식 설정하기

1. 단축 메뉴 창에서 장치를 클릭합니다.
2. 탐색 창에서 장치의 이름을 클릭합니다.
3. 장치 창에서 위갠드 탭을 클릭합니다.
4. 포맷 변경을 클릭합니다. Wiegand 설정 대화 상자가 나타납니다.
5. 다음 형식 중에 하나를 선택합니다.
 - **26 비트 표준 Wiegand 포맷:** 일반적으로 가장 널리 사용되는 형식이며, 8 비트 FC 코드와 16 비트 ID 로 이루어집니다. 이 형식은 비트 정의와 패리티 비트는 변경할 수 없습니다.
 - **패스 스루 Wiegand 포맷:** ID 비트만 변경할 수 있습니다. 인증하는 동안에 ID 가 인식되면, Wiegand 입력 데이터가 본래의 형태 그대로 전달됩니다. 이 형식의 패리티 비트나 다른 대체 값은 변경할 수 없습니다. 정의에 따르자면, 패스 스루 형식은 1:1 동작모드에서 유용합니다. 1:N 모드에서 ID 가 아닌 비트들은 모두 0 으로 설정됩니다. BioStation 2, BioStation A2, BioStation L2, BioEntry W2 는 지원하지 않습니다.
 - **사용자 설정 Wiegand 포맷:** 사용자 설정 형식을 이용하면, ID 비트, Custom ID 비트, 패리티 비트, 대체 값을 설정할 수 있습니다.
6. Wiegand 설정 대화 상자를 이용하여 필요에 맞게 위갠드 형식을 설정합니다. (자세한 내용은 다음 절 참조)
7. 적용을 클릭하여 변경 사항을 저장합니다.

3. BioStar 설정하기

3.2.16.1 26 비트 표준 위갠드 형식 설정하기

26 비트 표준 위갠드 형식을 선택하였다면, FC 코드만 변경할 수 있습니다.

FC 코드 변경하기

1. 26 비트 표준 Wiegand 포맷을 선택한 후 Wiegand 설정 - Alternative Value 대화 상자가 나올 때까지 다음을 클릭합니다.



2. FC Code 체크 상자를 선택한 후 FC 코드를 입력합니다.
3. 마침을 클릭하여 대화 상자를 닫습니다.

3.2.16.2 패스 스루 Wiegand 형식 설정하기

패스 스루 형식을 선택하면 총 비트 수를 변경할 수 있으며 ID 비트로 사용할 구간을 설정할 수 있습니다.

패스 스루 Wiegand 형식 설정하기

1. 패스 스루 Wiegand 포맷을 선택한 후 다음을 클릭합니다. Wiegand Configuration - Format 대화 상자가 나타납니다.



2. 필요하다면 새로운 전체 비트 수를 입력하고 적용을 클릭합니다.
3. 오른쪽에 있는 User ID 버튼(I)을 클릭합니다.
4. 사각형을 클릭하여 ID 비트로 사용할 구간을 설정합니다.
5. Wiegand 설정 - Alternative Value 대화 상자가 나올 때까지 다음을 클릭합니다.
6. 마침을 클릭하여 대화 상자를 닫습니다.

3. BioStar 설정하기

3.2.16.3 사용자 지정 위갠드 형식 설정하기

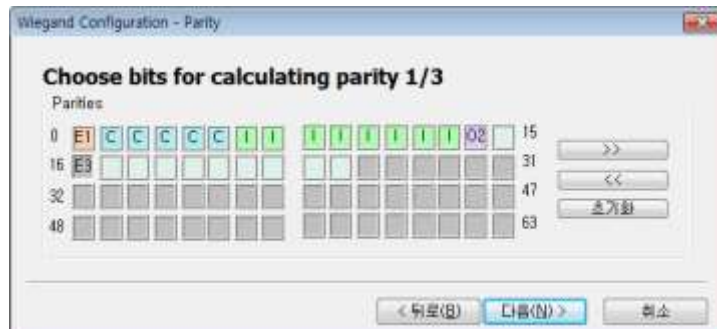
사용자 지정 위갠드 형식을 선택하면 전체 비트 수, 패리티 비트 수를 변경하고, ID 비트 구간 및 Custom ID 비트 구간을 할당하고, 패리티 비트를 정의하고, 특정 출력 데이터 구간에 대한 대체 값을 설정할 수 있습니다.

사용자 지정 위갠드 형식 설정하기

1. 사용자 설정 Wiegand 포맷을 선택한 후 다음을 클릭합니다. Wiegand Configuration - Format 대화 상자가 나타납니다.



2. 필요하다면 새로운 전체 비트 수를 입력하고 적용을 클릭합니다.
3. 패리티 설정이 변경된 경우라면 패리티 초기화를 클릭합니다.
4. 오른쪽에 있는 User ID 버튼(I)을 클릭한 후, 사각형을 클릭하여 ID 비트로 사용할 구간을 설정합니다.
Custom Wiegand Format 에 대하여 개선된 기능을 제공합니다.
5. 오른쪽에 있는 Custom ID 버튼(C)을 클릭한 후, 사각형을 클릭하여 Custom ID 비트로 사용할 구간을 설정합니다.
6. 오른쪽에 있는 Even parity 버튼(E)을 클릭한 후, 사각형을 클릭하여 짝수 패리티를 설정합니다.
7. 오른쪽에 있는 Odd parity 버튼(O)을 클릭한 후, 사각형을 클릭하여 홀수 패리티를 설정합니다.
8. 다음을 클릭합니다.
9. Wiegand Configuration - Parity 대화 상자에서 첫 번째 패리티 비트를 계산하는 데 사용되는 비트를 선택합니다.



10. 필요에 따라, >>을 클릭하여 추가적인 패리티 비트를 계산하는 데 사용될 비트를 선택합니다. 4~5 단계에서 할당된 각 패리티 비트에 대해 이 절차를 수행해야 합니다. 필요하다면, 초기화를 클릭하여 선택을 초기화할 수 있습니다.

3. BioStar 설정하기

11. 다음을 클릭합니다.
12. Wiegand 설정 - Alternative Value 대화 상자에서 변경할 필드(ID 가 아닌 비트만 가능)을 선택합니다.



13. Alt. Value 체크 상자를 선택한 다음 출력 데이터로 사용할 새로운 값을 입력합니다.
14. 필요하다면 10~11 단계를 반복하여 나머지 출력 데이터를 설정합니다.
15. **마침**을 클릭하여 대화 상자를 닫습니다.

3.3 출입문 설정하기

이 절에서는 BioStar 시스템에서 출입문을 설정하는 방법을 설명합니다. 물리적인 구성 장치를 설치하고 그것을 출입문에 연결하는 방법에 관한 정보는 각 장치에 함께 동봉된 사용 설명서를 참조하십시오.

주의: 2.x 장치(BioStation A2, BioStation 2, BioStation L2, BioEntry W2)는 1.x 장치(BioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, Xpass S2, X-Station, BioStation T2, FaceStation)와 함께 출입문을 구성할 수 없습니다.

3.3.1 출입문 추가하기

출입문 추가하기

1. 단축 메뉴 창에서 **출입문**을 클릭합니다.
2. 작업 창에서 **새 출입문 추가**를 클릭합니다.
3. **새 출입문**을 마우스 오른쪽 버튼으로 클릭한 후 **이름 바꾸기**를 클릭하여 출입문에 사용할 이름을 입력합니다.

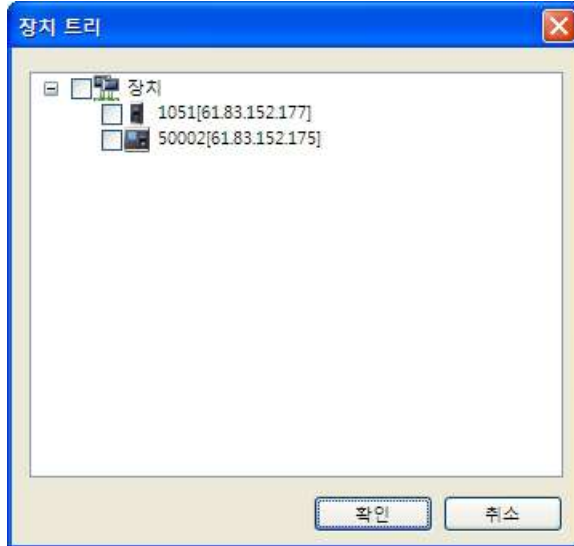
3.3.2 출입문에 장치 연결하기

BioStar 에서는 각 출입문에 최대 2 개의 장치를 연결할 수 있습니다. 하나의 출입문에 2 개의 장치를 연결할 때에는 반드시 RS485 를 이용하여 두 장치를 연결해야 합니다. 출입문 설정에 관한 자세한 내용은 5.2 를 참조하십시오.

출입문에 출입 인증 장치 연결하기

3. BioStar 설정하기

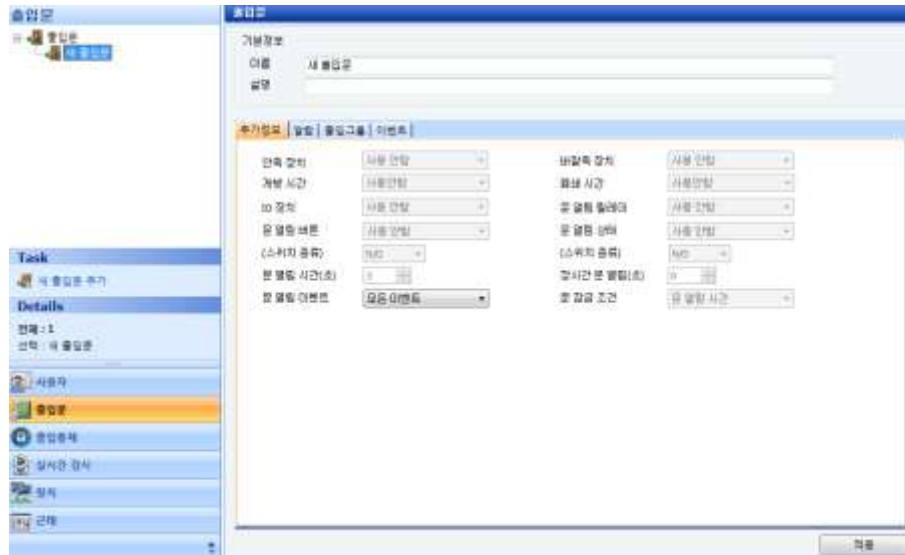
1. 단축 메뉴 창에서 **출입문**을 클릭합니다.
2. 출입문을 마우스 오른쪽 버튼으로 클릭한 후 **장치 추가**를 클릭합니다.
3. 장치 트리에서 장치를 선택합니다.



4. **확인**을 클릭합니다.

3.3.3 출입문 설정하기

1. 단축 메뉴 창에서 **출입문**을 클릭합니다.
2. 탐색 창에서 출입문의 이름을 클릭합니다. 출입문 창이 나타납니다.



3. 각 탭에서 출입문의 정보를 설정합니다. 출입문 설정에 관한 자세한 내용은 5.2 를 참조하십시오.
 - **추가정보:** 출입문, 인증 장치, 잠금 장치, 문 열림 버튼 간의 상호 작용을 설정합니다. 하나의 출입문에 2 개의 출입 인증 장치를 설치하면, 이 탭에서 Anti-passback 기능을 설정할 수 있습니다. 또한, 이중 인증
 - **알람:** 출입문이 강제로 열리거나 열린 채로 오랫동안 방치될 때 장치가 어떤 행동을 취할지 설정합니다.
 - **구역:** 구역을 구성하고 있는 출입문들을 확인할 수 있습니다.
 - **출입그룹:** 출입문에 등록된 출입그룹을 확인할 수 있습니다.

3. BioStar 설정하기

- **이벤트:** 출입문의 이벤트 기록을 가져오거나 확인할 수 있습니다.
4. **적용**을 클릭하여 변경 사항을 저장합니다.

3.3.4 출입문 그룹 만들기

1. 단축 메뉴 창에서 **출입문**을 클릭합니다.
2. 탐색 창에서 **출입문**을 마우스 오른쪽 버튼으로 클릭한 후 **출입문 그룹 추가**를 클릭합니다.
3. 그룹의 이름을 입력한 후 Enter 키를 누릅니다.
4. 그룹에 출입문을 추가하려면, 출입문을 클릭한 채로 그룹에 끌어다 놓습니다.

3.4 리프트 설정하기

이 절에서는 BioStar 시스템에서 엘리베이터를 설정하는 방법을 설명합니다. 해당 장치를 엘리베이터에 설치하고 연결하는 방법에 관해서는 각 장치의 사용 설명서를 참조하십시오. BioStar 는 최대 120 개의 엘리베이터를 지원합니다.

3.4.1 리프트 추가하기

리프트 추가하기

1. 단축 메뉴 창에서 **리프트**를 클릭합니다.
2. 작업 창에서 **새 리프트 추가**를 클릭합니다.
3. **새 리프트**를 마우스 오른쪽 버튼으로 클릭한 후 **이름 바꾸기**를 클릭하여 엘리베이터에 사용할 이름을 입력합니다.

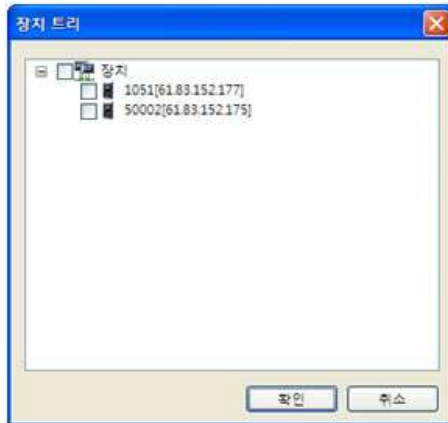
3.4.2 리프트에 출입 장치 연결하기

BioStar 에서는 Xpass 또는 Xpass S2 장치를 Lift I/O 장치와 연결하여 엘리베이터 출입을 제어할 수 있습니다. Lift I/O 장치는 BioEntry Plus, Xpass 및 Xpass S2 장치와 RS485 로 연결해야 합니다.

Xpass 및 Xpass S2 장치를 엘리베이터와 연결하기

1. 단축 메뉴 창에서 **리프트**를 클릭합니다.
2. 리프트 이름을 마우스 오른쪽 버튼으로 클릭한 후 **장치 추가**를 클릭합니다.
3. 장치 트리에서 연결할 장치를 선택합니다.

3. BioStar 설정하기



4. **확인**을 클릭합니다.

3.4.3 리프트 설정하기

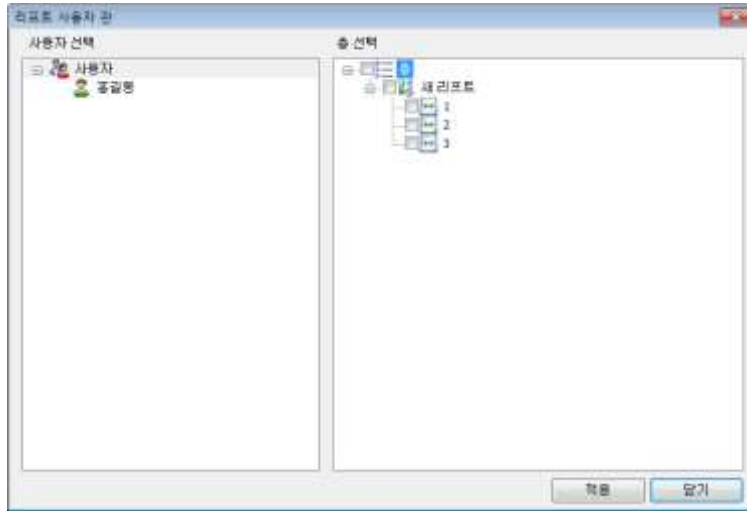
리프트 설정하기

1. 단축 메뉴 창에서 **리프트**를 클릭합니다.
2. 탐색창에서 리프트 이름을 클릭합니다. 리프트 창이 나타납니다.
3. 다음 사항을 설정합니다.
 - **LIFT IO**: Lift I/O 장치를 선택한 후 설정을 확인 및 변경합니다.
 - **릴레이 유지시간 설정**: Lift IO 의 Detail 탭에서 릴레이 유지시간 설정을 지원합니다. 설정 범위의 기본값은 10초이며, 최소 1초에서 60초까지 설정이 가능합니다. LIFT IO를 지원하는 Xpass, Xpass S2, BioEntry Plus 중에서 최신 정규 펌웨어에서만 지원합니다.
주의: 지원 펌웨어 버전: BioEntry Plus 1.6, Xpass 1.3
 - **OUTPUT**: Lift I/O 장치에서 사용할 수 있는 출력의 목록이 표시됩니다.
 - **층**: 출력을 제어하려는 층을 선택합니다. **사용안함**을 해제한 후 선택할 수 있습니다.
 - **사용안함**: LIFT I/O 의 출력 포트를 사용하지 않을 경우는 **사용안함** 체크박스를 선택하고, 출력과 연계하여 해당 층의 출력을 제어하려면 선택 해제합니다.
4. **적용**을 클릭하여 변경 사항을 저장합니다.

3.4.4 리프트에 사용자 추가하기

1. 단축 메뉴 창에서 **리프트**를 클릭합니다.
2. 작업창에서 **사용자 관리**를 클릭합니다. 리프트 사용자 관리 대화 상자가 나타납니다.

3. BioStar 설정하기



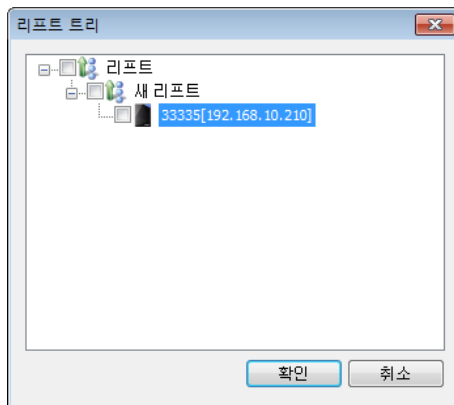
3. 대화 상자의 왼쪽 영역에서 사용자 이름을 클릭합니다.
4. 대화 상자의 오른쪽 영역에서 출입을 허용할 층의 체크박스를 클릭합니다.
5. 적용을 클릭합니다.

3.4.5 장치에 설정 정보 전송하기

주의: BioEntry Plus, Xpass 및 Xpass S2 에서 Lift I/O 정보는 사용자 정보에 포함되어 단말기로 전송됩니다. 리프트 리더로 사용되는 Xpass 및 Xpass S2 의 경우, 사용자 메뉴의 사용자 전송을 사용하면 BioEntry Plus, Xpass 및 Xpass S2 단말기에 저장된 리프트 설정 정보가 모두 초기화됩니다. 리프트 설정을 유지하려면 사용자 메뉴의 사용자 전송 대신 리프트 메뉴의 장치에 전송을 사용하십시오.

장치에 설정 정보 전송하기

1. 단축 메뉴 창에서 리프트를 클릭합니다.
2. 작업창에서 장치에 전송을 클릭합니다. 리프트 트리 대화 상자가 나타납니다.



3. 트리 목록에서 설정을 전송할 장치를 선택합니다.
4. 설정을 전송하려면 확인을 클릭합니다.

3. BioStar 설정하기

3.5 구역 설정하기

BioStar 를 이용하면 하나의 관리 지역을 여러 구역으로 나눠 좀더 정교하게 출입을 통제할 수 있습니다. 구역을 설정하면 출입 인증 장치, 출입문, 슬레이브 장치의 동작을 제어할 수 있습니다. 뿐만 아니라 anti-passback, timed anti-passback, 출입 제한 등과 같은 다양한 기능을 활용할 수 있습니다. 이 절에서는 사용할 구역을 어떻게 선택하는지 그리고 어떻게 구역을 추가하고 설정하는지에 대해서 설명합니다.

주의: 2.x 장치(BioStation A2, BioStation 2, BioStation L2, BioEntry W2)는 1.x 장치(BioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, Xpass S2, X-Station, BioStation T2, FaceStation)와 함께 구역을 구성할 수 없습니다. 또한, BioStation A2, BioStation 2, BioStation L2, BioEntry W2 는 이중출입 방지 구역, 화재 경보 구역으로만 구성할 수 있습니다.

3.5.1 사용할 구역을 결정하기

BioStar 시스템에서는 총 일곱 종류의 구역을 설정할 수 있습니다.

- **출입 구역:** 사용자 정보나 로그 정보를 동기화하려면, 출입 구역을 사용합니다. 사용자 동기화 옵션을 선택하면, 사용자 데이터에 변화가 생길 경우 이 변경된 정보들이 연결된 다른 장치에 자동적으로 전달됩니다. 로그 동기화 옵션을 선택하면, 모든 로그 기록들이 (서버뿐만 아니라) 호스트 장치에 저장됩니다. 이를 통해 호스트 장치에서 모든 로그 기록을 확인할 수 있습니다. 출입 구역 설정에 관한 자세한 내용은 5.3.5 를 참조하십시오.
- **이중출입 방지 구역:** 사용자가 자신의 카드를 제삼자에게 빌려준다든지 자신의 지문을 이용하여 제삼자를 안으로 들이는 상황을 방지하려면, 이중출입 방지 구역을 사용합니다. 이 구역은 두 가지 종류의 anti-passback 옵션(**Soft**, **Hard**)을 지원합니다. **Soft** 를 선택하면, anti-passback 을 위반해도 출입을 허용하며 다만 위반 사실을 사용자 로그에 기록합니다. **Hard** 를 선택하면, 모든 anti-passback 을 허락하지 않으며 위반 사실을 사용자 로그에 기록합니다. 이중출입 방지 구역 설정에 관한 자세한 내용은 5.3.1 를 참조하십시오.
- **인증 제한 구역:** 특정 구역에 사용자가 입장할 수 있는 횟수를 제한하려면 인증 제한 구역을 사용합니다. 인증 제한 구역을 출입시간(timezone)에 포함할 수도 있습니다. 이렇게 하면 설정된 출입시간에 걸쳐 한 구역에 입장할 수 있는 최대 횟수를 제한할 수 있습니다. timed anti-passback 기능을 강화하기 위하여 시간 제한을 설정할 수도 있습니다. 인증 제한 구역 설정에 관한 자세한 내용은 5.3.2 를 참조하십시오.
- **경보 구역:** 여러 장치를 묶어서 하나의 경보 구역을 구성하려면 이 구역을 사용합니다. 경보 발동 카드나 경보 해제 카드를 사용하면 경보 구역 안에 있는 장치의 경보를 발동하거나 해제할 수 있습니다. 경보 구역 설정에 관한 자세한 내용은 3.5.2.4 와 3.5.2.5 와 3.5.2.6 과 5.3.3 을 참조하십시오.
- **화재 경보 구역:** 화재가 발생했을 때 출입문이 어떻게 작동할지 미리 정하려면 화재 경보 구역을 사용합니다. 외부 신호가 BioStar 시스템에 전달되면 BioStar 는 자동으로 출입문을 여는 등의 행동을 취합니다. 화재 경보 구역 설정에 관한 자세한 내용은 5.3.4 를 참조하십시오.
- **소집 구역:** 비상시 사용자들을 감시하고 사용자들의 위치를 추적하기 위하여 소집 구역을 사용합니다. 또한 사용자들이 특정 시간에 특정 장소에 모이는 롤 콜(Roll Call)을 시행할 때 소집

3. BioStar 설정하기

구역을 사용합니다. 관리자는 모든 사용자들이 소집 구역에 모여 있는지를 확인하고 행방을 알 수 없는 사용자가 있을 경우 필요한 조치를 취할 수 있습니다. 소집 구역에 관한 자세한 내용은 5.3.6 을 참조하십시오.

- **Interlock 구역:** 장치가 연결된 두 출입문으로 Interlock 구역을 설정할 수 있습니다. 외부 입력이 한쪽 출입문이 열렸다는 신호를 보내면 보안을 위해 다른 한쪽 출입문이 자동으로 닫힙니다. 다른 구역에 속하지 않은, 장치가 장착된 출입문은 최대 4 개의 Interlock 구역에 포함될 수 있습니다(각 장치는 최대 4 개의 구역에 포함 가능). Interlock 구역 설정에 관한 자세한 내용은 5.3.7 을 참조하십시오.

3.5.2 구역을 추가하고 설정하기

구역을 추가하면, 구역 창에서 4 개의 탭을 사용하여 각 구역을 설정할 수 있습니다. 구역 설정에 관한 자세한 설명을 보려면 5.3 를 참조하십시오.

- **추가정보:** 장치를 추가하거나 입력과 설정값을 변경합니다.
- **알람:** 경보 동작과 출력을 설정합니다.
- **출입통제그룹:** 출입그룹을 구역에 적용합니다(화재 경보 구역에서는 사용할 수 없습니다).
- **이벤트:** 구역과 관련된 이벤트를 볼 수 있습니다.

3.5.2.1 구역 추가하기

새로운 구역 추가하기

1. 단축 메뉴 창에서 **출입문**을 클릭합니다.
2. 탐색 창에서 **구역**을 마우스 오른쪽 버튼으로 클릭합니다.
3. **구역 추가**를 클릭합니다.
4. 이름 필드에 구역의 이름을 입력합니다.
5. 종류 목록 상자에서 구역의 종류를 선택합니다(구역에 관한 설명은 3.5.1 을 참조).
6. **확인**을 클릭합니다. 구역 창이 나타납니다.

3.5.2.2 구역에 장치 추가하기

구역에 규칙을 적용하려면 먼저 구역에 장치를 포함시켜야 합니다. 구역 창의 추가정보 탭에서 장치 목록을 보면 각 구역에 연결된 장치들을 확인할 수 있습니다.

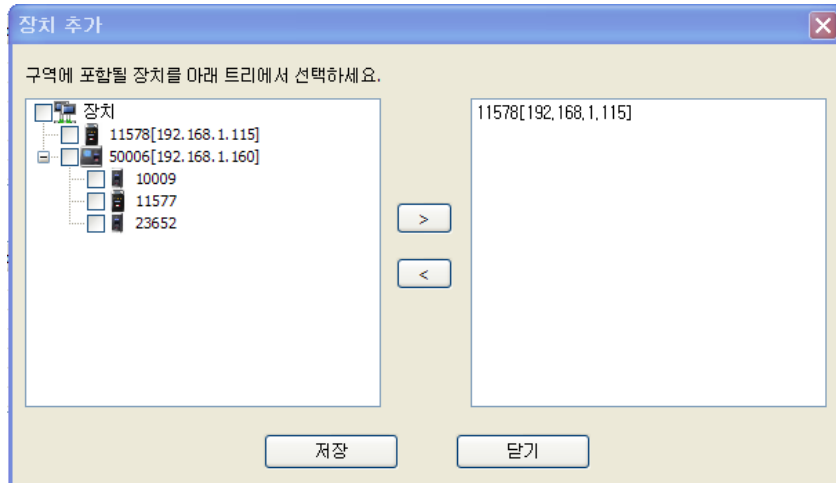
장치 목록			
No	장치	속성	경비 개시/해제 방식
1	40051[61.83.152.174]	마스터 장치	

주의: BioStation A2, BioStation 2, BioStation L2, BioEntry W2 는 이중출입 방지 구역, 화재 경보 구역으로만 구성할 수 있습니다.

3. BioStar 설정하기

구역에 장치 추가하기

1. 단축 메뉴 창에서 **출입문**을 클릭합니다.
2. 탐색 창에서 구역의 이름을 클릭합니다.
3. 구역 탭의 장치 목록 아래에 있는 **장치 추가**를 클릭합니다. 장치 추가 대화 상자가 나타납니다.



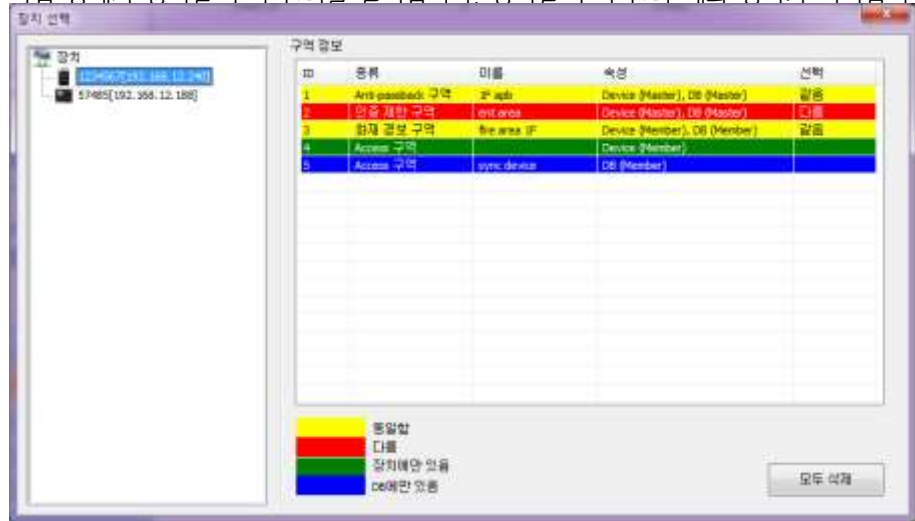
4. 목록에서 장치를 선택한 후 >을 클릭합니다.
 - **이중출입 방지 구역**을 선택한 경우: 구역 속성 선택 대화 상자가 나타나면 아래 화살표를 클릭하여 목록에서 **입실용** 또는 **퇴실용**을 선택합니다.
 - **경보 구역**을 선택한 경우: 구역 속성 선택 대화 상자가 나타나면 Device 속성 목록 상자에서 장치의 속성(**일반**, **경비 개시**, **경비 해제**, **경비 개시/해제**)을 선택합니다. **경비 개시**나 **경비 해제**를 선택했다면, 경보 기능을 시작하거나 해제할 방법으로 **경비 카드**나 **Key 설정** 둘 중 하나를 선택한 후 **확인**을 클릭합니다. 구역에서 경보 기능을 실행하거나 해제하는 방법에 관한 자세한 내용은 3.5.2.5 를 참조하십시오.
 - **출입 구역**을 선택한 경우: 구역 속성 선택 대화 상자가 나타나면 장치의 종류(**마스터 장치**, **일반 장치**)를 선택한 후 **다음**을 클릭합니다.
5. **저장**을 클릭하여 장치를 목록에 추가합니다.

장치에 설정된 구역 확인하기

1. 단축 메뉴 창에서 **출입문**을 클릭합니다.

3. BioStar 설정하기

- 작업 창에서 장치별 구역 관리를 클릭합니다. 장치별 구역 관리 대화 상자가 나타납니다.



- 왼편의 장치 목록에서 장치의 이름을 클릭하여 장치가 가지고 있는 구역 정보를 표시합니다.
 - 노란색: 장치와 서버에 설정된 정보가 동일.
 - 빨간색: 장치와 서버에 설정된 정보가 다름.
 - 초록색: 설정된 정보가 장치에만 적용되어 있음.
 - 파란색: 설정된 정보가 서버에만 있음.
- 선택 사항: 장치에 설정된 구역을 한 번에 삭제하려면 모두 삭제를 클릭합니다.

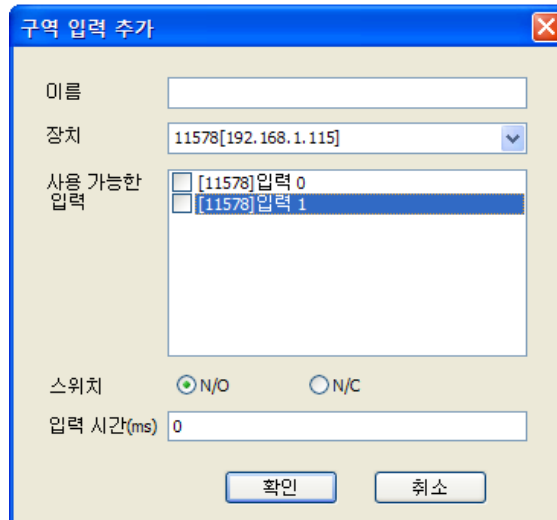
3.5.2.3 구역의 입력 설정하기

경보 구역이나 화재 경고 구역에 장치를 추가할 때에는 구역의 입력을 설정해야 합니다.

구역의 입력 설정하기

- 단축 메뉴 창에서 **출입문**을 클릭합니다.
- 탐색 창에서 구역의 이름을 클릭합니다.
- 추가정보 탭의 장치 목록 아래에 있는 **입력 추가**를 클릭합니다. 구역 입력 추가 대화 상자가 나타납니다.

3. BioStar 설정하기



4. 이름 상자에 입력의 이름을 입력합니다.
5. 장치 목록 상자에서 장치를 선택합니다.
6. 사용 가능한 입력 목록에서 하나를 선택합니다.
7. 입력의 기본 상태(**N/O**: 평상시 열림, **N/C**: 평상시 닫힘)를 선택합니다.
8. 입력 신호의 지연 시간(1000 분의 1 초 단위)을 입력합니다.
9. **확인**을 클릭하여 입력 목록에 입력을 추가합니다.

3.5.2.4 경보 동작과 출력 설정하기

경보 동작을 설정하여 어떤 경보를 받아들일지 설정합니다. 만약, 경보 동작을 설정한다면 어떤 포트와 릴레이를 이용하여 경보 출력을 사용할지 선택해야 합니다. 구역 창에 있는 알람 탭에서 출입 구역을 제외한 모든 구역에 대한 옵션을 설정할 수 있습니다. 경보 기능에 관한 자세한 내용은 3.5.2.5 와 3.10 을 참조하십시오.

- **PC 사운드**: PC(호스트 컴퓨터 또는 BioStar 서버)에서 소리가 발생하도록 설정합니다. 임의의 소리를 추가하는 방법에 관해서는 3.10.1.2 를 참조하십시오.
- **장치 사운드**: 개별 장치가 소리를 발생하도록 설정합니다.
- **Email 전송**: 경보가 동작할 때 입력된 수신자에게 이메일로 통보하도록 설정합니다. 이메일 통지에 관한 자세한 내용은 3.10.2 를 참조하십시오.
- **Output 장치**: 경보 사이렌과 같은 슬레이브 장치에 경보 신호를 전송할 장치를 선택합니다.
- **Output 포트**: 출력 신호에 사용할 포트를 설정합니다.
- **Output 신호파형**: 출력 신호의 종류를 설정합니다.

3.5.2.5 경비 개시와 경비 해제 설정하기

경보 구역을 추가한 다음에 해당 구역에 경비 기능을 적용할지 또는 해제할지 설정할 수 있습니다.

주의: BioStation A2, BioStation 2, BioStation L2, BioEntry W2 로 구성된 출입문/구역은 경비 개시와 경비 해제를 설정할 수 없습니다.

3. BioStar 설정하기

경비 개시 또는 해제하기

1. 단축 메뉴 창에서 **출입문**을 클릭합니다.
2. 탐색 창에서 경비 구역의 이름을 클릭합니다.
3. 구역 창에서 추가정보 탭을 클릭합니다.
4. **경비 개시/해제 종류** 옆에 있는 **설정**을 클릭합니다. 경비 개시/해제 설정 대화 상자가 나타납니다.

5. 구역에 경비를 개시하거나 해제할 카드를 설정하려면 다음의 절차를 따릅니다.
 - a. 장치 ID 목록 상자에서 장치를 선택합니다.
 - b. 카드 읽기를 클릭합니다. 선택한 장치의 LED가 깜빡이기 시작합니다.
 - c. 카드를 장치에 댁니다.
 - d. 장치가 카드 읽기를 완료하면 **추가**를 클릭합니다. 이 카드로 경비 구역 내에 있는 장치들의 경비 기능을 개시하거나 해제할 수 있습니다.

참고: BioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, X-Station 에서 지원합니다.

6. 구역에 경비를 적용하거나 해제하기 위한 키를 설정하려면 다음의 절차를 따릅니다.
 - a. 경비 개시 목록 상자에서 장치의 경비 기능을 개시할 때 사용할 키를 선택합니다.
 - b. 경비 해제 목록 상자에서 경비 기능을 해제할 때 사용할 키를 선택합니다.

참고: BioStation, X-Station 에서 지원합니다. BioLite Net 에서 경비 개시는 “<” 1 번이며 경비 해제는 “>” 1 번으로 키가 고정되어 있습니다. 경비 개시와 경비 해제가 동일한 키로 중복 설정되면 동작 오류가 발생합니다.

7. 경비 개시/해제 설정을 모두 마친 후 **확인**을 클릭합니다.

3. BioStar 설정하기

3.5.2.6 외부 I/O 연동 설정하기

경보 구역의 경비를 수동으로 개시하거나 해제하지 않고, 지정된 입력의 상태에 따라 BioStar 시스템이 자동으로 경보 구역의 경비를 개시하거나 해제하도록 설정할 수 있습니다. 또한 다른 입력을 지정하여 입력의 상태에 따라 자동 경비가 개시되지 않도록 설정할 수 있습니다. 뿐만 아니라 BioStar 시스템이 경비를 개시하거나 해제할 때 지정된 외부 출력(예를 들어, 외부 사이렌 등)으로 설정된 신호를 보내도록 설정할 수 있습니다. 외부 I/O 설정은 BioStationV1.8, BioEntry PlusV1.4, BioEntry W V1.0, BioLite NetV1.2, Xpass 및 Xpass S2 V1.0, X-StationV1.0, BioStation T2 및 FaceStation V1.0 또는 그 이상에서 사용할 수 있습니다.

외부 I/O 연동 설정하기

1. 단축 메뉴 창에서 **출입문**을 클릭합니다.
2. 탐색 창에서 경보 구역의 이름을 클릭합니다.
3. 구역 창에서 추가정보 탭을 클릭합니다.
4. **외부 I/O 연동** 옆에 있는 **설정**을 클릭합니다. 외부 I/O 연동 설정 대화 상자가 나타납니다.



5. BioStar 시스템이 자동으로 경비를 개시하기 전에 점검할 입력을 설정하려면 다음의 절차를 따릅니다.
 - a. 경비 불가 상태 입력 영역에서, 장치 목록 상자에서 장치를 선택합니다.
 - b. 포트 목록 상자에서 입력을 선택합니다.
 - c. 스위치 목록 상자에서 경비를 개시하는 입력의 상태(N/O: 평상시 열림 또는 N/C: 평상시 닫힘)를 선택합니다.
6. BioStar 시스템이 자동으로 경보 구역의 경비를 개시하거나 해제하도록 설정하려면 다음의 절차를 따릅니다.
 - a. 경비 개시/해제 입력 영역에서, 장치 목록 상자에서 장치를 선택합니다.
 - b. 포트 목록 상자에서 입력을 선택합니다.
 - c. 스위치 목록 상자에서 BioStar 시스템이 자동으로 경비를 개시하는 입력의 상태(N/O: 평상시 열림 또는 N/C: 평상시 닫힘)를 선택합니다. 선택하지 않은 다른 입력 상태의 경우는 BioStar 시스템이 경비를 해제합니다.

3. BioStar 설정하기

7. 경비가 개시될 때 외부 장치에 신호를 보내려면 다음의 절차를 따릅니다.
 - a. 경비 개시 출력 영역에서, 장치 목록 상자에서 장치를 선택합니다.
 - b. 릴레이목록 상자에서 신호를 보낼 릴레이를 선택합니다.
 - c. Output 신호파형 목록 상자에서 신호 파형을 선택합니다.
 - d. 우선순위 상자에 우선순위를 입력합니다.
8. 경비가 해제될 때 외부 장치에 신호를 보내려면 다음의 절차를 따릅니다.
 - a. 경비 해제 출력 영역에서, 장치 목록 상자 장치를 선택합니다.
 - b. 릴레이 목록 상자에서 신호를 보낼 릴레이를 선택합니다.
 - c. Output 신호파형 목록 상자에서 신호 파형을 선택합니다.
 - d. 우선순위 상자에 우선순위를 입력합니다.
9. **확인**을 클릭합니다.

3.5.2.7 출입통제 그룹 선택하기

구역 창의 출입통제그룹 탭에서 구역에 설정된 일반적인 제한 사항을 모두 무시할 수 있도록 출입통제그룹을 설정할 수 있습니다. 예를 들어, 특정 출입그룹을 선택하여 이중출입 방지 구역을 제한없이 출입할 수 있도록 설정할 수 있습니다. 경보 구역의 출입통제그룹 탭에서는 경보를 개시하거나 멈출 수 있는 출입그룹을 설정할 수 있습니다. 출입그룹을 선택하려면, 그룹 이름의 앞에 있는 체크 상자를 선택한 후 **적용**을 클릭합니다.

3.5.2.8 구역 이벤트 보기

구역 창의 이벤트 탭에서 구역의 이벤트 기록을 볼 수 있습니다. 달력에서 기간을 설정한 후 **로그확인**을 클릭하여 이벤트 기록을 확인할 수 있습니다. 이벤트 기록 감시와 이벤트 기록 보기에 관한 자세한 정보는 4.1 을 참조하십시오.

3.6 사용자 설정하기

사용자의 지문을 입력하려면 지문 스캐너가 필요합니다. 그렇기 때문에 인사 부서나 보안 부서와 같은 등록 센터에 지문 등록 장치를 설치하면 유용합니다. BioStation, BioEntry Plus, BioEntry W, BioLite Net 이 BioStar 에 연결되어 있다면 이 장치들을 지문 스캐너로 활용할 수 있습니다. 또는 BioMini 지문 스캐너를 이용하면 편리하게 지문을 등록할 수 있습니다.

사용자를 추가할 때는 먼저 사용자 계정을 만들어야 합니다. 사용자 계정을 만든 후, 지문과 출입 카드를 등록하고 필요에 따라 사용자의 상세 정보를 입력합니다.

3.6.1 사용자 계정 만들기

사용자 데이터는 사용자 계정을 통해서 관리합니다. 새로운 사용자 계정을 만들 수도 있고, 장치에서 사용자 데이터를 가져올 수도 있습니다. 장치에서 사용자 데이터를 가져오는 방법에 관해서는 3.6.5.3 을 참조하십시오. 기존의 BioAdmin 데이터베이스에서 사용자 데이터를 옮기는 방법에 관해서는 2.7 를 참조하십시오.

새로운 부서 추가하기

1. 단축 메뉴 창에서 **사용자**를 클릭합니다.

3. BioStar 설정하기

2. 탐색 창에서 부서 최상위 단계인 사용자를 마우스 오른쪽 버튼으로 클릭한 후 부서 추가를 클릭합니다. 새 부서가 추가됩니다.
3. 부서 이름을 입력합니다.

참고: 부서는 최대 4 개의 단계까지 추가할 수 있습니다.

새로운 사용자 계정 추가하기

1. 단축 메뉴 창에서 **사용자**를 클릭합니다.
2. 탐색 창에서 **사용자** 또는 부서의 이름을 마우스 오른쪽 버튼으로 클릭한 후 **사용자 추가**를 클릭합니다. 사용자 창이 나타납니다.

The screenshot shows the '사용자' (User) configuration window. The '기본정보' (Basic Information) tab is active, displaying fields for Name (이름: 나영진), Department (부서: 영업부), Phone Number (전화번호), E-Mail, Password (비밀번호), and User Level (사용자 등급: 일반). Below this is the '추가정보' (Additional Information) section, which includes fields for ID, Start Date (시작일: 2000-01-01), End Date (만료일시: 2030-12-31), Authentication Mode (개인별 인증 모드: 장치설정을 따름), Job Title (직급: 부장), Handphone Number (핸드폰번호: 010-1111-1111), Gender (성별: 남자), and Birth Date (생일: 1990-09-14). Buttons for '추가' (Add), '삭제' (Delete), and '적용' (Apply) are located at the bottom right of the window.

3. 사용자 창에 사용자의 상세 정보를 입력합니다.
 - **이름:** 사용자의 이름을 입력합니다.
 - **부서:** 부서 이름을 직접 입력하거나 또는 줄임표(...) 버튼을 클릭하여 BioStar 시스템에 추가된 부서 중에서 선택합니다.
 - **전화번호:** 사용자의 전화번호를 입력합니다(숫자만 입력할 수 있습니다).
 - **E-mail:** 사용자의 이메일 주소를 입력합니다.
 - **비밀번호:** 필요하다면, 사용자의 비밀번호를 입력합니다.
 - **사용자 등급:** 사용자의 등급(**일반** 또는 **관리자**)을 선택합니다.
 - **ID:** 사용자에게 부여할 식별 번호를 입력합니다.
 - **시작일:** BioStar 시스템으로부터 인증을 받을 수 있는 시작 날짜를 입력합니다.
 - **만료일시:** 사용자 계정이 만료되는 날짜를 입력합니다(계정이 만료되는 시간까지 입력할 수 있습니다).

3. BioStar 설정하기

- 직급, 핸드폰번호, 성별, 생일은 사용자 정의항목입니다. 수정, 추가 및 삭제는 사용자 정의 항목 대화 상자에서 설정합니다. 사용자 정의 항목에 관한 자세한 내용은 4.5.3 을 참조하십시오.

참고: 사진 및 개인인증화면 편집을 클릭하면 사용자의 사진을 추가할 수 있습니다.

4. 지문(3.6.2 참조)과 얼굴 이미지(3.6.3)를 등록하고 필요에 따라 출입 카드를 등록(3.6.4 참조)합니다.
5. 적용을 클릭합니다.

3.6.2 지문 등록하기

BioStar 는 지문 정보를 암호화할 수 있는 옵션을 제공합니다. 만약 이 옵션을 사용할 계획이라면, 지문을 스캔하기 전에 암호화 옵션을 설정해야 합니다. 암호화를 실행하면 이전에 입력한 모든 지문 정보는 사용할 수 없게 됩니다. 지문 정보 암호화에 관한 자세한 내용은 4.8 을 참조하십시오.

지문을 등록할 때에는 높은 품질의 지문을 입력하는 것이 무엇보다 중요합니다. 지문을 등록하기에 앞서 등록자의 지문이 깨끗하고 물기가 없는지 확인하십시오. 필요하다면 지문 등록자에게 지문을 한번 청소하도록 요청하십시오. 그리고 지문이 너무 건조하다면 손가락에 입김을 불도록 요청하십시오. 지문을 등록할 때는 다음 사항에 유의하십시오.

- 같은 손가락의 지문을 반드시 두 번(즉, 같은 손가락에 대한 지문 정보가 2 개가 되도록) 입력해야 합니다. 한 사용자는 두 개의 손가락(4 개의 지문 정보)을 등록할 수 있습니다.
- 상처가 있거나 지문이 희미한 손가락을 등록하지 마십시오.
- 지문의 인증률이 낮으면 그 지문 정보를 삭제하고 새로운 지문을 등록하는 것이 좋습니다.

3.6.2.1 지문 스캔하기

좋은 품질의 지문 정보를 얻으려면, 등록자는 되도록 자신의 지문이 센서를 모두 덮을 수 있도록 해야 합니다. 센서에 편하게 놓을 수 있는 손가락을 사용하는 것이 좋으므로, 검지나 중지 지문을 등록할 것을 권장합니다. 센서의 표면을 지문으로 덮는다는 생각으로 센서에 손가락을 대야 올바르게 지문을 등록할 수 있습니다. 아래의 그림에서 올바른 방법과 잘못된 방법을 확인할 수 있습니다.



BioMini 에서의 지문 등록

- BioMini 장치를 사용하여 지문을 등록하는 경우, 지문 이미지가 애니메이션으로 실시간으로 보여지며, Enrollment Threshold 를 지원합니다.

주의: 슬레이브 연결된 2.x 장치로 지문을 등록할 수 없습니다.

3. BioStar 설정하기

3.6.2.2 지문 등록하기

한 사용자마다 10 개의 지문을 BioStar 에 등록할 수 있습니다. 그러나 일부 장치는 제한된 개수의 지문만 저장할 수 있습니다. 각 장치마다 저장할 수 있는 지문의 개수는 다음과 같습니다.

장치	저장 가능한 지문 개수
BioEntry Plus	2
BioEntry W	
BioLite Net	5
BioStation	
BioStation T2	
BioStation A2	10
BioStation 2	
BioStation L2	
BioEntry W2	

저장 개수가 제한된 장치들은 첫 번째 지문부터 순서대로 최대 저장 개수만큼 저장합니다.

필요하다면, 하나의 지문을 협박 알림으로 등록할 수 있습니다. 누군가에게 협박을 당해 강제로 출입문을 열어야 하는 경우, 이 지문으로 인증을 하면 경보 신호를 보낼 수 있습니다. 협박 알림 지문을 등록할 때는 다음 사항에 유의하십시오.

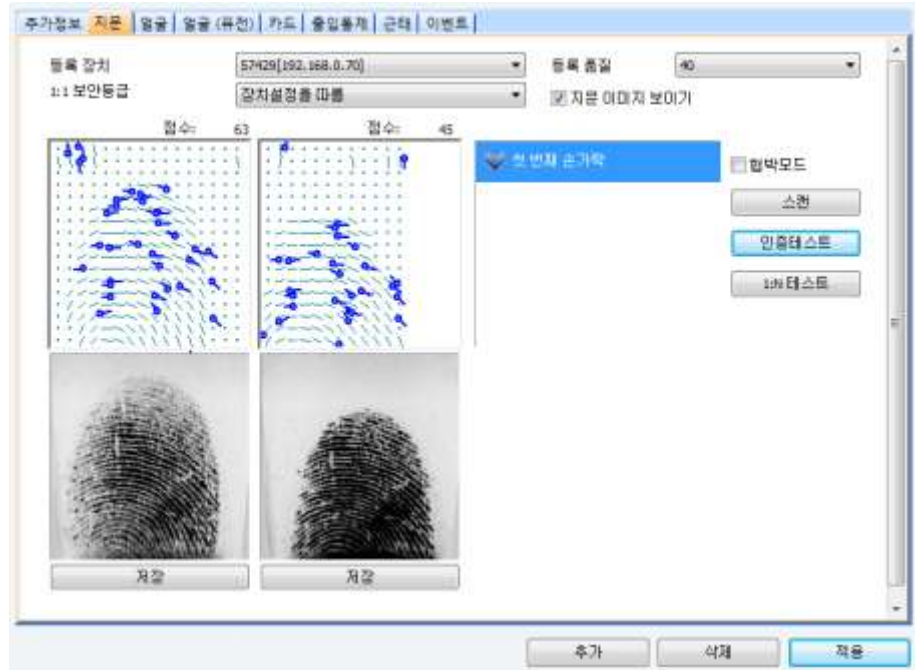
- 일상적으로 출입할 때는 협박 알림 지문을 사용해서는 안됩니다.
- 자연스럽게 사용할 수 있는 손가락을 협박 알림 지문으로 등록해야 합니다. 새끼 손가락으로 인증을 시도한다면 범인이 경보 알림에 대해 알아차릴 가능성이 있습니다.
- 협박 알림 지문으로 인증할 때 어떠한 상황이 발생하는지 잘 알고 있어야 합니다. 예를 들어, 협박 알림 지문으로 인증을 하면 자동적으로 문이 닫히거나 무소음 경보 알림이 발생할 수 있습니다.

지문 등록하기

1. 단축 메뉴 창에서 **사용자**를 클릭합니다.
2. 탐색 창에서 사용자의 이름을 클릭합니다.
3. 사용자 창에서 **지문** 탭을 클릭합니다.
4. 등록 장치 목록 상자에서 지문을 등록할 장치를 선택합니다.
5. 1:1 보안등급 목록 상자에서 보안 등급을 선택합니다.
6. 필요에 따라 상세 옵션을 설정합니다.
 - **등록 품질:** 지문 인증의 정확도를 높이기 위해 지문의 품질 수준을 지정할 수 있습니다. 지문의 품질은 지문의 특징점과 분포 정도를 비롯한 여러 개 데이터를 기준으로 산정되며, 4 개 값(20, 40, 60, 80) 중에서 선택할 수 있습니다. 숫자가 클수록 요구되는 지문 정보의 품질이 높고, 품질 수준에 못 미치는 지문이 입력되면, 지문 정보가 등록되지 않습니다. 이 옵션은 BioStar 표준 버전에서만 사용할 수 있습니다.

3. BioStar 설정하기

- **지문 이미지 보기:** 지문 스캔 시 지문 이미지가 화면에 표시되고, 개별 지문 이미지를 로컬 PC 에 저장할 수 있습니다. 지문 이미지는 BioStar 서버의 데이터베이스에 저장되지 않습니다.
7. 사용자 창의 오른쪽 아래에 있는 **추가**를 클릭합니다. 지문을 등록할 빈 공간이 생성됩니다.
 8. 비어 있는 지문 영역에서 **스캔**을 클릭한 후, 프로그램의 지시에 따라 손가락을 두 번 스캔합니다.



9. 나머지 지문을 등록하려면 6~8 단계를 반복합니다.
10. 오른쪽 아래 **적용**을 클릭하여 지문 정보를 저장합니다.
11. 입력된 지문 정보가 유효한지 검증합니다. 두 가지 검증 옵션이 있습니다.
 - **인증테스트:** 장치에 저장된 지문 정보와 사용자가 입력한 지문 정보가 일치하는지 확인합니다.
 - **1:N 테스트:** 서버에 저장된 지문 정보와 사용자가 입력한 지문 정보가 일치하는지 확인합니다.

3.6.2.3 커맨드 카드를 이용하여 사용자 등록하기

커맨드 카드를 가지고 있다면 BioEntry Plus, BioEntry W 및 Xpass 에서 직접 사용자를 등록할 수 있습니다. 커맨드 카드 발급에 관한 자세한 내용은 3.2.6.1 과 3.2.8.1 을 참조하십시오.

BioEntry Plus, BioEntry W 에서 사용자 등록하기

1. BioEntry Plus 또는 BioEntry W 장치에 등록 카드(커맨드 카드)를 가까이 가져갑니다. 인증이 필요하다면, 관리자가 자신의 지문으로 인증해야 계속 진행할 수 있습니다.
2. 지문만 등록하려면, 장치의 지시에 따라 사용자가 자신의 지문을 센서 위에 두 번 대도록 요청하십시오.
3. 지문을 등록하고 출입 카드를 발급하려면, 먼저 카드를 장치에 댁니다. 그 후 장치의 지시에 따라 사용자가 자신의 지문을 센서 위에 두 번 대도록 요청합니다.

3. BioStar 설정하기

Xpass 에서 사용자 등록하기

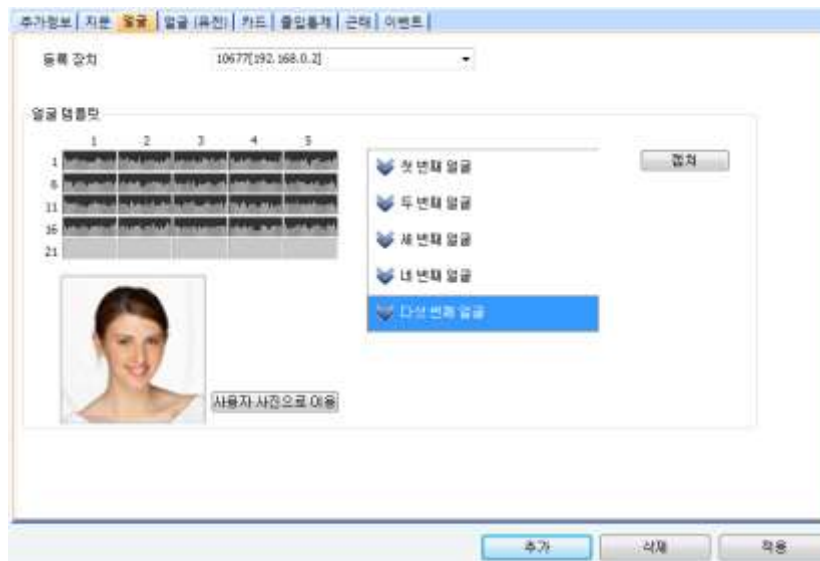
1. Xpass 에 등록 카드(커맨드 카드)를 가까이 가져갑니다.
2. 인증이 필요하면, 관리자가 자신의 카드로 인증해야 계속 진행할 수 있습니다.
3. 등록할 사용자의 출입 카드를 장치에 가까이 가져갑니다.
4. Xpass 에 커맨드 카드를 다시 가까이 가져갑니다.

3.6.3 얼굴 이미지 캡처하기

카메라가 내장된 장치(FaceStation)로 사용자의 얼굴 이미지를 캡처하여 저장하면 BioStar 의 얼굴 검출 기술을 활용하여 사용자를 인증할 수 있습니다. 얼굴 검출은 지문 인식과 함께 보다 엄격한 출입 통제를 실행하려 할 때 사용할 수 있습니다. 얼굴 검출 설정에 관한 자세한 내용은 5.4.3 를 참조하십시오.

FaceStation 으로 얼굴 이미지를 캡처하기

1. 단축 메뉴 창에서 **사용자**를 클릭합니다.
2. 탐색 창에서 사용자의 이름을 클릭합니다.
3. 사용자 창에서 **얼굴** 탭을 클릭합니다.



4. 등록 장치 상자에서 얼굴 이미지를 캡처할 때 사용할 장치를 선택합니다.
5. 화면 오른쪽 아래의 **추가**를 클릭하면 '첫 번째 얼굴'부터 '다섯 번째 얼굴'까지의 선택 항목이 차례로 추가됩니다.

참고: FaceStation 은 최대 5 개까지 사용자 얼굴을 저장하므로, 헤어 스타일 및 화장을 바꾸거나 다른 안경을 착용하는 등의 경우에도 정확한 얼굴 인식 기능을 제공합니다.

6. 추가된 얼굴 항목을 선택하고 **캡처**를 클릭한 후, 프로그램의 지시에 따라 얼굴의 위치를 카메라 앞에서 조정합니다. 얼굴을 추가하려면 5~6 단계를 반복하십시오.
7. **사용자 사진으로 이용**을 클릭하면 현재 선택되어 있는 캡처 이미지를 사용자 창의 프로필 사진으로 사용할 수 있습니다.

3. BioStar 설정하기

8. 적용을 클릭하여 설정을 저장합니다.

3.6.4 출입 카드 발급하기

슈프리마의 출입 제어 장치는 다음과 같이 다양한 종류의 카드를 지원합니다.

- EM4100 카드: BioStation, BioEntry Plus, BioLite Net, BioStation 2, BioStation L2, BioEntry W2
- MiFARE 카드: BioStation, BioEntry Plus, BioEntry W, BioLite Net, BioStation 2, BioStation L2, BioEntry W2
- iCLASS 카드: BioEntry Plus, BioStation 2, BioStation A2, BioEntry W2
- FeliCa 카드: BioEntry Plus, BioStation 2, BioStation A2, BioStation L2, BioEntry W2
- HID 근접식 카드: BioStation, BioEntry Plus, BioStation 2, BioStation L2, BioEntry W2

EM4100 카드와 HID 카드는 카드를 등록하기 위해 단지 카드 ID 만 필요한 반면, MiFARE 및 iCLASS 카드는 두 가지 동작 모드, 즉 1) 일련번호카드(CSN)모드와 2) 지문내장카드(Template-on-Card)모드를 지원합니다. FeliCa 카드는 CSN 모드만을 지원합니다. CSN 모드를 사용하면, EM4100 카드나 HID 카드와 마찬가지로 카드의 일련번호만 필요합니다. 지문내장카드(Template-on-Card) 모드를 사용하면, 지문 정보를 포함하여 사용자 정보를 직접 카드에 입력해야 합니다.

다음의 절차를 따라 카드를 발급하고, 발급한 카드를 사용자 계정에 추가합니다.

참고: BioStation 2, BioStation A2, BioStation L2, BioEntry W2 는 카드를 1 장만 발급하여 사용할 수 있습니다.

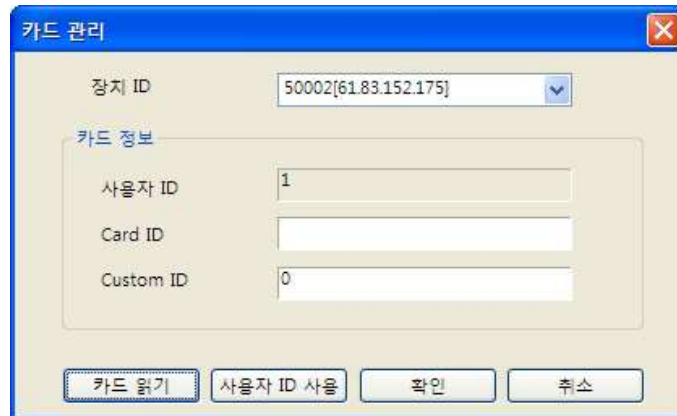
주의: 슬레이브로 연결된 2.x 장치로 카드를 발급할 수 없습니다.

3.6.4.1 EM4100 카드 발급하기

사용자 계정에 EM4100 카드 등록하기

1. 단축 메뉴 창에서 **사용자**를 클릭합니다.
2. 탐색 창에서 사용자의 이름을 클릭합니다.
3. 사용자 창에서 카드 탭을 클릭합니다.
4. 카드 종류 목록 상자에서 **EM 4100** 을 선택합니다.
5. **카드 발급/관리**를 클릭합니다. 카드 관리 대화 상자가 나타납니다.

3. BioStar 설정하기



- 장치 ID 목록 상자에서 장치를 선택합니다.
- Card ID(32 비트)와 Custom ID(8 비트)를 직접 입력하거나 **카드 읽기**를 클릭하여 카드에서 읽어 들입니다. **사용자 ID 사용**을 클릭하여 사용자 ID 를 카드 ID 로 사용할 수도 있습니다.
 - 데이터를 직접 입력하려면, Card ID 상자와 Custom ID 상자에 값을 입력한 후 **확인**을 클릭하고, 8 번으로 이동합니다.
 - 카드에서 데이터를 읽어 들이려면, **카드 읽기**를 클릭(장치의 LED 가 깜빡임)한 후 장치에 카드를 댁니다. 장치가 카드 읽기를 완료하면 **확인**을 클릭합니다.
- 적용**을 클릭하여 사용자 계정에 카드를 등록합니다.

3.6.4.2 HID 근접식 카드 발급하기

사용자의 계정에 HID 카드 등록하기

- 단축 메뉴 창에서 **사용자**를 클릭합니다.
- 탐색 창에서 사용자의 이름을 클릭합니다.
- 사용자 창에서 카드 탭을 클릭합니다.
- 카드 종류 목록 상자에서 **HID Prox** 를 선택합니다.
- 카드 발급/관리를** 클릭합니다. 카드 관리 대화 상자가 나타납니다.



- 장치 ID 목록 상자에서 장치를 선택합니다.
- Card ID**(32 비트)와 Facility Code(FC)를 직접 입력하거나 **카드 읽기**를 클릭하여 카드에서 읽어 들입니다. **사용자 ID 사용**을 클릭하여 사용자 ID 를 카드 ID 로 사용할 수도 있습니다.

3. BioStar 설정하기

- 데이터를 직접 입력하려면, Card ID 상자와 FC 상자에 값을 입력한 후 **확인**을 클릭하고, 8 단계로 건너뛵니다.
 - 카드에서 데이터를 읽어 들이려면, **카드 읽기**를 클릭(장치의 LED 가 깜빡임)한 후 장치에 카드를 댁니다. 장치가 카드 읽기를 완료하면 **확인**을 클릭합니다.
8. **적용**을 클릭하여 사용자 계정에 카드를 등록합니다.

3.6.4.3 FeliCa 카드 발급하기

사용자의 계정에 FeliCa 카드 등록하기

1. 단축 메뉴 창에서 **사용자**를 클릭합니다.
2. 탐색 창에서 사용자의 이름을 클릭합니다.
3. 사용자 창에서 카드 탭을 클릭합니다.
4. 카드 종류 목록 상자에서 **FeliCa** 를 선택합니다.
5. **카드 발급/관리**를 클릭합니다. 카드 관리 대화 상자가 나타납니다.

6. 장치 ID 목록 상자에서 장치 또는 Smart Card Reader 를 선택합니다.
7. **선택 사항:** Card ID 또는 Custom ID를 직접 입력한 후 9번 또는 10번으로 이동합니다.
8. **선택 사항:** **카드 읽기**를 클릭하여 카드에서 직접 카드 정보를 읽어 들입니다. 장치의 LED 가 깜박거리면 장치에 카드를 댁니다. 장치가 카드 읽기가 완료되면 **확인**을 클릭합니다.
9. **선택 사항:** **사용자 ID 사용**을 클릭하여 사용자 ID 를 CSN 으로 사용합니다.
10. **적용**을 클릭하여 사용자 계정에 카드를 등록합니다.

3.6.4.4 MiFARE, DESFire, iCLASS CSN 카드 발급하기

MiFARE, DESFire, iCLASS CSN 카드는 각 사용자에게 할당된 편집할 수 없는 카드 일련번호 (CSN)를 저장한다는 점에서 EM4100 카드나 HID 카드와 유사합니다.

사용자의 계정에 MiFARE, DESFire, iCLASS 카드 등록하기

1. 단축 메뉴 창에서 **사용자**를 클릭합니다.
2. 탐색 창에서 사용자의 이름을 클릭합니다.
3. 사용자 창에서 카드 탭을 클릭합니다.
4. 카드 종류 목록 상자에서 **Mifare CSN** 또는 **iCLASS CSN** 을 선택합니다.

3. BioStar 설정하기

- 카드 발급/관리를 클릭합니다. 카드 관리 대화 상자가 나타납니다.

- 장치 ID 목록 상자에서 장치 또는 Smart Card Reader 를 선택합니다.
- 선택 사항: Card ID 또는 Custom ID 를 직접 입력한 후 9번 또는 10번으로 이동합니다.
- 선택 사항: 카드 읽기를 클릭하여 카드에서 직접 카드 정보를 읽어 들입니다. 장치의 LED 가 깜박거리면 장치에 카드를 삽입합니다. 장치가 카드 읽기가 완료되면 확인을 클릭합니다.
- 선택 사항: 사용자 ID 사용을 클릭하여 사용자 ID 를 CSN 으로 사용합니다.
- 적용을 클릭하여 사용자 계정에 카드를 등록합니다.

3.6.4.5 MIFARE, DESFire, iCLASS 템플릿 카드 발급하기

MIFARE, DESFire 및 iCLASS 템플릿 카드는 사용자 정보와 지문 정보를 카드에 직접 저장합니다.

주의: DESFire 템플릿 카드는 2.x 장치에서만 발급할 수 있습니다.

사용자의 계정에 카드 등록하기

- 단축 메뉴 창에서 **사용자**를 클릭합니다.
- 탐색 창에서 사용자의 이름을 클릭합니다.
- 사용자 창에서 카드 탭을 클릭합니다.
- 카드 종류 목록 상자에서 **Mifare/DESFire Template** 또는 **iCLASS Template** 을 선택합니다.
- 카드 발급/관리를 클릭합니다. 카드 관리 대화 상자가 나타납니다.

3. BioStar 설정하기



6. 장치 ID 목록 상자에서 장치 또는 Smart Card Reader 를 선택합니다.
7. 필요하다면, **항시 통과 카드**를 클릭하여 인증 절차를 거치지 않도록 설정할 수 있습니다.
8. **카드 읽기**를 클릭합니다. 선택한 장치의 LED 가 깜빡이기 시작합니다.
9. 카드를 장치에 겁니다.
10. 장치가 카드 읽기를 완료하면 **확인**을 클릭합니다.
11. **적용**을 클릭하여 사용자 계정에 카드를 등록합니다.

참고: iCLASS 2000, 2002, 2004 카드는 템플릿 카드로 사용될 수 없습니다.

3.6.4.6 MiFARE, DESFire, iCLASS 사이트 키 변경하기

MIFAR, DESFire, iCLASS 카드의 데이터 암호화는 48 비트의 사이트 키를 통해 이루어집니다. 장치는 적절한 사이트 키를 가지고 있는 카드만 읽어 들일 수 있습니다. BioStar 에서는 총 2 개의 MIFARE, DESFire, iCLASS 사이트 키(주 사이트 키와 보조 사이트 키)를 정의할 수 있기 때문에, 기존의 카드에 설정된 사이트 키를 변경할 수 있습니다.

참고: 사이트 키의 변경은 템플릿 온 카드에서만 지원되며, 사이트 키의 보안은 철저히 유지되어야 합니다. 사이트 키가 노출되면 보안 시스템의 위험 요인이 됩니다.

주의: 사이트 키는 반드시 숫자를 사용하십시오.

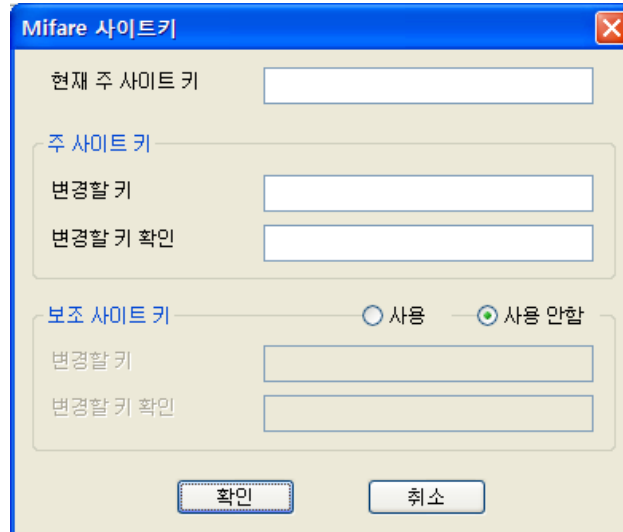
주의: DESFire 사이트 키는 2.x 장치에만 적용됩니다.

사이트 키 변경하기

1. 메뉴 표시줄에서 **옵션 > 카드 > Mifare 카드 > Mifare 사이트키** 또는 **옵션 > 카드 > iCLASS 카드 > iCLASS 사이트키** 또는 **옵션 > 카드 > DESFire 카드 > DESFire**

3. BioStar 설정하기

사이트키를 클릭합니다. Mifare 사이트키 또는 iCLASS 사이트키 또는 DESFire 사이트키 대화 상자가 나타납니다.



Mifare 사이트키 대화 상자의 스크린샷입니다. 상단에는 '현재 주 사이트 키' 필드가 있습니다. 그 아래는 '주 사이트 키' 섹션으로, '변경할 키'와 '변경할 키 확인' 필드가 있습니다. 그 다음은 '보조 사이트 키' 섹션으로, '사용'과 '사용 안함' 라디오 버튼이 있으며, '사용 안함'이 선택되어 있습니다. 이 섹션에는 '변경할 키'와 '변경할 키 확인' 필드가 있습니다. 하단에는 '확인'과 '취소' 버튼이 있습니다.

2. 주 사이트 키 영역에서 변경할 키 필드에 새 사이트 키를 입력합니다.
3. 변경할 키 확인 필드에 키를 다시 입력합니다.
4. 보조 사이트 키를 사용하려면 **사용**을 클릭합니다. 이 기능을 사용하면 기존의 사이트 키를 읽어 들여 새로운 사이트 키로 덮어 씁니다.
 - a. 보조 사이트 키 영역에서 변경할 키 필드에 기존의 사이트 키를 입력합니다.
 - b. 보조 사이트 키 영역에서 변경할 키 필드에 사이트 키를 다시 입력합니다.
5. 사이트 키의 편집을 마치면, **확인**을 클릭합니다.

참고: 새 사이트 키로 덮어쓰기를 완료하였다면, 이전의 카드로 출입하는 것을 방지하기 위해 보조 사이트 키를 **사용 안함**으로 설정할 것을 권장합니다.

3.6.4.7 MiFARE 레이아웃 편집하기

사용자 정보와 지문 정보(템플릿)의 기록에 사용되는 MiFARE 카드의 레이아웃을 수정할 수 있습니다. 레이아웃을 수정하면 일련의 장치를 통하여 발급되는 모든 새로운 MiFARE 카드에 수정된 레이아웃이 적용됩니다.

MiFARE 1K 카드는 16 개의 섹터로 구성되어 있으며, 각 섹터는 4 개의 블록으로 이루어져 있습니다. 하나의 블록은 16 바이트입니다. MiFARE 4K 카드는 4 개의 블록을 가지는 32 개의 섹터와 16 개의 블록을 가지는 8 개의 섹터로 구성되어 있습니다. MiFARE 레이아웃에는 다음과 같은 제한 사항이 적용됩니다.

- 첫 번째 섹터(0~3 번 블록)는 사용이 보류된 곳으로 다른 데이터를 기록하기 위해 사용할 수 없습니다.
- 각 섹터의 마지막 블록(3 번, 7 번, 11 번 블록 등)은 사이트 키 정보를 기록하기 위한 곳입니다.
- 카드 정보 섹터(CIS)는 3 개의 연속적인 블록을 차지하며, 어느 섹터가 되었든 가장 처음 블록(4 번, 8 번, 12 번 블록 등)부터 시작합니다.
- 각 템플릿(지문 정보) 데이터가 겹치게 해서는 안됩니다.

3. BioStar 설정하기

MiFARE 레이아웃을 편집하려면 다음의 절차를 따릅니다.

1. 메뉴 표시줄에서 **옵션 > 카드 > Mifare 카드 > Mifare 레이아웃**을 클릭합니다. Mifare 레이아웃 설정 대화 상자가 나타납니다.



2. 각 상자에 값을 입력하여 MiFARE 레이아웃 옵션을 변경합니다.
 - **CIS 인덱스 블록:** 헤더 정보를 기록하는 데 사용할 블록 인덱스(4, 8, 12, 16)를 선택합니다.
 - **템플릿 수:** 레이아웃에 포함할 템플릿의 수(0~4)를 선택합니다.
 - **템플릿 크기:** 템플릿이 사용하는 바이트의 수를 선택합니다. 기본값은 334 바이트입니다.
 - **템플릿 1-4 시작 블록:** 각 템플릿이 저장될 시작 블록을 선택합니다.
3. 현재 설정된 레이아웃을 사용하려면, **장치에 적용**을 클릭한 후 장치 트리 대화 상자에서 적용할 장치를 선택한 다음, **확인**을 클릭합니다.
4. **저장**을 클릭합니다.

참고: 변경 사항을 초기값으로 설정하려면 **기본값으로 변경**을 클릭합니다. 변경 사항을 저장하지 않고 대화 상자를 닫으려면 **닫기**를 클릭합니다.

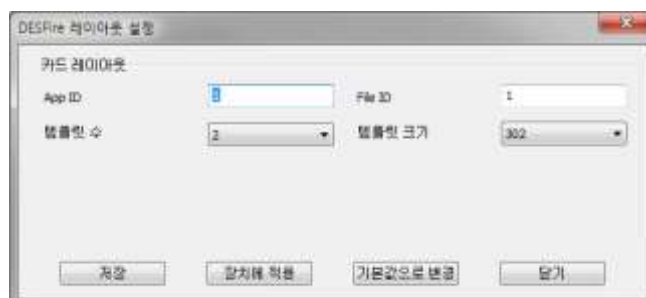
3.6.4.8 DESFire 레이아웃 편집하기

사용자 정보와 지문 정보(템플릿)의 기록에 사용되는 DESFire 카드의 레이아웃을 수정할 수 있습니다. 레이아웃을 수정하면 일련의 장치를 통하여 발급되는 모든 새로운 DESFire 카드에 수정된 레이아웃이 적용됩니다.

주의: DESFire 레이아웃은 2.x 장치에만 적용됩니다.

DESFire 레이아웃 편집하기

1. 메뉴 표시줄에서 **옵션 > 카드 > DESFire 카드 > DESFire 레이아웃**을 클릭합니다. DESFire 레이아웃 설정 대화 상자가 나타납니다.



3. BioStar 설정하기

2. 각 상자에 값을 입력하여 DESFire 레이아웃 옵션을 변경합니다.
 - **App ID:** 애플리케이션 ID를 설정합니다. File ID를 포함하는 일종의 디렉터리 역할을 합니다.
 - **File ID:** 파일 ID를 설정합니다.
 - **템플릿 수:** 레이아웃에 포함할 템플릿의 수(기본값 2)를 선택합니다.
 - **템플릿 크기:** 템플릿이 사용하는 바이트의 수(기본값 302)를 선택합니다.
3. 현재 설정된 레이아웃을 사용하려면 **장치에 적용**을 클릭한 후 장치 트리 대화 상자에서 적용할 장치를 선택한 다음, **확인**을 클릭합니다.
4. **저장**을 클릭합니다.

참고: 변경 사항을 초기값으로 설정하려면 **기본값으로 변경**을 클릭합니다. 변경 사항을 저장하지 않고 대화 상자를 닫으려면 **닫기**를 클릭합니다.

3.6.4.9 iCLASS 레이아웃 편집하기

사용자 정보와 지문 정보(템플릿)의 기록에 사용되는 iCLASS 카드의 레이아웃을 수정할 수 있습니다. 레이아웃을 수정하면 일련의 장치를 통하여 발급되는 모든 새로운 iCLASS 카드에 수정된 레이아웃이 적용됩니다.

BioEntry Plus iCLASS 는 16k 비트(2k 바이트) 및 32k 비트(4k 바이트) iCLASS 카드를 지원합니다. 16k 카드는 2 또는 16 개의 응용 영역에서 사용할 수 있으며, 8 바이트 크기의 블록 237 개로 이루어져 있습니다. 32k 카드는 2 또는 16 개의 응용 영역에서 사용할 수 있으며, 사용자가 구성할 수 있는 16k 메모리와 함께 8페이지, 8바이트 크기의 블록 26 개로 이루어져 있습니다.

iCLASS 레이아웃 편집하기

1. 메뉴 표시줄에서 **옵션 > 카드 > iCLASS 카드 > iCLASS 레이아웃**을 클릭합니다. iCLASS 레이아웃 설정 대화 상자가 나타납니다.



2. 각 상자에 값을 입력하여 iCLASS 레이아웃 옵션을 변경합니다.
 - **CIS 인덱스 블록:** 헤더 정보를 기록하는 데 사용할 블록 인덱스(기본값 13)를 선택합니다.
 - **템플릿 수:** 레이아웃에 포함할 템플릿의 수(기본값 2)를 선택합니다.
 - **템플릿 크기:** 템플릿이 사용하는 바이트의 수(기본값 382)를 선택합니다.
 - **템플릿 1-4 시작 블록:** 각 템플릿이 저장될 시작 블록을 선택합니다. (템플릿 1의 기본값은 19이며 템플릿 2의 기본값은 67입니다)
3. 현재 설정된 레이아웃을 사용하려면 **장치에 적용**을 클릭한 후 장치 트리 대화 상자에서 적용할 장치를 선택한 다음, **확인**을 클릭합니다.

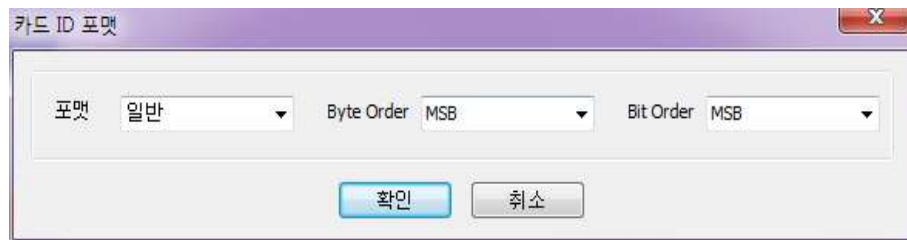
3. BioStar 설정하기

4. 저장을 클릭합니다.

참고: 변경 사항을 초기값으로 설정하려면 **기본값으로 변경**을 클릭합니다. 변경 사항을 저장하지 않고 대화 상자를 닫으려면 **닫기**를 클릭합니다.

3.6.4.10 USB 기반 리더로부터 카드 정보 읽기

DE-620 과 같은 USB 기반의 비접촉 리더로부터 정보를 읽기 위한 옵션을 설정할 수 있습니다. **옵션 > 카드 > USB 리더기 > 카드 ID 포맷**을 클릭하면, 다음과 같이 카드 ID 포맷 대화 상자가 나타납니다.



- **포맷:** 카드 ID 데이터를 일반적인 형식으로 처리합니다. Wiegand 포맷은 지원하지 않습니다.
- **Byte Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. MSB 는 큰 단위의 바이트에서 작은 단위의 바이트 순, LSB 는 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.
- **Bit Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 비트를 처리할지 선택합니다. MSB 는 최상위 비트에서 최하위 비트 순, LSB 는 최하위 비트에서 최상위 비트 순으로 처리합니다.

3.6.5 사용자 데이터 전송하기

메뉴 표시줄에서 **옵션 > 사용자 > 전송 모드 > 자동**을 클릭하여, 사용자 정보가 장치에 자동적으로 전송되도록 설정할 수 있습니다. 또한, 수동으로 장치에 데이터를 전송할 수도 있습니다. 수동으로 전송할 때에는 사용자를 선별해서 원하는 장치에만 전송할 수도 있고, 또는 모든 사용자 데이터를 동기화할 수도 있습니다. BioStar 를 이용하면 장치에서 사용자 데이터를 가져와서 그것을 다시 BioStar 서버에 전송할 수 있습니다.

3.6.5.1 사용자 정보를 장치에 전송하기

장치에 사용자 정보 전송하기

1. 단축 메뉴 창에서 **사용자**를 클릭합니다.
2. 작업 창에서 **수동 사용자 관리**를 클릭합니다. 장치 선택 관리 대화 상자가 나타납니다.

3. BioStar 설정하기



3. 왼편에서 장치 이름 앞에 있는 체크 상자를 선택하여 장치를 선택합니다.
4. 같은 사용자인데 정보가 다를 경우 덮어쓰려면, 사용자 정보가 다를 때 덮어쓰기 체크 상자를 선택합니다.
5. 선택한 장치에 사용자 정보를 전송하려면 장치로 전송을 클릭합니다.

참고: 이 메뉴를 이용하여 사용자를 장치에서 삭제할 수도 있습니다. 삭제를 실행하면 다시 되돌릴 수 없으므로 주의해서 사용해야 합니다. 사용자를 장치에서 삭제하려면, 사용자 이름을 클릭한 후 장치에서 삭제를 클릭합니다.

주의: Xpass 및 Xpass S2 에서 Lift I/O 정보는 사용자 정보에 포함되어 단말기로 전송됩니다. 리프트 리더로 사용되는 Xpass 및 Xpass S2 의 경우, 사용자 메뉴의 사용자 전송을 사용하면 Xpass 및 Xpass S2 단말기에 저장된 리프트 설정 정보가 모두 초기화됩니다. 리프트 설정을 유지하려면 사용자 메뉴의 사용자 전송 대신 리프트 메뉴의 장치에 전송을 사용하십시오.

3.6.5.2 모든 사용자 정보 동기화하기

BioStar 서버와 서버에 연결된 모든 장치의 사용자 정보를 동기화하려면 다음의 절차를 따릅니다.

1. 단축 메뉴 창에서 사용자를 클릭합니다.
2. 작업 창에서 수동 사용자 관리를 클릭합니다. 수동 사용자 관리 대화 상자가 나타납니다. (3.6.5.1 참조)
3. 왼편에서 장치 이름 앞에 있는 체크 상자를 선택하여 장치를 선택합니다.
4. 장치와 동기화를 클릭합니다.

3.6.5.3 장치에서 사용자 정보 가져오기

장치에서 사용자 정보를 가져오려면 다음의 절차를 따릅니다.

1. 단축 메뉴 창에서 사용자를 클릭합니다.
2. 작업 창에서 장치별 사용자 관리를 클릭합니다. 장치별 사용자 관리 대화 상자가 나타납니다.

3. BioStar 설정하기



3. 왼편의 장치 목록에서 장치의 이름을 클릭하여 장치가 가지고 있는 사용자의 지문 정보를 표시합니다.
4. 지문 데이터 정보 목록에서 사용자를 클릭합니다(새로 등록된 사용자는 노란색으로 표시됩니다).
5. 장치에서 가져오기를 클릭합니다.

참고: 이 메뉴를 이용하여 사용자를 장치에서 삭제할 수도 있습니다. 삭제를 실행하면 다시 되돌릴 수 없으므로 주의해서 사용해야 합니다. 사용자를 장치에서 삭제하려면, 사용자의 이름을 클릭한 후 삭제를 클릭합니다. 모든 사용자를 한번에 삭제하려면 모두 삭제를 클릭합니다.

주의: Xpass 장치에서 사용자 정보를 가져오면 동일한 ID 를 가진 사용자가 있는 경우 BioStar 데이터베이스에 있는 지문 정보가 지워집니다. 이는 Xpass 장치에 지문 정보가 저장되지 않기 때문입니다.

주의: BioStation 2, BioStation A2, BioStation L2 에 저장된 사용자 정보를 가져올 때 부서 정보와 PIN 을 가져올 수 없습니다.

3.6.5.4 장치에서 사용자 정보 병합하여 가져오기

기존 서버 DB 의 내용을 보호하면서 장치에서 변경되거나 추가된 내용만 서버에 가져오도록 하는 기능입니다. 덮어쓰기인 경우 장치에서 사용자 정보를 가져왔을 때 서버에 있는 해당 사용자 정보가 전부 지워지고 장치에서 가져온 정보만으로 다시 쓰여져 보존됩니다.

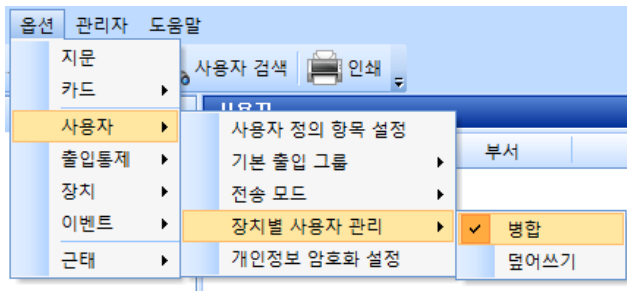
중요한 사용자 정보의 보호 차원에서 다음 5 개 항목에 대해서는 병합으로 가져오더라도 서버 DB 에 장치 데이터가 반영되지 않습니다.

- 관리자 권한 (사용자 권한이 서버 DB 에 일반이고 장치 쪽에 권한이 관리자인 경우에 한해 변경됩니다.)
- 인증 모드
- 인증 횟수
- 인증제한시간
- Password2

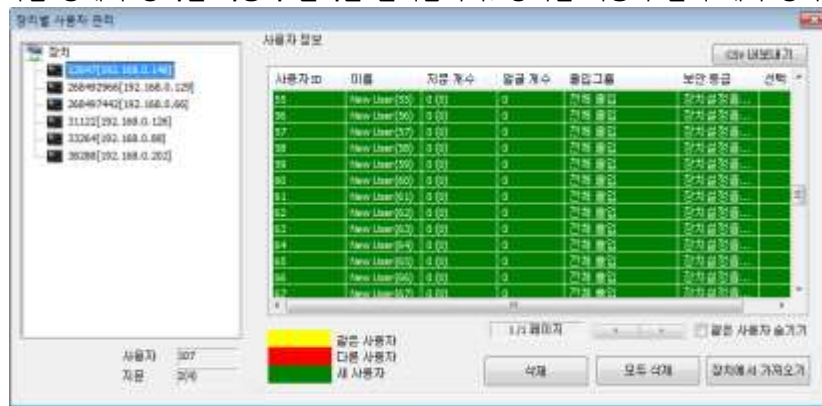
사용자 정보 병합하여 가져오기

3. BioStar 설정하기

1. **옵션 > 사용자 > 장치별 사용자 관리**를 클릭합니다. **병합**에 체크합니다. (기본값)



2. 단축 메뉴 창에서 **사용자**를 클릭합니다.
3. 작업 창에서 **장치별 사용자 관리**를 클릭합니다. 장치별 사용자 관리 대화 상자가 나타납니다.



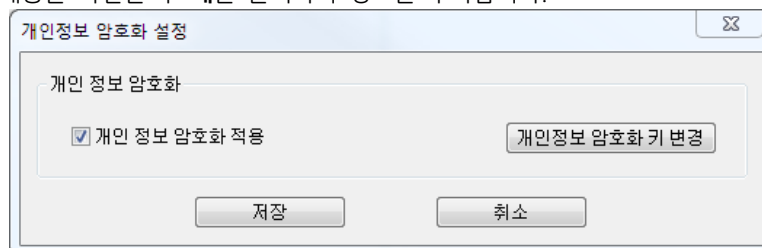
4. 왼편의 장치 목록에서 장치의 이름을 클릭하여 장치가 가지고 있는 사용자의 정보를 표시합니다.
5. 색상 정보를 통해 장치와 서버 쪽 사용자 정보를 비교하고 필요한 사용자를 선택합니다.
6. 장치에서 **가져오기**를 클릭합니다.

3.6.6 사용자 데이터 암호화하기

BioStar 는 개인 정보 보호법에 의거하여 사용자 정보에 대해 AES256 방식의 암호화를 제공합니다. 암호화를 사용하면 뜻하지 않은 사고 또는 인위적인 공격에 의해 DB 가 유출된 경우, 개인 정보를 보호하고 신분 도용 등의 범죄를 사전에 예방할 수 있습니다.

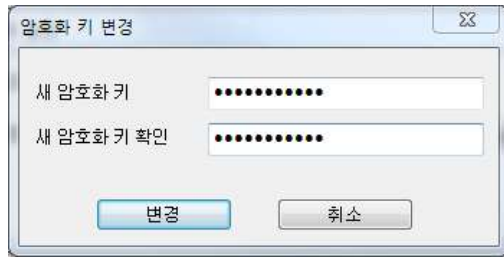
개인 정보 암호화하기

1. **옵션 > 사용자 > 개인 정보 암호화 설정**을 클릭합니다. **개인 정보 암호화 설정** 창에서 **개인 정보 암호화 적용** 체크 상자를 선택합니다. 경고 메시지가 나타납니다.
2. 내용을 확인한 후 **예**를 클릭하여 경고를 수락합니다.



3. 개인정보 암호화 키 변경을 클릭한 후 암호 입력 창에 암호를 입력합니다.

3. BioStar 설정하기



참고: 암호를 입력하지 않아도 개인정보 암호화를 사용할 수 있습니다. 암호는 0~32 자리까지 지원되며, 영문 대소문자 및 숫자, 특수 문자를 모두 사용할 수 있습니다.

4. **확인**을 클릭하여 창을 닫은 후, **저장**을 클릭하십시오. **저장**을 클릭하지 않으면 변경한 값이 적용되지 않습니다.

3. BioStar 설정하기

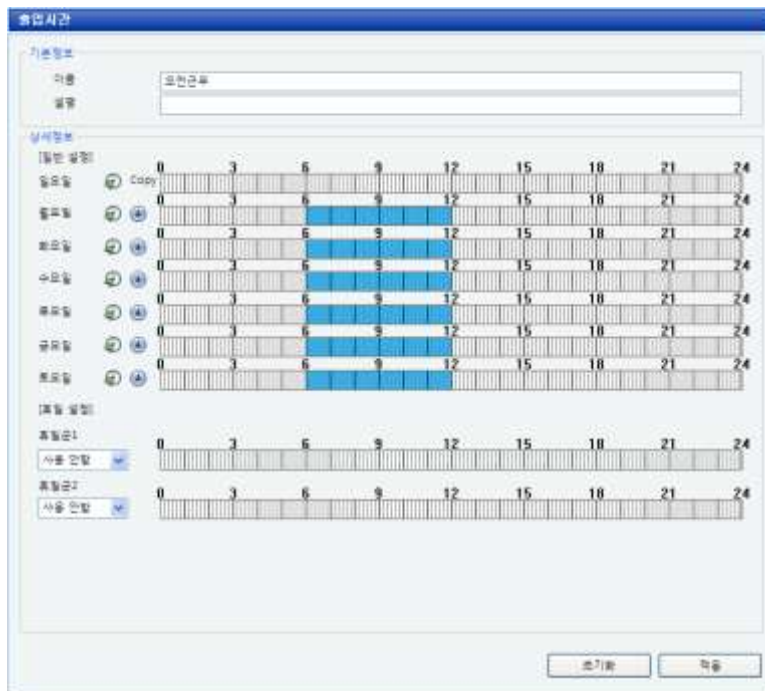
3.7 출입시간 설정하기

BioStar 시스템에서 출입 허용 시간과 출입 금지 시간을 설정하기 위하여 출입시간 기능을 사용합니다. 출입그룹에서 출입문과 출입시간을 조합(3.8 참조)하면 사용자가 허용된 시간 동안에만 허용된 출입문을 이용하여 출입할 수 있도록 설정할 수 있습니다.

3.7.1 출입시간 만들기

출입시간 생성하기

1. 단축 메뉴 창에서 **출입통제**를 클릭합니다.
2. 작업 창에서 **출입시간 추가**를 클릭합니다.
3. 출입시간의 이름을 입력합니다.



4. 출입시간 창에서 막대 그래프 위를 마우스로 드래그하여 각 요일의 출입시간을 설정합니다. 시계 모양 아이콘을 클릭하면 수동으로 출입시간을 설정 가능하며, 동근 아래 화살표를 클릭하면 위쪽 막대 그래프에 설정된 출입시간을 현재의 막대 그래프로 복사가 됩니다.
5. 필요하다면 2 개의 휴일군을 출입시간에 포함시킵니다. 휴일군을 만드는 방법은 3.7.2 를 참조하십시오.
6. **적용**을 클릭합니다.
7. 다음으로 출입시간 정보를 장치에 전송합니다.
 - a. 작업 창에서 **장치에 전송**을 클릭합니다. 장치 트리 대화 상자가 나타납니다.
 - b. 출입시간 정보를 전송할 장치를 선택합니다.
 - c. **확인**을 클릭합니다.

이제 출입시간과 출입문을 조합해서 출입그룹을 만들 수 있습니다(3.8 참조).

3. BioStar 설정하기

3.7.2 휴일군 만들기

휴일군 생성하기

1. 단축 메뉴 창에서 **출입통제**를 클릭합니다.
2. 작업 창에서 **휴일군 추가**를 클릭합니다.
3. 휴일군의 이름을 입력합니다.
4. 휴일군 창에서 휴일의 시작 날짜를 선택합니다.

날짜	반복	기간
2009-10-03	한 번	3일간

5. 매년 반복되는 휴일이라면, **매년 반복** 체크 상자를 선택합니다.
6. 휴일의 기간을 지정합니다.
7. **추가**를 클릭하여 설정한 휴일을 목록에 추가합니다.
8. **적용**을 클릭합니다.

3. BioStar 설정하기

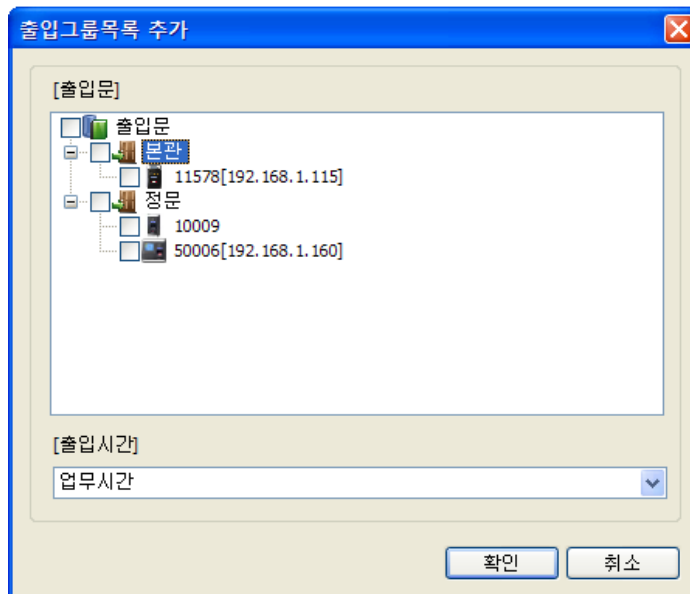
3.8 출입그룹 설정하기

출입그룹을 이용하면 출입문, 사용자, 출입시간을 연계하여 출입 권한을 설정할 수 있습니다. 출입그룹을 추가하기 전에 먼저 출입문(3.3 참조)과 출입시간(3.7 참조)을 설정해야 합니다. 출입그룹을 만든 후 이 정보를 관계된 장치에 수동으로 전송해야 합니다(3.8.4 참조).

3.8.1 출입그룹 추가하기

출입그룹 추가하기

1. 단축 메뉴 창에서 **출입통제**를 클릭합니다.
2. 작업 창에서 **출입그룹 추가**를 클릭합니다.
3. 탐색 창에 나타나는 이름 필드에서 출입그룹의 이름을 입력한 후 **추가**를 클릭합니다.
4. 출입그룹 창의 출입통제 탭에서 **추가**를 클릭합니다. 출입그룹목록 추가 대화 상자가 나타납니다.



5. 출입문 그룹이나 출입문을 클릭한 후, 출입그룹에 적용할 출입문을 선택합니다.
6. 출입시간 목록 상자에서 출입그룹에 적용할 출입시간을 선택합니다.
7. **확인**을 클릭하여 출입그룹에 선택 사항을 적용합니다.
8. 출입그룹에 여러 출입문과 출입시간을 포함시키려면 4~7 단계를 필요한 만큼 반복합니다.
9. **적용**을 클릭합니다.

3.8.2 출입그룹에 사용자 추가하기

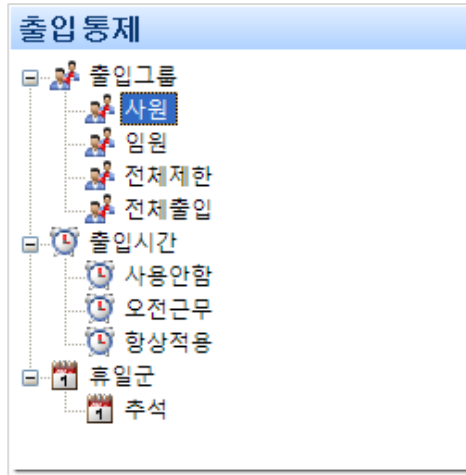
출입문과 출입시간을 출입그룹에 추가한 후 사용자를 출입그룹에 추가해야 합니다. 아래 설명에 따라 사용자 탭에서 사용자를 출입그룹에 추가하거나 또는 3.8.3 의 설명에 따라 사용자 창에서 각 사용자에게 출입그룹을 할당할 수 있습니다.

출입그룹에 사용자 추가하기

1. 단축 메뉴 창에서 **출입통제**를 클릭합니다.

3. BioStar 설정하기

2. 탐색 창에서 사용자가 포함될 출입그룹을 선택합니다.



3. 출입그룹 창의 사용자 탭을 클릭한 후, 창의 아래에 있는 추가를 클릭합니다. 새 사용자 추가 대화 상자가 나타납니다.



4. 개인이나 그룹 이름 앞에 있는 체크 상자를 선택하여 사용자를 선택합니다.
참고: 사용자 그룹을 설정했다면, 각 사용자는 그가 속한 그룹 아래에 나타납니다.
5. 확인을 클릭합니다. 선택한 사용자가 출입그룹에 포함됩니다.
6. 적용을 클릭합니다.

3.8.3 사용자에게 출입그룹 할당하기

사용자 창에서 출입그룹을 개별 사용자에게 할당할 수 있습니다. 한 명의 사용자에게 최대 4 개의 출입 그룹을 할당할 수 있습니다.

사용자에게 출입그룹 할당하기

1. 단축 메뉴 창에서 **사용자**를 클릭합니다.
2. 탐색 창에서 사용자의 이름을 클릭합니다.
3. 사용자 창에서 출입통제 탭을 클릭합니다.

3. BioStar 설정하기

4. **추가**를 클릭합니다. 사용자 출입그룹 대화 상자가 나타납니다.



5. [해제된 항목] 목록에서 출입그룹을 선택한 후 > 을 클릭하여 [선택한 항목] 목록으로 옮깁니다.
6. 여러 개의 출입그룹을 할당하려면 5 단계를 반복합니다.
7. 출입그룹을 할당하는 것을 마치면, **확인**을 클릭합니다.
8. **적용**을 클릭합니다.

3.8.4 출입그룹을 장치에 전송하기

장치에 출입그룹 전송하기

1. 단축 메뉴 창에서 **출입통제**를 클릭합니다.
2. 작업 창에서 **장치에 전송**을 클릭합니다. 장치 트리 대화 상자가 나타납니다.
3. 장치를 선택합니다.
4. **확인**을 클릭합니다.

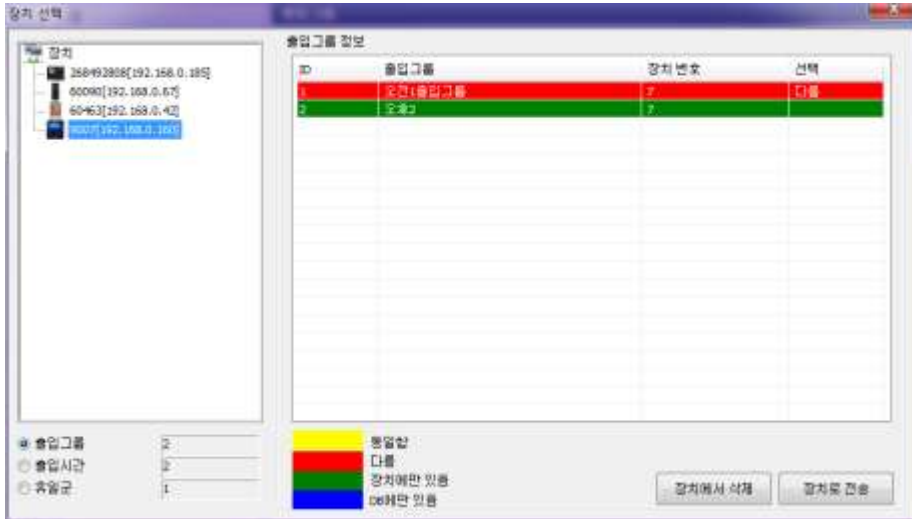
3.8.5 장치별 출입 그룹 확인하기

장치에 적용되어 있는 출입 규칙을 확인할 수 있습니다. 또한, 장치와 서버 데이터베이스의 출입 규칙이 서로 다르다면, 장치에서 해당 정보를 삭제하거나 데이터베이스의 정보를 장치로 전송하여 장치와 데이터베이스 간의 출입 규칙을 동일하게 유지할 수 있습니다.

3. BioStar 설정하기

장치에 설정되어 있는 출입 그룹 확인하기

1. 단축 메뉴 창에서 **출입통제**를 클릭합니다.
2. 작업 창에서 **장치별 출입그룹 관리**를 클릭합니다. 장치 선택 대화 상자가 나타납니다.



3. 장치를 선택합니다.
4. 왼쪽 아래에서 출입그룹, 출입시간, 또는 휴일군을 선택합니다. 선택한 옵션에 해당하는 데이터 목록이 오른쪽에 나타납니다. 장치와 서버 데이터베이스의 데이터가 일치하는지, 또는 데이터가 어느 한쪽에만 존재하는지 색깔로 표시됩니다.
5. 선택 사항: 장치에만 있는 데이터를 삭제할 때는, 목록에서 삭제하고자 하는 데이터를 선택한 후, 오른쪽 아래에 있는 장치에서 삭제를 클릭합니다.
6. 선택 사항: 서버 데이터베이스에만 있는 데이터를 장치로 전송할 때는, 목록에서 전송하고자 하는 데이터를 선택한 후, 오른쪽 아래에 있는 장치로 전송을 클릭합니다.

3. BioStar 설정하기

3.9 근태관리 설정하기

BioStar의 근태관리 기능을 이용하여 시간구분, 일일규칙, 근무규칙, 휴일규칙을 설정합니다. 근태관리 기능을 설정하기 위해서는 이 절과 함께 3.7.2를 참조하세요.

3.9.1 시간구분 추가하기

시간구분 추가하기

1. 단축 메뉴 창에서 **근태**를 클릭합니다.
2. 작업 창에서 **시간구분 추가**를 클릭합니다. 시간구분 창이 열립니다.

The screenshot shows a dialog box titled "시간구분" (Time Division). It is divided into two sections: "기본정보" (Basic Information) and "상세정보" (Detailed Information). In the "기본정보" section, there are two input fields: "이름" (Name) containing the text "야간근무" and "설명" (Description) which is currently empty. In the "상세정보" section, there are three fields: "시간당 급여율" (Hourly Rate) with a numeric input of "1", "시간 집계 단위(분)" (Time Unit) with a numeric input of "1", and "지정색" (Designated Color) with a dropdown menu showing a green color swatch. At the bottom right of the dialog, there is a button labeled "적용" (Apply).

3. 시간구분의 이름과 설명을 입력합니다.
4. 시간구분의 상세사항을 입력합니다.
 - **시간당 급여율**: 시간대에 적용될 임금의 요율을 입력합니다. 1은 기본 임금 요율을 뜻합니다.
 - **시간 집계 단위(분)**: 반내림이 적용되는 시간의 단위를 입력합니다. 예를 들어, "5"를 입력하면 사용자의 근무 시간은 가장 가까운 5 단위 숫자로 반내림되어 처리됩니다. 즉, 1~4는 0으로 반내림되며 6~9는 5로 반내림됩니다.
 - **지정색**: 이 시간 구분이 적용된 시간대에 표시될 색깔을 선택합니다.
5. **적용**을 클릭하여 시간구분의 설정을 저장합니다.

3. BioStar 설정하기

3.9.2 일일규칙 추가하기

BioStar 1.35 또는 그 이상에서는 최대 256 개의 일일규칙을 추가할 수 있습니다.

일일규칙 추가하기

1. 단축 메뉴 창에서 **근태**를 클릭합니다.
2. 작업 창에서 **일일규칙 추가**를 클릭합니다. 일일규칙 창이 열립니다.

시간구분	시작/종료 시간	시작 허용(분)	종료 허용(분)	들어올 타...	나감 타각 ...
오전근무	08:30~12:00	10	0	5	0
오후근무	13:00~17:30	사용 안함	5	0	5
야간근무	19:00~21:00	사용 안함	사용 안함	0	0
철야근무	24:00~06:00(+1)	사용 안함	사용 안함	0	0

3. 일일규칙의 이름과 설명을 입력합니다.
4. 일일규칙의 시작 시간을 입력하고, 하루 중 처음으로 인증에 성공한 시간을 출근으로 마지막으로 인증에 성공한 시간을 퇴근으로 인식하게 하려면 **처음 시간 출근/마지막 시간 퇴근** 체크 상자를 선택합니다.
5. 시간대를 추가하여 일일규칙을 설정합니다.
 - a. 시간대를 상세하게 설정합니다.
 - **시작 시간**: 시간대의 시작 시간을 입력합니다. 시간대가 다음 날에 시작한다면 **명일** 체크 상자를 선택합니다.
 - **종료 시간**: 시간대의 종료 시간을 입력합니다. 시간대가 다음 날에 끝난다면 **명일** 체크 상자를 선택합니다.
 - **시간구분**: 아래 화살표를 클릭하여 목록에서 시간구분을 선택합니다. 이 목록에서 나타나는 시간구분을 설정하려면 3.9.1 을 참조하십시오.
 - **최소 근무인정 시간(분)**: 시간대에 적용되는 최소 시간(분 단위)을 입력하세요. 입력된 시간만큼 근무하지 않을 경우 BioStar 시스템은 전혀 근무하지 않은 것으로 처리합니다.

3. BioStar 설정하기

- **시작 허용(분):** 시간대의 시작 시간보다 늦게 들어올 경우 지각으로 기록할 것인지 선택합니다. 이 옵션을 선택할 경우 몇 분 이후를 지각으로 처리할 지 입력합니다. 입력한 시간 안에 들어오면 제 시간에 들어온 것으로 처리합니다.
- **종료 허용(분):** 시간대의 종료 시간보다 빨리 나갈 경우 조퇴로 처리할 지 선택합니다. 이 옵션을 선택할 경우 몇 분 이전을 조퇴로 처리할 지 입력합니다. 입력한 시간 안에 나가면 제 시간에 나간 것으로 처리합니다.
- **들어옴 타각 시간 반올림(분):** 늦게 들어오는 것을 몇 분 단위로 반올림하여 처리할지 입력합니다. 예를 들어 “5”를 입력하면 1~4 분 늦더라도 5 분 늦은 것으로, 6~9 분 늦더라도 10 분(5의 가장 가까운 배수) 늦은 것으로 처리합니다.
- **나감 타각 시간 반올림(분):** 빨리 나가는 것을 몇 분 단위로 반올림하여 처리할지 입력합니다. 예를 들어 “5”를 입력하면 1~4 분 일찍 나가더라도 5 분 일찍 나간 것으로, 6~9 분 일찍 나가더라도 10 분(5의 가장 가까운 배수) 일찍 나간 것으로 처리합니다.
- **들어옴 이벤트 누락 시 정시 들어옴 처리:** 이 옵션을 선택하면, 출입통제 단말기의 근태기능을 이용하지 않고 들어와서 들어온 기록이 누락되더라도 그 시간대의 시작 시간에 들어온 것으로 처리합니다.
- **나감 이벤트 누락 시 정시 나감 처리:** 이 옵션을 선택하면, 출입통제 단말기의 근태기능을 이용하지 않고 나가서 나간 기록이 누락되더라도 그 시간대의 종료 시간에 나간 것으로 처리합니다.
- **당일 근무 결과에 영향을 줌:** 이 옵션을 선택하면 시간대에 일어난 기록(지각, 조퇴, 정상근무 등)이 계산되어 근태 보고서의 그날 결과 열에 표시됩니다.

b. **추가**를 클릭하여 설정한 시간대를 일일규칙에 추가합니다.

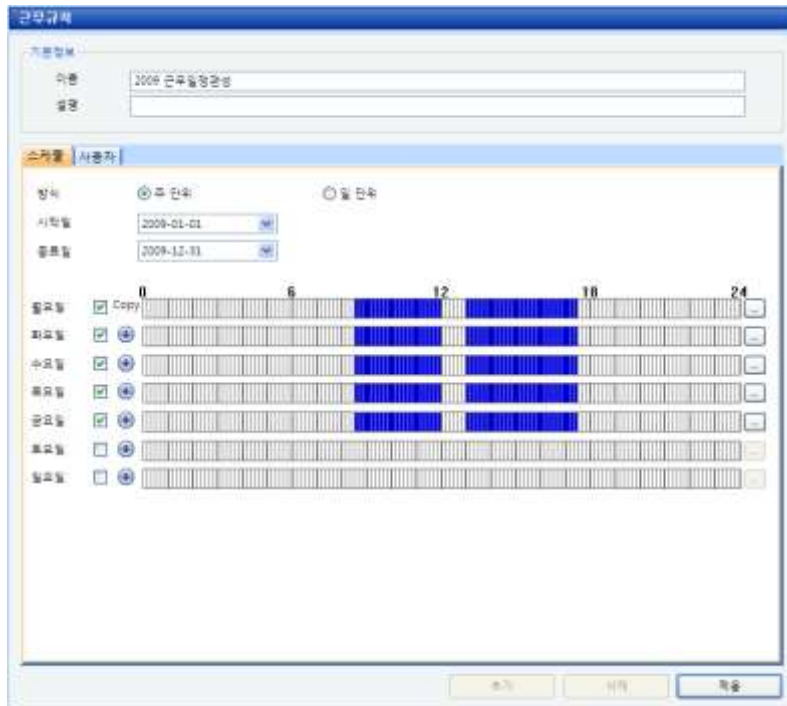
6. **적용**을 클릭하여 일일규칙을 저장합니다.

3.9.3 근무규칙 추가하기

근무규칙 추가하기

1. 단축 메뉴 창에서 **근태**를 클릭합니다.
2. 작업 창에서 **근무규칙 추가**를 클릭합니다. 근무규칙 창이 나타납니다.

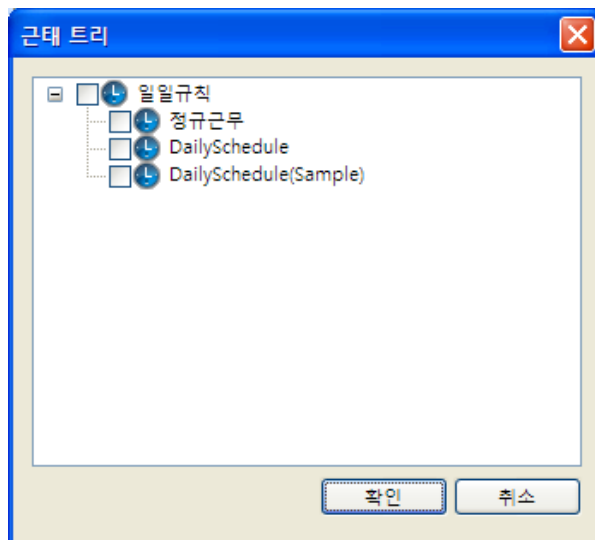
3. BioStar 설정하기



3. 스케줄 방식옵션에서 한 주를 주기로 순환하는 근무규칙(주 단위)을 편성할지 임의의 며칠을 주기로 순환하는 근무규칙(일 단위)을 편성할지 선택합니다. 일 단위를 선택한 경우에는 편성한 근무규칙이 순환되는 주기를 입력한 후 업데이트를 클릭해야 합니다. 입력한 날짜의 수에 따라 근무규칙 표가 바뀝니다.

참고: 일 단위 방식은 BioStar 표준 버전에서만 지원됩니다.

4. 시작일 목록 상자에서 근무규칙의 시작 날짜를 입력하고 종료일 상자의 아래 화살표를 클릭하여 근무규칙의 종료 날짜를 입력합니다.
5. 순환 주기의 각 날짜의 옆에 위치한 체크 상자를 선택하여 일일규칙을 적용할 날들을 선택합니다.
6. 선택한 각 날짜의 오른쪽 끝에 있는 버튼(...)을 클릭하여 해당 날짜에 적용할 일일규칙을 선택합니다. 아래와 같은 근태 트리 대화 상자 속에 일일규칙 목록이 나타납니다. 이 목록에 나타나는 일일규칙을 설정하는 방법에 관해서는 3.9.2 를 참조하십시오.



3. BioStar 설정하기

7. 근태 트리 대화 상자의 목록에서 일일규칙을 선택한 후 **확인**을 클릭합니다.
8. 선택한 날짜 수에 맞게 5~7 단계를 반복합니다.

참고: 각 표 앞에 위치한 버튼을 클릭하면 그 날짜의 위에 있는 일일규칙을 현재의 날짜에 복사할 수 있습니다. 근무 규칙은 1,024 개까지 추가할 수 있습니다.

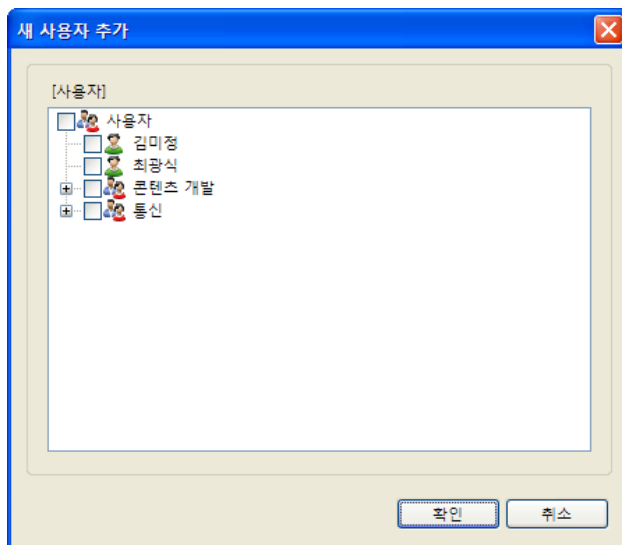
9. **적용**을 클릭하여 근무규칙을 저장합니다.

3.9.4 사용자에게 근무규칙 적용하기

BioStar 시스템이 사용자의 근무시간을 계산하기 위해서 관리자나 운영자는 생성한 근무규칙을 사용자에게 적용해야 합니다. 근무규칙을 사용자에게 적용하는 방법에는 2 가지가 있습니다. 하나는 근무규칙 창의 사용자 탭에서 적용하는 것이며, 다른 하나는 사용자 창의 근태 탭에서 적용하는 것입니다.

사용자에게 근무규칙 적용하기

1. 단축 메뉴 창에서 **근태**를 클릭합니다.
2. 탐색 창에서 적용하려는 근무규칙을 클릭합니다.
3. 근무규칙 창에서 **사용자** 탭을 클릭한 후 창의 아래에 있는 **추가**를 클릭합니다. **새 사용자 추가** 대화 상자가 나타납니다.

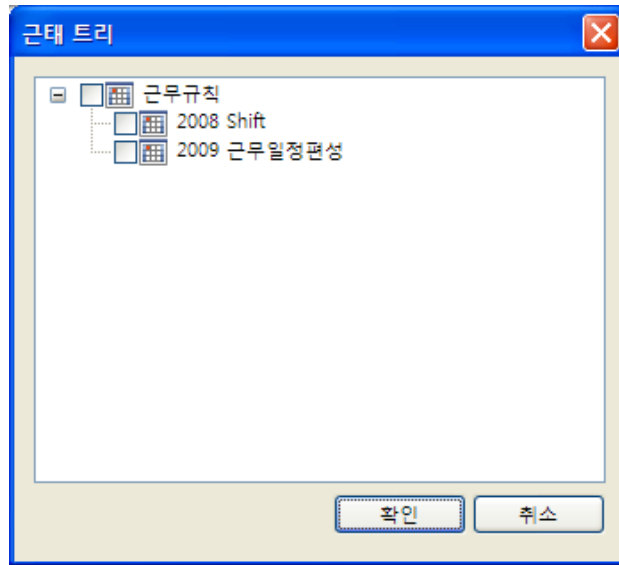


4. 목록에서 근무규칙을 적용할 사용자를 선택한 후 **확인**을 클릭합니다.
5. **적용**을 클릭하여 설정을 저장합니다.

사용자 창의 근태 탭에서 사용자에게 근무규칙을 적용하려면 다음 절차를 따릅니다.

1. 단축메뉴 창에서 **사용자**를 클릭합니다.
2. 탐색 창에서 사용자의 이름을 클릭합니다.
3. **사용자** 창에서 **근태** 탭을 클릭합니다.
4. 근무규칙 설정을 클릭한 후 창의 아래에 있는 **추가**를 클릭합니다. **근태 트리 대화** 상자가 나타납니다.

3. BioStar 설정하기



5. 근무규칙을 선택한 후 **확인**을 클릭합니다.
6. **적용**을 클릭하여 설정을 저장합니다.

사용자별 근무 규칙 추가하기

1. 단축 메뉴 창에서 **근태**를 클릭합니다.
2. 작업 창에서 개인별 근무규칙을 클릭합니다. **개인별 근무규칙** 대화 상자가 나타납니다.



3. 왼쪽에서 사용자를 선택합니다. 사용자에게 적용되어 있는 근무 규칙, 휴일 규칙, 개인 휴가의 내용이 오른쪽에 나타납니다.
4. 근무 규칙, 휴일 규칙, 개인 휴가를 추가하려면, 해당 버튼을 클릭한 후, 오른쪽 아래에 있는 **추가**를 클릭합니다.
5. 추가하고자 하는 항목을 선택한 후 **확인**을 클릭합니다.

3. BioStar 설정하기

6. 기존에 적용한 근무 규칙을 재정의하려면 근무규칙 재정의 버튼을 선택한 후 오른쪽 아래에 있는 **추가**를 클릭합니다.

참고: 재정의한 근무 규칙은 보고서 생성 시 일일 보고서와 개인별 보고서에서만 지원되며, '새로 작성' 옵션을 선택한 경우와 '모두 새로 작성' 옵션을 선택한 경우에도 삭제되지 않습니다.

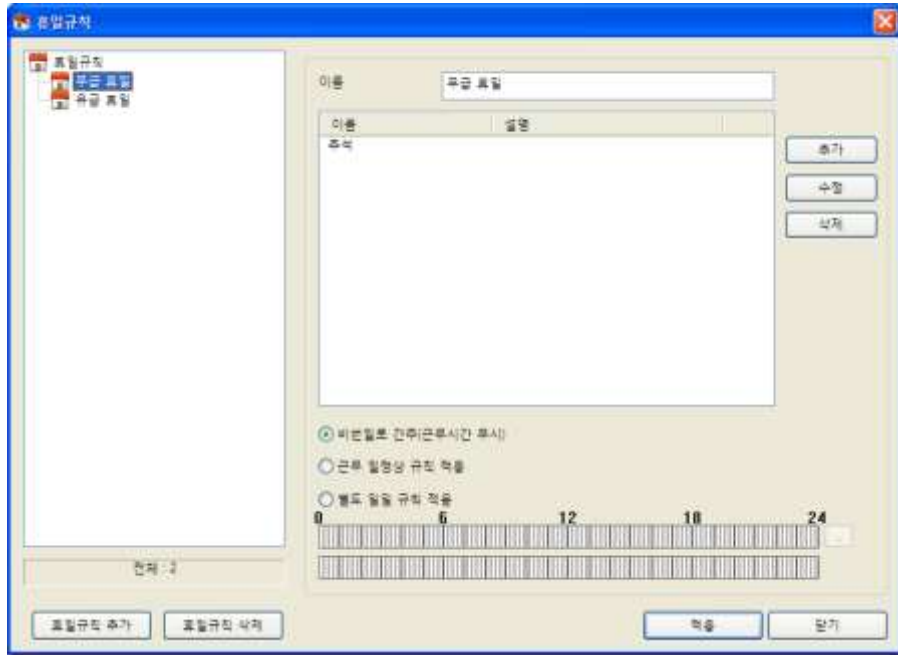
근무규칙의 재정의: 일시적으로 적용되는 우선 근무 규칙

7. 새로 적용하고자 하는 근무 규칙을 선택한 후 **확인**을 클릭합니다.
8. **적용**을 클릭합니다.

3.9.5 휴일규칙 추가하기

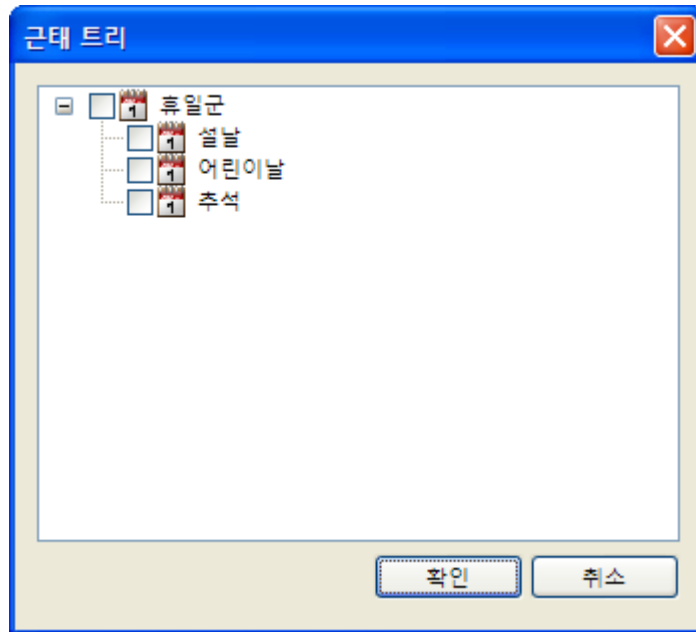
휴일규칙 추가하기

1. 단축 메뉴 창에서 **근태**를 클릭합니다.
2. 작업 창에서 **휴일규칙 관리**를 클릭합니다. 휴일규칙대화 상자가 나타납니다.



3. **휴일규칙 추가**를 클릭합니다.
4. 휴일규칙의 이름을 입력합니다.
5. **추가**를 클릭합니다. 근태 트리 대화 상자가 나타납니다.

3. BioStar 설정하기



6. 근태 트리대화 상자의 목록에서 휴일규칙을 적용할 휴일군을 선택한 후 **확인**을 클릭합니다. 휴일군을 추가하려면 3.7.2 를 참조하십시오.
7. 일일규칙 대화 상자의 오른쪽 아래에 있는 버튼을 클릭하여 선택한 휴일군에 어떠한 규칙을 적용할지 선택합니다.
 - **비번일로 간주(근무시간 무시)**: 근무일에서 완전히 제외되는 휴일로 처리됩니다. BioStar 시스템은 이 휴일동안 이루어지는 근태 결과를 처리하지 않습니다.
 - **근무 일정상 규칙 적용**: 선택한 휴일 군을 편성된 근무규칙에 포함합니다. 근무규칙 편성의 흐름에 맞는 일일 규칙이 선택한 휴일 군에 적용됩니다.
 - **별도 일일 규칙 적용**: 선택한 휴일 군에만 적용할 특별한 일일 규칙을 선택하여 적용합니다.
8. **별도 일일 규칙 적용** 옵션을 선택한 경우 아래에 위치한 표의 오른쪽에 있는 버튼(...)을 클릭한 후 근태 트리 대화 상자의 목록에서 일일 규칙을 선택한 다음 **확인**을 클릭합니다. 일일 규칙을 추가하는 방법에 대해서는 3.9.2 를 참조하십시오.
9. **적용**을 클릭하여 설정한 휴일규칙을 저장합니다.

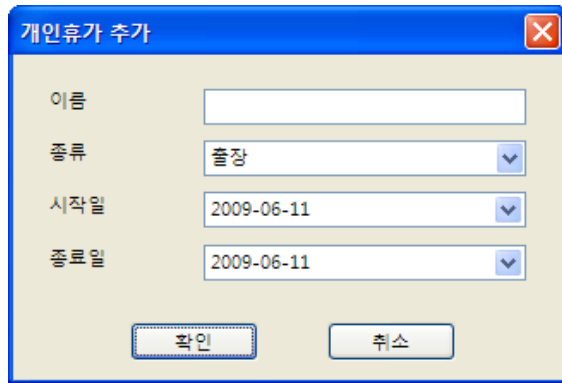
3.9.6 개인휴가 추가하기

사용자 개인에게만 적용되는 개인휴가를 추가하여 개인 사정이나 근무 상황에 따른 올바른 출결 결과를 근태 보고서에 반영할 수 있습니다.

개인 휴가 추가하기

1. 단축메뉴 창에서 **사용자**를 클릭합니다.
2. 사용자 창에서 **근태** 탭을 클릭합니다.
3. **개인휴가 설정** 버튼을 클릭한 후 **추가**를 클릭합니다. **개인휴가 추가** 대화 상자가 나타납니다.

3. BioStar 설정하기



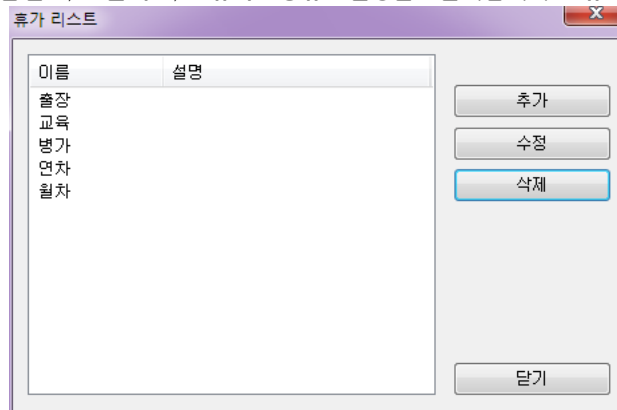
4. 휴가의 이름을 입력합니다.
5. 종류 목록 상자에서 휴가 종류를 선택합니다.
6. 시작일 목록 상자와 종료일 목록 상자에서 시작 날짜와 종료 날짜를 선택합니다.
7. 확인을 클릭하여 사용자의 근태 설정에 휴가를 추가합니다.
8. 사용자 창의 아래에 있는 적용을 클릭하여 사용자의 근태 설정을 저장합니다.

3.9.7 사용자 지정 휴가 추가하기

BioStar에서는 기본적으로 5 가지(출장, 교육, 병가, 연차, 월차) 개인 휴가를 지원합니다. 이 외에 사용자 지정 휴가를 추가하여 사용할 수 있습니다.

사용자 지정 휴가 추가하기

1. 옵션 > 근태 > 휴가 종류 설정을 클릭합니다. 휴가 리스트 대화 상자가 나타납니다.

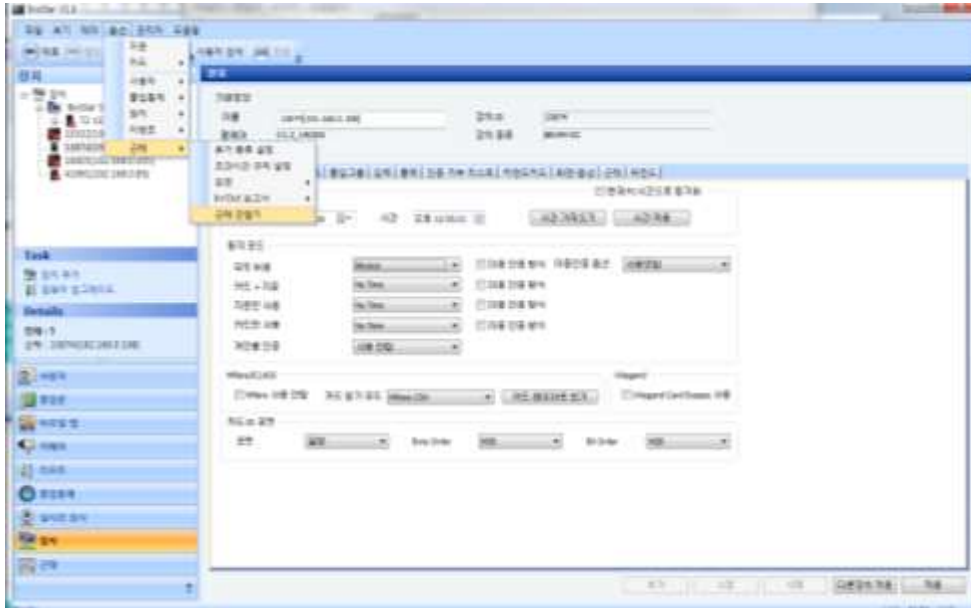


2. 추가를 클릭합니다.
3. 휴가 이름과 설명을 입력한 후, 확인을 클릭합니다. 새로 추가한 휴가 이름이 목록에 추가됩니다.
4. 닫기를 클릭합니다.

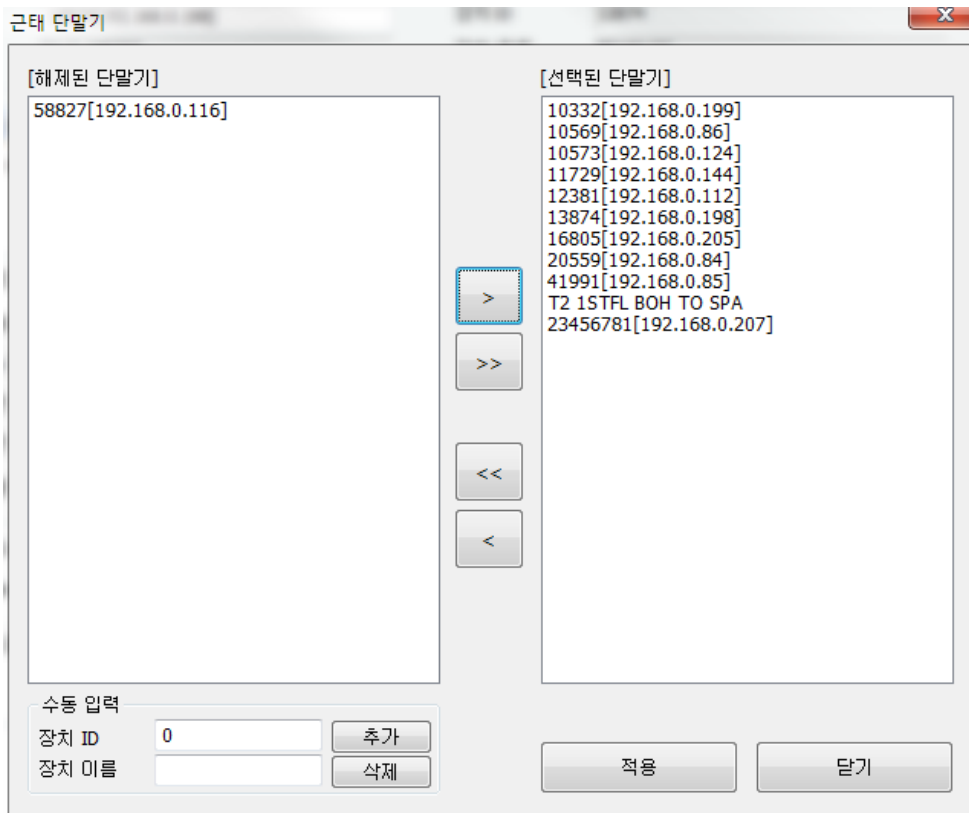
3.9.8 근태 사용 단말기 설정

근태 결과에 반영할 단말기를 선택할 수 있습니다. 근태 리포트에서는 근태에 반영할 장치를 선택할 수 있도록 메뉴 및 설정 창을 제공합니다. 기본값을 선택하면 모든 장치가 근태 리포트에 반영됩니다. 근태 처리 시, 선택한 장치들의 이벤트 로그만을 이용하여 리포트를 생성하며, 근태 리포트의 상세 창에서 근태 단말기가 아닌 경우는 근태 이벤트 키 참조 목록에 표시되지 않습니다.

3. BioStar 설정하기



>, >> 혹은 <, <<으로 선택과 해제가 가능하며, 현재 추가된 단말기 목록은 선택된 단말기 혹은 해제된 단말기 목록에 포함되어 있습니다. 수동 입력은 추가된 단말기 목록에는 없지만 기존 로그에 포함된 특정 장치의 ID를 추가할 때 사용합니다.



3. BioStar 설정하기

3.10 경보 설정하기

BioStar 는 여러 수준의 경보 기능을 제공합니다. 연결된 장치나 컴퓨터에서 경보음을 발생시키도록 설정할 수 있습니다. 또한 지정된 수신자에게 이메일로 통지하도록 설정할 수 있습니다. 뿐만 아니라 슬레이브 장치(예, 화재 경보 장치)로부터 입력 신호를 받을 수 있도록 설정할 수 있으며, 슬레이브 장치(예, 경보 사이렌)에 출력 신호를 보내도록 설정할 수 있습니다.

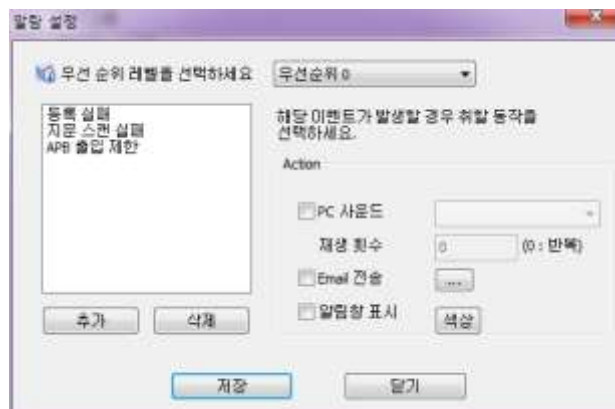
3.10.1 경보와 경보음 설정하기

BioStar 가 각 이벤트에 어떻게 반응할지 설정할 수 있습니다. 우선 순위를 결정하고 이벤트가 발생했을 때 BioStar 가 어떤 동작을 취할 지 설정할 수 있습니다. 또한 경보음으로 사용할 소리를 추가할 수도 있습니다.

3.10.1.1 경보 동작 설정하기

경보 동작 설정하기

1. 메뉴 표시줄에서 **옵션 > 이벤트 > 알람 설정**을 클릭합니다. 알람 설정 대화 상자가 나타납니다.



2. "우선 순위 레벨을 선택하세요" 목록 상자를 클릭하여 우선순위를 선택한 후 **추가**를 클릭합니다. 모든 이벤트 대화 상자가 나타납니다.
3. 선택한 우선순위에 포함할 이벤트를 선택한 후 **확인**을 클릭합니다.
4. 왼쪽에 있는 Action 영역에서 체크 상자를 선택하여 경보 동작을 설정합니다.
 - **PC 사운드**: 목록 상자에서 경보음을 선택합니다. 임의의 소리를 추가하는 방법에 관해서는 3.10.1.2 를 참조하십시오.
 - **Email 전송**: 줄임표(...) 버튼을 클릭하여 메일 수신자를 지정합니다. 메일 통지의 설정 방법에 관해서는 3.10.2 를 참조하십시오.
 - **알림창 표시**: 이벤트가 발생할 때 로컬 컴퓨터에 팝업 메시지를 띄웁니다.
 - **색상**: 알림창이 나타날 때, 이벤트의 우선 순위별 텍스트와 배경의 색깔을 지정합니다.
5. 다른 우선순위를 설정하려면 2~4 단계를 반복합니다.
6. **저장**을 클릭합니다.

3.10.1.2 임의의 경보음 추가하기

3. BioStar 설정하기

경보음 추가하기

1. 메뉴 표시줄에서 **옵션 > 이벤트 > 사운드 설정**을 클릭합니다. 사운드 설정 대화 상자가 나타납니다.
2. **추가**를 클릭합니다.
3. 웨이브(wav) 형식의 파일을 선택한 후 **열기**를 클릭합니다.
4. 필요하다면, 추가된 파일을 목록에서 선택한 후 **재생**을 클릭하여 소리를 들어볼 수 있습니다.
5. **저장**을 클릭합니다.

3.10.2 메일 통지 설정하기

경보 이벤트가 발생하면 지정된 수신자에게 메일로 통지할 수 있습니다(무료 버전에서는 사용할 수 없음). 3.10.1.1 에 설명된 바와 같이, 어떤 이벤트가 발생해야 BioStar 가 자동으로 메일을 발송할지는 사용자가 직접 설정할 수 있습니다. BioStar 는 TLS 및 SSL 보안 기능을 사용하는 메일 서버를 통한 메일 통지 기능을 지원합니다.

메일 통지 설정하기

1. 메뉴 표시줄에서 **옵션 > 이벤트 > E-mail 설정**을 클릭합니다. E-mail 전송 설정 대화상자가 나타납니다.



2. 보내는 사람 영역에서 **Email**(메일주소), **SMTP 서버**(IP 주소), **포트** 번호, **SMTP ID**, **SMTP 비밀번호**를 입력하고, **보안 종류** 드롭다운 목록에서 **NO SECURITY**, **TLS** 또는 **SSL** 중 한 가지를 선택합니다.
3. 받는 사람 영역에서 메일 주소를 입력합니다.
4. **추가**를 클릭하여 메일 수신자를 목록에 추가합니다.

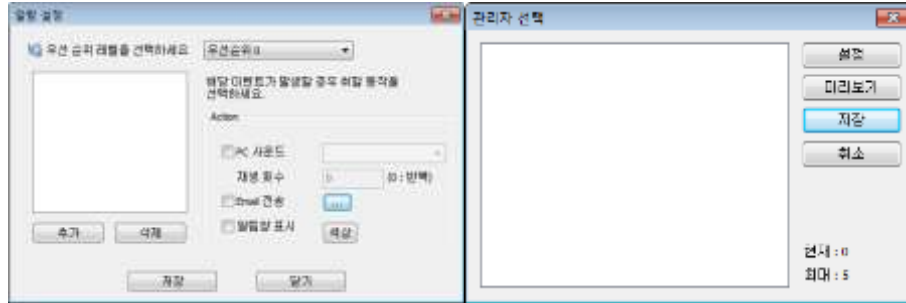
3. BioStar 설정하기

5. 수신자를 더 추가하려면 2~4 단계를 반복합니다.
6. 저장을 클릭합니다.

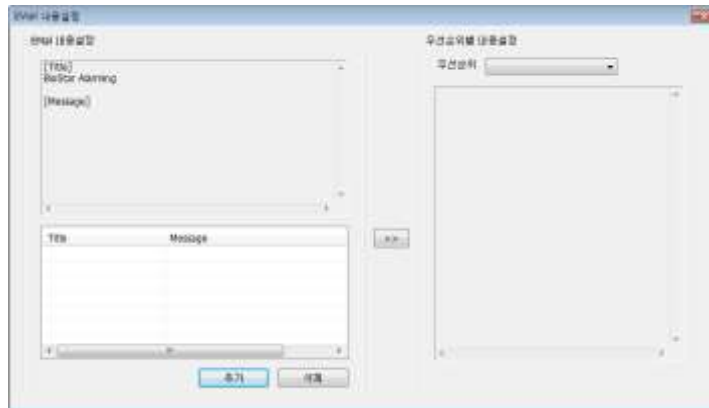
메일 내용 설정하기

알람 설정을 사용하여 사용자가 지정한 포맷으로 메일을 전송할 수 있습니다.

1. **옵선 > 이벤트 > 알람 설정 > Email 전송 > “...”** 버튼을 클릭하여 **관리자 선택** 창을 엽니다.



2. 설정을 클릭하여 **Email 전송 설정** 창을 엽니다.
3. 보내는 사람 항목을 작성하고 **추가** 버튼을 클릭합니다.
4. **추가** 버튼을 클릭합니다.
5. **미리보기**를 클릭하여 Email 내용 설정을 변경할 수 있습니다.



6. >, >>, <, << 버튼을 사용하여 우선순위를 설정할 수 있으며, Email 내용은 우선순위 기준으로만 지정할 수 있습니다.
7. **추가**를 클릭하여 **내용설정** 창을 엽니다.
8. **실제 데이터 추가**의 6 개 항목 중에서 필요한 것을 선택하면 Message 에 추가됩니다. 이 내용은 실제 메일 전송 시 해당 위치에 데이터로 치환됩니다. 예를 들어, ##DATE##는 이벤트 발생 일자 시간으로 변경되며, ##USER##는 사용자 이름으로 변경됩니다. 메시지 항목을 삭제하려면 직접 해당 문자열을 마우스로 선택하여 삭제할 수 있습니다.

3. BioStar 설정하기



3.10.3 슬레이브 장치 설정하기

BioStar 와 함께 슬레이브 장치를 사용한다면, 입력 신호를 받아 어떤 동작을 취할지 그리고 어떤 상황에서 출력 신호를 내보낼지 미리 설정해 두어야 합니다. 장치 설정에 관한 자세한 내용은 3.2 와 5.1 을 참조하십시오.

3.10.3.1 슬레이브 장치에 내보내는 출력 설정하기

이벤트가 발생했을 때 BioStar 에서 지정한 장치가 경보 사이렌과 같은 슬레이브 장치에 신호를 보내도록 설정할 수 있습니다.

출력 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 장치의 이름을 클릭합니다.
3. 장치 창에서 **출력** 탭을 클릭합니다.
4. 창의 아래에 있는 **추가**를 클릭합니다. **Output** 설정 대화 상자가 나타납니다.

3. BioStar 설정하기



5. 슬레이브 장치에 신호 내보내기를 시작할 이벤트를 설정합니다:
 - a. **알람 동작 게시 이벤트**: 이벤트 종류를 선택합니다.
 - b. **장치**: 개별 장치를 선택하거나 **모든 장치**를 선택합니다.
 - c. **신호파형**: 신호파형을 선택합니다.
 - d. **우선순위**: 이벤트의 우선순위를 입력합니다.
6. **추가**를 클릭합니다
7. 슬레이브 장치에 신호 내보내기를 멈추게 할 이벤트를 설정합니다.
 - a. **알람 멈춤 이벤트**: 이벤트를 선택합니다.
 - b. **장치**: 개별 장치를 선택하거나 **모든 장치**를 선택합니다.
 - c. **우선순위**: 이벤트의 우선순위를 입력합니다.
 - d. **추가**를 클릭합니다.
8. **추가**를 클릭합니다.
9. **저장**을 클릭합니다.

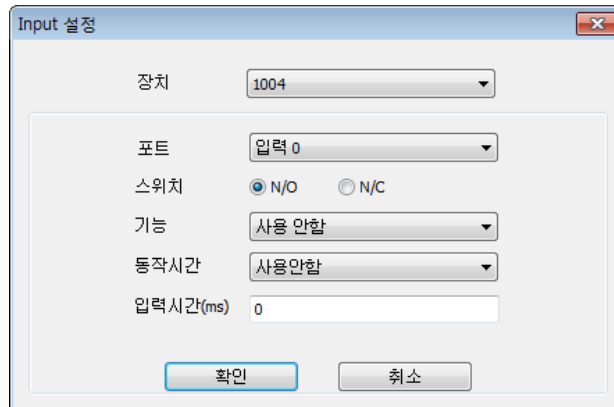
3.10.3.2 슬레이브 장치에서 받아들이는 입력 신호 설정하기

BioStar의 출입문 제어 기능을 화재 경보 시스템과 같은 다른 경보 시스템과 통합하여 운영하기 위해서는, 슬레이브 장치에서 입력 신호가 들어왔을 때 BioStar가 취할 동작을 설정해야 합니다. 또한, 문열림 버튼이나 다른 종류의 슬레이브 장치에 반응하도록 하기 위하여 입력을 설정할 수 있습니다.

입력 설정하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 장치의 이름을 클릭합니다.
3. 장치 창에서 **입력** 탭을 클릭합니다.
4. 창의 아래에 있는 **추가**를 클릭합니다. **Input 설정** 대화상자가 나타납니다.

3. BioStar 설정하기



5. 포트 목록 상자에서 입력 포트를 선택합니다.
6. 입력의 기본 상태(N/O: 평상시 열림, N/C: 평상시 닫힘)를 선택합니다.
7. 기능 목록 상자에서 입력을 받으면 실행할 기능(사용 안함, 일반 입력, 비상 문 열림, 모든 경보 해제, 장치 재 시작, 장치 잠금, LED 녹색, LED 적색, 부저 입력, 출입 허가, 출입 거부)을 선택합니다.

주의: BioStar 1.8v 에서 LED 녹색, LED 적색, 부저 입력, 출입 허가, 출입 거부 기능이 추가되었으며, BioStation (FW 1.93v), BioStation T2 (FW 1.3v), FaceStation (FW 1.3v), BioEntry Plus (FW 1.6v), BioEntry W (FW 1.2v), BioLite Net (FW 1.4v), Xpass (FW 1.3v) 에서만 지원됩니다.

8. 동작시간 목록 상자에서 기능을 적용할 일정(항상적용, 사용안함 또는 사용자가 설정한 출입시간)을 선택합니다.
9. 동작을 발생시키기 위한 입력 신호의 지속 시간(1000분의 1 초)을 설정합니다.
10. 확인을 클릭합니다.

3.11 카메라 설정

이 절에서는 NVR(네트워크 비디오 레코더) 서버 및 IP(인터넷 프로토콜) 카메라를 BioStar 시스템에 추가하는 방법에 대해서 설명합니다 NVR 서버와 IP 카메라를 올바르게 설치하면 특정 지역을 실시간으로 감시할 수 있으며 로그를 확인할 때 저장된 정지 영상이나 동영상을 함께 볼 수 있습니다.

BioStar 는 다음의 IP 카메라와 NVR 서버를 지원합니다.

	모델 이름	제조사/소프트웨어 개발사
IP(인터넷 프로토콜) 카메라	AXIS PTZ 215	AXIS
	AXIS M3203-V	AXIS
	SNP-3120VH	Samsung Techwin
NVR(네트워크 비디오 레코더) 서버	AXIS Camera Station	AXIS
	NET-I Ware	Samsung Techwin

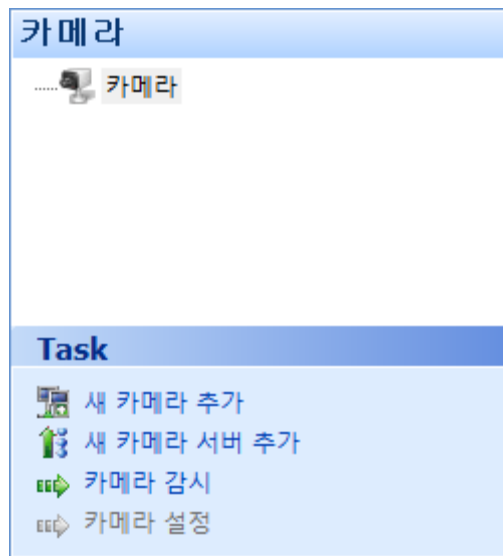
3. BioStar 설정하기

3.11.1 NVR 서버 추가하기

NVR(네트워크 비디오 레코더) 서버는 연결된 카메라로부터 전송되는 아날로그 신호나 비디오 스트림을 동영상으로 저장합니다. BioStar 와 함께 NVR 서버를 활용하면 이벤트 로그를 확인할 때 같은 시간에 녹화된 동영상을 확인할 수 있습니다.

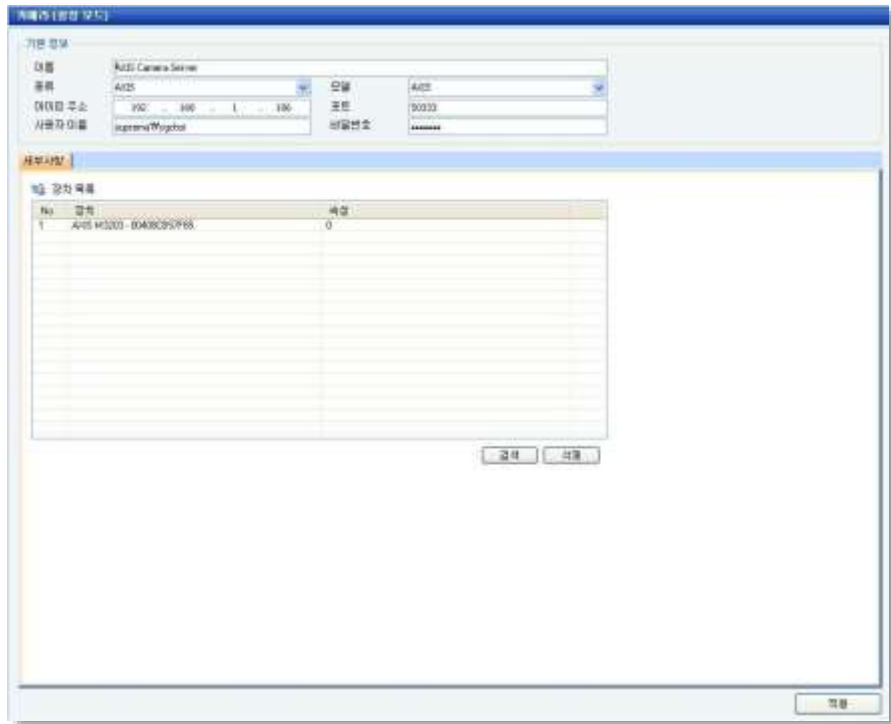
BioStar 시스템에 NVR 서버 추가하기

1. 단축 메뉴 창에서 **카메라**를 클릭합니다.
2. 작업 창에서 **카메라 설정**을 클릭합니다.

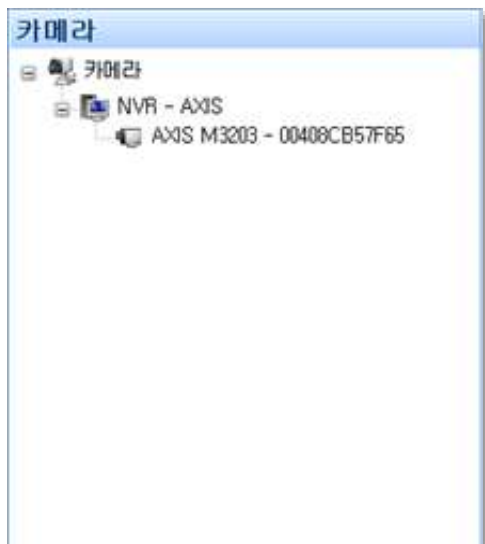


3. BioStar 설정하기

3. 작업 창에서 새 카메라 서버 추가를 클릭합니다. 카메라(설정 모드) 창이 열립니다.



4. 기본 정보 영역에서 NVR 서버의 이름, 종류, 모델, 아이피 주소, 포트 번호를 입력한 후 BioStar가 NVR 서버에 접속하기 위한 사용자 이름과 비밀번호를 입력합니다.
5. 검색을 클릭하여 NVR 서버에 연결된 카메라 목록을 가져옵니다.
6. 오른쪽 아래에 있는 적용을 클릭하면 아래 그림과 같이 검색된 카메라가 탐색 창에 있는 NVR 서버 아래에 추가됩니다.

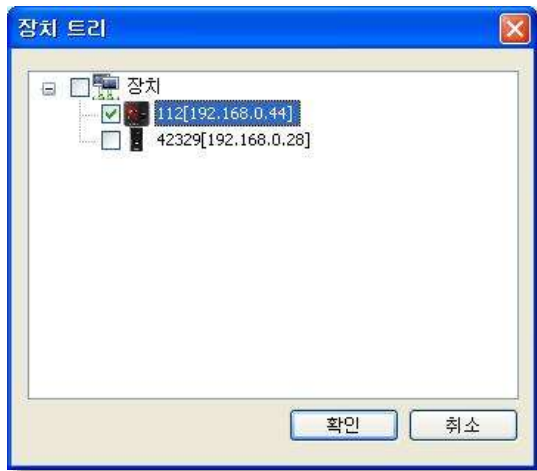


3. BioStar 설정하기

7. 탐색 창에서 NVR 서버에 연결된 카메라를 선택하면 아래와 같은 카메라 (설정 모드) 창이 열립니다.

No.	장치	속성
1	21111[192.168.0.62]	

8. 장치 목록의 오른쪽 아래에 있는 추가를 클릭합니다. 장치 트리 대화 상자가 나타납니다.



9. 장치 목록에서 카메라와 연결할 장치를 선택한 후 확인을 클릭합니다.
10. 오른쪽 아래에 있는 적용을 클릭하여 BioStar 시스템에 변경사항을 적용합니다.

3.11.2 IP 카메라 추가하기

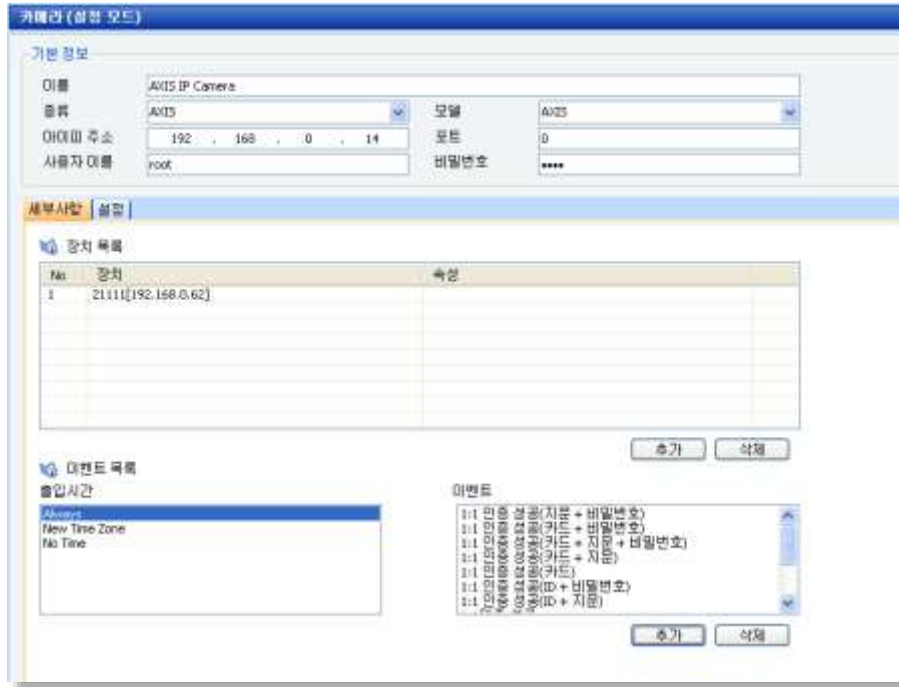
BioStar 에 IP 카메라를 추가하면 IP 카메라를 출입 통제 장치와 연결하여 IP 카메라가 정지 영상을 전송할 이벤트를 설정할 수 있습니다.

BioStar 시스템에 IP 카메라추가하기

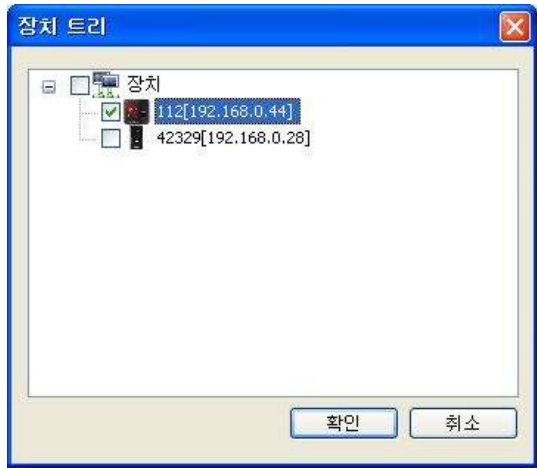
1. 단축 메뉴 창에서 카메라를 클릭합니다.
2. 필요하다면, 작업 창에서 카메라 설정을 클릭합니다.

3. BioStar 설정하기

3. 작업 창에서 **새 카메라 추가**를 클릭합니다. 카메라(설정 모드) 창이 열립니다.



4. 기본 정보 영역에서 IP 카메라의 **이름**, **종류**, **모델**, **아이피 주소**, **포트 번호**를 입력한 후 BioStar가 IP 카메라에 접속하기 위한 **사용자 이름**, **비밀번호**를 입력합니다.
5. 세부사항 탭에서 장치 목록의 오른쪽 아래에 있는 **추가**를 클릭합니다. 장치 트리 대화 상자가 나타납니다.



6. 장치 트리에서 IP 카메라와 연결할 장치를 선택한 후 **확인**을 클릭합니다.
7. 이벤트 목록의 오른쪽 아래에 있는 **추가**를 클릭한 후 IP 카메라가 정지 영상을 전송할 이벤트를 선택합니다.
8. 오른쪽 아래에 있는 **적용**을 클릭하여 BioStar 시스템에 변경사항을 적용합니다.

3. BioStar 설정하기

3.11.3 IP 카메라 설정하기

BioStar 는 PTZ(팬-틸트-줌) 카메라의 시야를 제어할 수 있는 사용자 인터페이스를 제공합니다. PTZ 기능을 지원하는 IP 카메라를 사용한다면 이 기능을 이용하여 PTZ 카메라의 시야를 제어할 수 있습니다.

PTZ 카메라의 시야 제어하기

1. 단축 메뉴 창에서 **장치**를 클릭합니다.
2. 탐색 창에서 설정하려면 PTZ 카메라를 선택합니다.
3. 카메라(설정 모드) 창에서 **설정** 탭을 클릭합니다.
4. Pan & Tilt 및 Zoom 영역에 있는 제어 버튼을 이용하여 PTZ 카메라의 시야를 이동합니다.



BioStar 관리하기

BioStar의 설정을 마쳤다면 관리하는 것은 비교적 간단합니다. BioStar를 이용하면 이벤트를 실시간으로 감시할 수 있고, 이벤트 기록(event log)을 날짜 별로 확인할 수 있으며, 시스템의 일부분을 원격으로 제어할 수 있을 뿐 아니라, 사용자를 관리하고, BioStar에서 장치의 펌웨어를 교체할 수 있습니다. 또한, 보안을 강화하기 위하여 필요하다면 지문을 암호화할 수 있습니다.

4.1 실시간으로 이벤트 감시하기

BioStar 시스템은 연결된 모든 장치에서 일어나는 이벤트를 기록합니다. 실시간으로 이벤트를 감시하려면, 단축 메뉴 창에서 **실시간 감시**를 클릭한 후 실시간 감시 탭을 클릭합니다.





그림 4.1

이 탭에서 마지막으로 시스템에 접속한 이후로 일어난 모든 이벤트를 볼 수 있습니다. 또한 현재의 감시 상태(**실시간 감시 시작**, **실시간 감시 멈춤**)를 확인할 수 있으며 시작 버튼이나 멈춤 버튼을 클릭하여 실시간 감시를 시작하게 하거나 멈추게 할 수 있습니다. 또한 알람으로 설정한 PC 사운드가 발생했을 경우 사운드 버튼(녹색: 사운드 재생 중, 회색: 사운드 멈춤을 나타냄)을 클릭하여 정지할 수 있습니다.

4. BioStar 관리하기

BioStar 1.5 이후로 이벤트 로그 앞에 2 개의 아이콘을 사용하여 정지 영상이나 동영상을 함께 확인할 수 있음을 표시합니다.

아이콘	설명
	이벤트 로그와 함께 정지 영상을 확인할 수 있습니다. 이미지를 확인하려면 이벤트 로그를 클릭하세요.
	이벤트 로그와 함께 동영상을 확인할 수 있습니다. 동영상을 확인하려면 이벤트 로그를 두 번 클릭하세요.

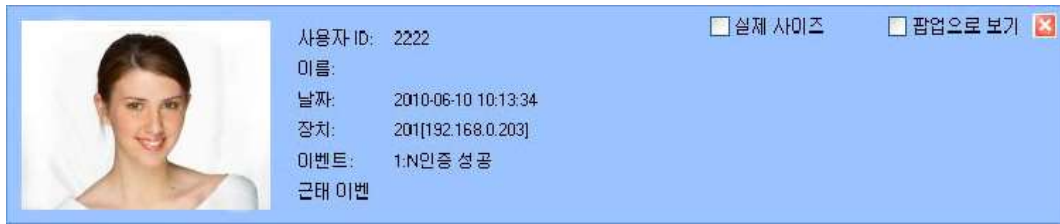
이벤트 로그에 2 개의 아이콘이 모두 표시되어 있다면, 해당 이벤트 로그를 한 번 클릭하여 정지 영상을 확인할 수 있으며 두 번 클릭하여 이벤트가 발생하였을 때 녹화된 동영상을 확인할 수 있습니다. 이벤트 로그를 두 번 클릭하면 아래와 같은 재생 창이 나타납니다.



그림 4.2

관리자는 BioStar의 롤 콜(Roll Call) 기능을 이용하여 사용자의 위치와 인증 상태를 감시할 수 있습니다. 이 기능을 통하여 관리자는 사용자가 사무실에 있는지, 승인되지 않은 곳에 있는지, 행방을 알 수 없는 곳에 있는지를 알 수 있습니다. X-Station, BioStation T2, FaceStation, BioStation A2 의 얼굴 검출 기능과 연계하여 **이미지 보기**와 **실시간 이미지 업데이트**를 선택하면 관리자는 사용자의 이미지를 확인할 수 있습니다. **실제 사이즈**를 선택하면 640x480 크기의 이미지를 볼 수 있고 **팝업으로 보기**를 선택하면 새 창을 열어서 이미지를 볼 수 있습니다.

4. BioStar 관리하기



인증에 성공한 사용자의 이미지를 보려면 메뉴 표시줄에서 **옵션 > 이벤트 > 프로필 이미지 설정**을 클릭하고 이벤트 종류를 선택한 후 프로필 이미지 보이도록 체크 상자를 선택합니다. 사용자가 인증에 성공한 경우 사용자의 이미지가 **실시간 감시** 탭에 나타납니다.

4.1.1 실시간으로 소집구역 감시하기

사용자들의 위치를 추적하여 화재와 같은 비상시에 사용자들이 안전한 구역으로 대피하였는지를 확인할 수 있습니다.

비상시 사용자들의 위치 파악하기

1. 단축 메뉴 창에서 **실시간 감시**를 클릭합니다.
2. 탐색 창에서 소집 구역을 클릭합니다.
3. 작업창에서 **출석 상황표**를 클릭합니다. 출석 상황표 창이 열립니다.



4. 출석 상황표를 보고서 형식으로 보려면 **View Report** 를 클릭합니다. 아래와 같은 출석 보고서 창이 열립니다. 출석 상황표를 CSV 형식으로 저장하려면 **Save as CSV** 를 클릭합니다.

4. BioStar 관리하기

- 출석보고서를 여러 가지 문서 형식으로 내보내려면 보고서 내보내기 아이콘을 클릭합니다. 출석 보고서를 인쇄하려면 프린터 아이콘을 클릭합니다.

사원번호	Status	사원명	장차	대행명	날짜
1	Missing	김영호			
2	Missing	손남희			
3	Missing	남대호			
4	Date	나병업	101 192.168.0.203	1차인출 성공	2010-06-10 18:28:25
5	Date	박민호	101 192.168.0.203	1차인출 성공	2010-06-10 18:28:20
6	Date	이영민	101 192.168.0.203	1차인출 성공	2010-06-10 18:28:14

4.1.2 카메라를 통해 실시간으로 감시하기

BioStar에 연결된 카메라를 통해 특정 지역을 실시간으로 감시할 수 있습니다.

카메라 실시간 감시하기

- 단축 메뉴 창에서 **카메라**를 클릭합니다.
- 필요하다면, 작업 창에서 **카메라 감시**를 클릭합니다.
- 탐색 창에서 실시간으로 감시할 카메라를 선택합니다.

4.2 이벤트 기록 보기

BioStar를 이용하면 각 사용자, 출입문, 구역 별로 이벤트 기록을 볼 수 있습니다. 사용자, 출입문, 구역 창의 이벤트 탭에서, 미리 설정된 형식으로 표시되는 이벤트 기록을 볼 수 있습니다. 또한 모니터링 창의 로그확인 탭에서 여러 옵션을 설정할 수 있습니다.

BioStar 서버가 실행되고 있으면, BioStar는 연결된 장치에서 발생하는 모든 이벤트 기록을 자동적으로 수집합니다. 그러나 장치가 BioStar 서버에 직접 연결되어 있지 않다면, 이벤트 기록을 보기 위해서는 먼저 기록을 수동으로 BioStar 클라이언트에 전송해야 합니다.

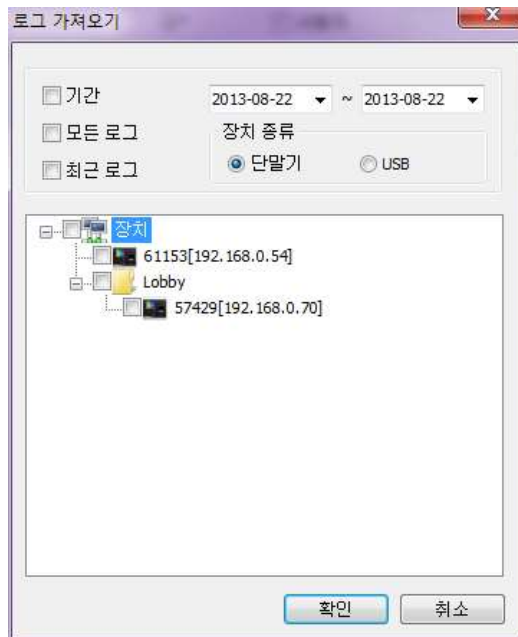
4. BioStar 관리하기

4.2.1 이벤트 로그 업로드 하기

장치가 BioStar 서버에 직접 연결되어 있지 않다면, 장치로부터 이벤트 로그를 수동으로 업로드 할 수 있습니다.

이벤트 로그 업로드 하기

1. 단축 메뉴 창에서 **실시간 감시**를 클릭합니다.
2. 모니터링 창에서 **로그확인** 탭을 클릭합니다.
3. 작업 창에서 **로그 가져오기**를 클릭합니다. **로그 가져오기** 대화 상자가 나타납니다.



4. 필요에 따라 다음 옵션을 설정합니다.
 - **기간**: 이벤트 로그의 기간을 지정합니다. 옵션을 선택합니다.
 - **모든 로그**: 모든 이벤트 로그를 업로드 합니다.
 - **최근 로그**: 마지막으로 로그를 업로드 한 이후에 발생한 로그를 업로드 합니다.
 - **장치 종류**
 - **단말기**: 단말기에서 로그를 업로드 할 때 선택합니다.
 - **USB**: USB로부터 장치 로그를 업로드 할 때 선택합니다.
5. 장치 또는 **USB 로그**를 선택합니다.
6. **확인**을 클릭합니다. 선택한 장치의 이벤트 기록이 로그확인 탭의 목록에 표시됩니다.

참고: USB 로부터 이벤트 로그를 업로드 할 수 있는 기능은 X-Station, BioStation T2, FaceStation 에서 지원됩니다.

4.2.2 사용자, 출입문, 구역 창에서 이벤트 로그 보기

사용자, 출입문, 구역 창에서 이벤트 로그 보기

1. 단축 메뉴 창에서 **사용자** 또는 **출입문**을 클릭합니다.
2. 탐색 창에서 사용자, 출입문, 또는 구역의 이름을 클릭합니다.
3. 사용자, 출입문, 또는 구역 창에서 **이벤트** 탭을 클릭합니다.

4. BioStar 관리하기

4. 기간 목록 상자에서 기간의 첫 날짜와 마지막 날짜를 선택합니다.
5. **로그확인**을 클릭합니다. 지정한 기간 동안 발생한 이벤트가 표시됩니다.

추가정보 지문 얼굴 카드 출입통제 근태 이벤트				
기간	2010-06-09	~	2010-06-10	로그확인
No	날짜	출입문	장치 ID	상태
1	2010-06-10 10:25:32	출입문A	201	1:N인출성공
2	2010-06-10 10:25:27	출입문A	201	1:N인출성공
3	2010-06-10 10:25:22	출입문A	201	1:N인출성공
4	2010-06-10 10:25:16	출입문A	201	1:N인출성공
5	2010-06-10 10:25:09	출입문A	201	1:N인출성공
6	2010-06-10 10:24:36	출입문A	201	등록성공

4.2.3 모니터링 창에서 이벤트 로그 보기

사용자 그룹, 출입문, 구역별로 이벤트 로그 보기

1. 단축 메뉴 창에서 **실시간 감시**를 클릭합니다.
2. 모니터링 창에서 **로그확인** 탭을 클릭합니다.
3. 기간 상자의 아래 화살표를 클릭하여 달력에서 기간의 첫 날짜와 마지막 날짜를 선택합니다.
4. 기록을 표시하기 위한 옵션을 설정합니다.
 - 우선순위를 기준으로 기록을 표시하려면, **이벤트** 체크 상자를 선택한 후 아래 화살표를 클릭하여 목록에서 우선순위를 선택합니다. 새로운 우선순위를 추가하려면, **출입표(...)** 버튼을 클릭하여 알람 설정 대화 상자를 엽니다.
 - 사용자를 기준으로 기록을 표시하려면, **사용자** 체크 상자를 선택한 후 **출입표(...)** 버튼을 클릭한 다음, 사용자(부서) 트리 대화 상자에서 사용자를 선택합니다. 사용자 목록에서 가장 위에 있는 체크 상자를 선택하면 모든 사용자를 선택할 수 있습니다.
 - 장치를 기준으로 기록을 표시하려면, **장치 ID** 체크 상자를 선택한 후 **출입표(...)** 버튼을 클릭한 다음, 장치 트리 대화 상자에서 장치를 선택합니다. 네트워크와 관련된 기록만 보려면 네트워크 정보 변경 이력 체크 상자를 선택합니다.
 - 모든 기록을 보려면 체크 상자를 선택하지 않습니다.
 - 사용자의 이미지를 보려면 **이미지 보기**를 선택합니다. 사용자 이미지 보기에 관한 자세한 내용은 4.1 을 참조하십시오.

4. BioStar 관리하기

- 로그확인을 클릭합니다. 지정한 기간 동안 발생한 이벤트가 표시됩니다.

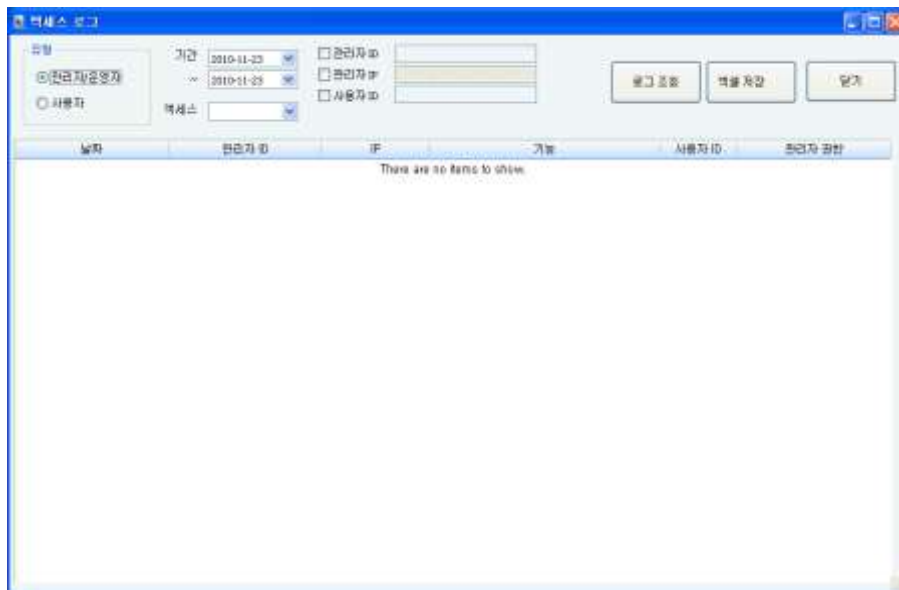


4.2.4 액세스 로그 보기

관리자 메뉴에서 시스템 액세스 로그 및 사용자 수정 이력을 볼 수 있습니다.

액세스 로그 보기

- 메뉴 표시줄에서 관리자 > 액세스 로그를 클릭합니다. 액세스 로그 대화 상자가 나타납니다.



- 관리자 또는 사용자를 클릭하여 선택합니다.
- 기간 상자의 아래 화살표를 클릭하여 달력에서 기간의 첫 날짜와 마지막 날짜를 선택합니다.
- 액세스 드롭다운 목록에서 액세스 종류를 선택합니다.
- 관리자 ID, 관리자 IP 또는 사용자 ID 체크 상자를 선택하여 특정 관리자 또는 사용자를 지정할 수 있습니다.

4. BioStar 관리하기

6. 로그 조회를 클릭하여 지정한 기간 동안의 로그를 조회할 수 있습니다.

날짜	관리자 ID	IP	기능	사용자 ID	관리자 권한
2010-11-23 11:58:14	administrator	192.168.0.246	logout	administrator	Normal User
2010-11-23 11:59:26	admin	192.168.0.246	logout	admin	Administrator
2010-11-23 11:59:34	admin	192.168.0.246	login	admin	Administrator
2010-11-23 13:30:42	admin	192.168.0.246	logout	admin	Administrator
2010-11-23 13:31:04	admin	192.168.0.246	login	admin	Administrator
2010-11-23 13:29:24	admin	192.168.0.246	logout	admin	Administrator
2010-11-23 14:00:56	admin	192.168.0.246	login	admin	Administrator

4.3 비주얼 맵으로 출입문 감시하기

BioStar 는 실제 건물 도면을 이용하여 출입문을 편리하게 감시할 수 있는 기능을 지원합니다. 비주얼 맵을 이용하면 실제 도면을 삽입할 수 있으며, 여기에 출입문을 추가하여 출입문의 상태나 동작(예를 들어, 문 열림, 문 닫힘, 인증 이벤트, 경보 이벤트)을 감시할 수 있습니다. 하나 이상의 도면이 사용된다면 각 도면에 맞추어 비주얼 맵을 추가할 수 있습니다. 비주얼 맵은 BioStar 표준 버전에서만 사용할 수 있습니다.

4.3.1 비주얼 맵 추가하기

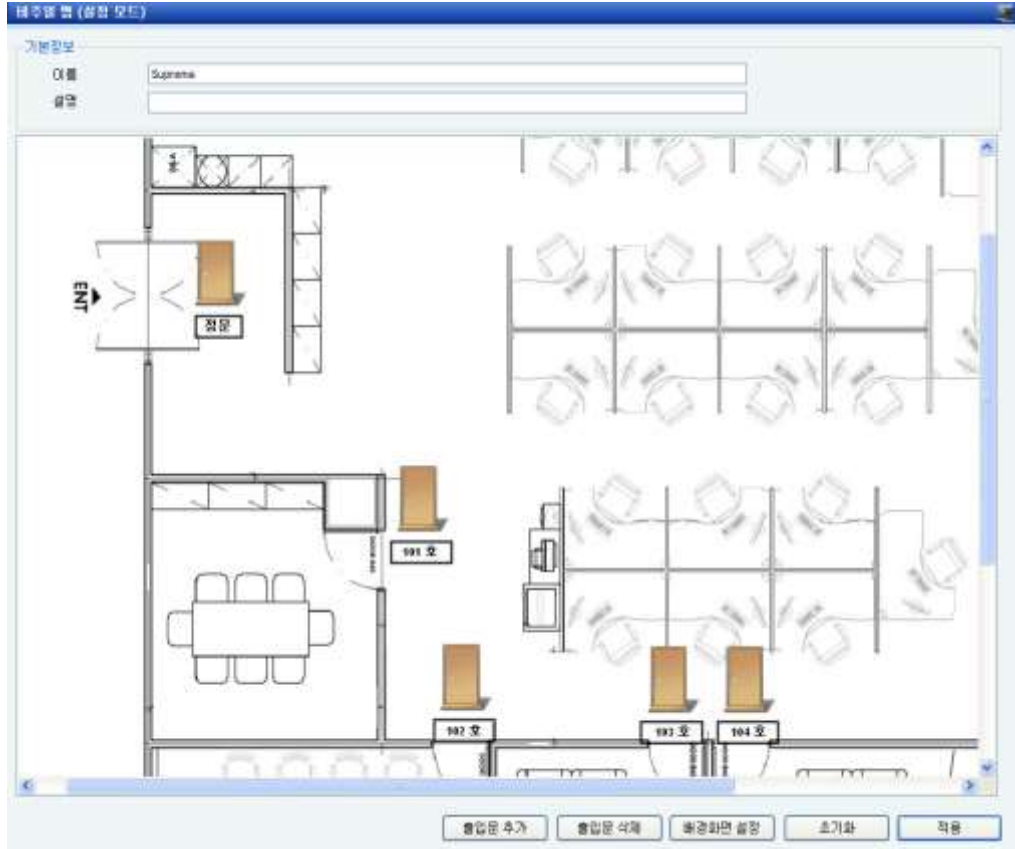
비주얼 맵 설정 모드에서 건물의 도면을 삽입한 후 출입문의 실제 위치에 맞게 도면 위에 출입문을 배치할 수 있습니다.

출입문 배치하기

1. 단축 메뉴 창에서 **비주얼 맵**을 클릭합니다.
2. 작업 창에서 **비주얼 맵 설정**을 클릭합니다.
- 비주얼 맵 창의 제목 표시줄에 **설정 모드**가 표시됩니다.
3. 작업 창에서 **비주얼 맵 추가**를 클릭합니다. 오른쪽에 새 비주얼 맵 창이 열립니다.
4. 비주얼 맵 창에서 새 비주얼 맵의 이름을 입력합니다.
5. 비주얼 맵 창의 아래에 있는 **배경화면 설정**을 클릭하여 도면을 삽입합니다.
730x470 이상의 해상도를 가지는 jpg, bmp, gif, png 형식의 파일만 지원합니다.
6. 이미지를 선택한 후 **열기**를 클릭합니다.
7. **출입문 추가**를 클릭하여 출입문을 추가합니다. 출입문 목록 대화 상자가 나타납니다.

4. BioStar 관리하기

- 출입문 목록에서 추가하려는 출입문 앞에 놓인 체크 상자를 선택한 후 **확인**을 클릭합니다. 출입문이 도면 위에 나타납니다.



- 출입문을 클릭한 후 드래그하여 도면 위의 원하는 위치로 이동합니다. 출입문 아이콘이나 출입문 이름을 두 번 클릭하여 드래그하면 개별적으로 위치를 이동할 수 있습니다.
- 도면에서 출입문을 삭제하려면, 출입문을 클릭한 후 **출입문 삭제**를 클릭합니다.
- 7~10 단계를 반복하여 필요한 출입문을 모두 추가합니다.
- 출입문 추가를 모두 마쳤으면 **적용**을 클릭합니다.
- 도면과 출입문을 모두 삭제하고 처음부터 다시 시작하려면 **초기화**를 클릭합니다.

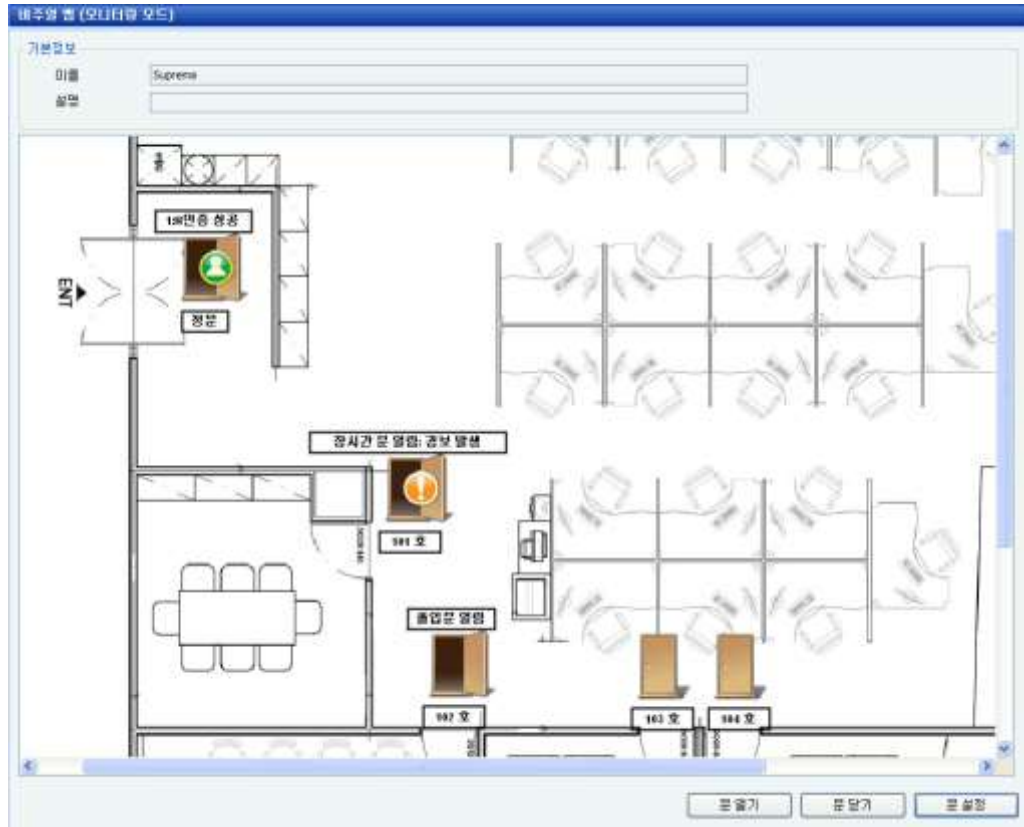
4. BioStar 관리하기

4.3.2 비주얼 맵에서 출입문 감시하기

비주얼 맵 감시 모드에서 도면 위에 배치된 각 출입문의 상태나 동작을 확인할 수 있습니다.








출입문 감시하기

1. 작업 창에서 **비주얼 맵 모니터링**을 클릭합니다. 비주얼 맵 창의 제목 표시줄에 **모니터링 모드**가 표시됩니다.



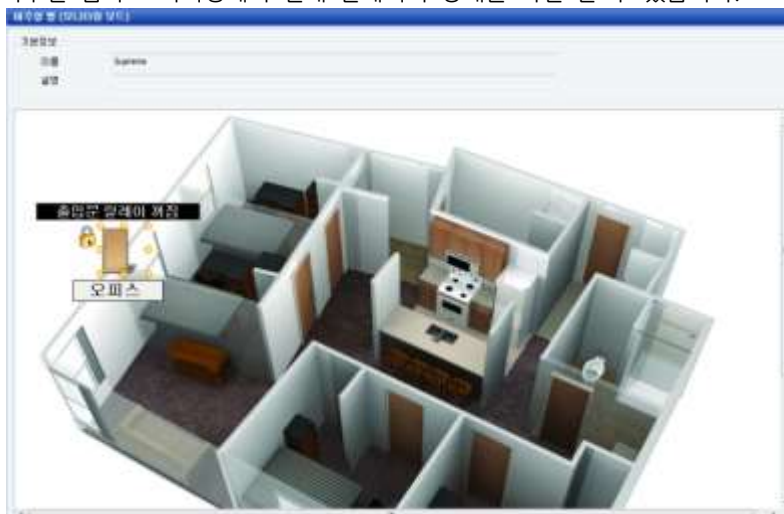
4. BioStar 관리하기

- 다음 아이콘을 참조하여 출입문의 상태나 동작을 감시합니다. 출입문 아이콘 위에 출입문에서 발생한 최종 이벤트(인증, 인증 실패, 경보)가 표시됩니다.

아이콘	표시되는 상황
	출입문이 닫혔을 때 / 출입문 경보가 해제되었을 때
	출입문이 열렸을 때
	출입문이 닫힌 상태에서 인증이 성공했을 때
	출입문이 열린 상태에서 인증이 성공했을 때
	출입문이 닫힌 상태에서 인증이 실패했을 때
	출입문이 열린 상태에서 인증이 실패했을 때
	강제로 출입문이 열렸거나 또는 출입문이 열린 채로 장시간 방치되어 있을 때 / 강제 문열림 경보 또는 장시간 문열림 경보가 발생했을 때

참고: 출입문 아이콘은 출입문 센서가 출입문의 상태를 감지했을 때만 변경됩니다. 즉, 출입문 아이콘은 문 열기 또는 문 닫기 버튼을 눌렀을 때가 아니라 실제로 출입문이 열리거나 닫힐 때 변경됩니다. 이를 위해서는 출입문을 설정할 때 출입문 센서에 대한 입력이 설정되어 있어야 합니다. 출입문 설정에 관한 자세한 내용은 5.2.1 추가정보 탭의 문열림 상태 설정을 참조하십시오.

- 출입문을 열거나 닫으려면 출입문을 클릭한 후 문 열기 또는 문 닫기를 클릭합니다. 출입문의 설정을 변경하려면 출입문을 클릭한 후 문 설정을 클릭합니다.
- 비주얼 맵의 모니터링에서 현재 릴레이의 상태를 확인 할 수 있습니다.



4. BioStar 관리하기

5. 비주얼 맵의 모니터링에서 정보 텍스트 툴팁이 추가되어 출입문의 현재 상태를 확인할 수 있습니다.



6. 비주얼 맵 설정 모드에서 출입문 이름의 폰트 크기를 조절하여 확대하거나 축소하여 표시할 수 있으며, 모니터링에서도 폰트 크기를 조절하여 이벤트 내용을 표시할 수 있습니다.

4.4 출입문, 경보, 장치를 원격으로 제어하기

BioStar 를 이용하면 관리자나 운영자가 출입문, 경보, 장치를 원격으로 제어할 수 있습니다. BioStar 클라이언트가 설치된 연결된 컴퓨터에서 출입문을 열거나 닫을 수 있습니다. 또한 경보를 원격으로 해제할 수 있으며 장치를 잠그거나 장치의 잠금을 해제할 수 있습니다.

4.4.1 출입문을 열거나 닫기

상황에 따라서는 관리자나 운영자가 원격으로 출입문을 열거나 닫아야 할 때가 있습니다. 출입문을 열거나 닫는 방법은 다음과 같습니다.

1. 단축 메뉴 창에서 **실시간 감시**를 클릭합니다.
2. 출입문/구역 탭에 출입문의 이름과 상태가 표시됩니다. 출입문의 상태(열림 또는 닫힘)를 변경하려면, 출입문의 이름을 클릭한 후 **문 열기** 또는 **문 닫기**를 클릭합니다.

또한, 비주얼 맵에서 출입문을 감시하면서 출입문을 열거나 닫을 수 있습니다. 자세한 정보는 4.3.2 를 참조하십시오.

4.4.2 경보 해제하기

어떤 이벤트로 인해 경보가 울릴 때, 관리자나 운영자는 원격으로 이 경보를 해제할 수 있습니다. 경보를 해제하는 방법은 다음과 같습니다.

1. 단축 메뉴 창에서 **실시간 감시**를 클릭합니다.
2. 출입문/구역 탭에 출입문의 이름과 경보 이벤트가 표시됩니다. 경보를 해제하려면, 출입문의 이름을 클릭한 후 **경보 해제**를 클릭합니다.

4. BioStar 관리하기

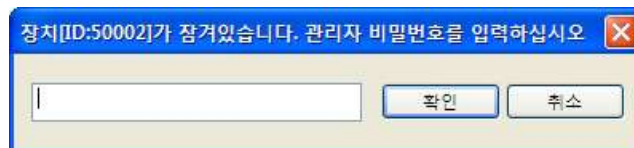
4.4.3 장치를 잠그거나 잠금 해제하기

BioStar 클라이언트를 사용하지 않는 시간에 허락 없이 장치에 접속하는 것을 방지하기 위하여 장치를 잠글 수 있습니다. 수동으로 모든 장치를 잠그거나 또는 BioStar 클라이언트가 종료할 때 자동으로 모든 장치를 잠그도록 설정할 수 있습니다. 그러나 BioStar 서버에 직접 연결된 장치를 잠그거나 잠금을 해제할 수는 없습니다.

4.4.3.1 연결된 장치를 잠그거나 잠금 해제하기

연결된 모든 장치를 잠그기

1. 메뉴 표시줄에서 **옵션 > 장치 > 모든 장치 잠금**을 클릭합니다. 연결된 모든 장치의 잠금을 해제하려면 다음의 절차를 따릅니다.
2. 비밀번호 입력 대화 상자에 비밀번호를 입력한 후 **확인**을 클릭합니다. 잠금 비밀번호를 설정하지 않았다면 바로 **확인**을 클릭합니다. 잠금 비밀번호를 설정하는 방법은 4.3.3.2 를 참조하십시오.

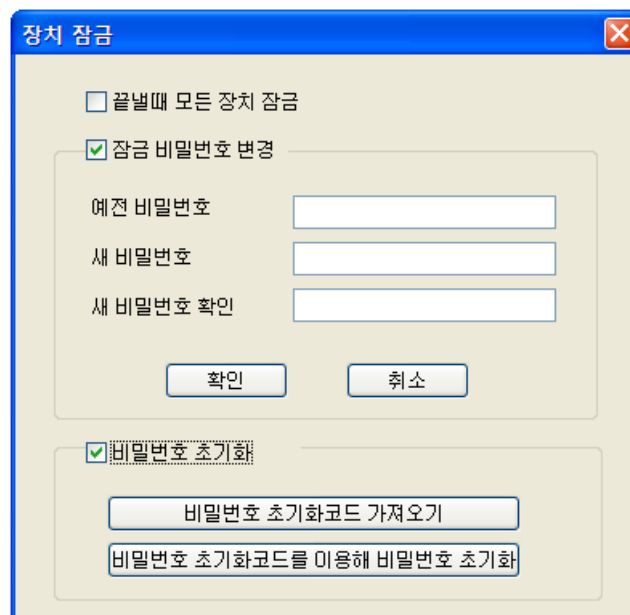


주의: 2.x 장치(BioStation 2, BioStation A2, BioStation L2, BioEntry W2)는 이 기능을 지원하지 않습니다.

4.4.3.2 장치 자동 잠금 설정하기

자동으로 장치 잠그기

1. 메뉴 표시줄에서 **옵션 > 장치 > 장치 잠금**을 클릭합니다. 장치 잠금 대화 상자가 나타납니다.



4. BioStar 관리하기

2. BioStar 를 종료할 때 모든 장치를 잠그려면 **끝낼 때 모든 장치 잠금** 체크 상자를 선택합니다.
3. 필요하다면 **잠금 비밀번호 변경** 체크 상자를 선택합니다.
 - a. 예전 비밀번호를 입력합니다.
 - b. 새 비밀번호를 입력합니다.
 - c. 새 비밀번호를 다시 입력합니다.

주의: 2.x 장치(BioStation 2, BioStation A2, BioStation L2, BioEntry W2)는 이 기능을 지원하지 않습니다.

4.4.3.3 장치 잠금 초기화하기

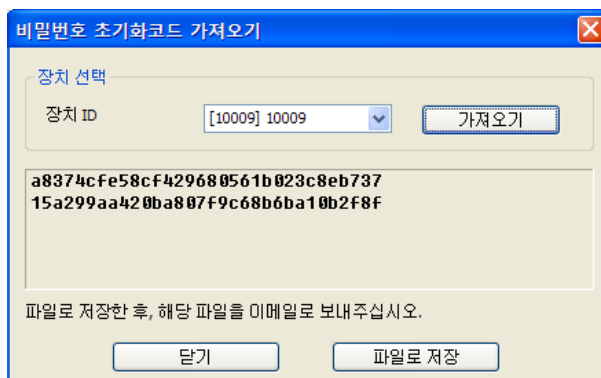
장치의 잠금 비밀번호를 잊어버렸다면, 슈프리마의 기술지원팀이 비밀번호 초기화 코드를 보내줄 수 있습니다.

비밀번호 초기화 코드 요청하기

1. 메뉴 표시줄에서 **옵션 > 장치 > 장치 잠금**을 클릭합니다. 장치 잠금 대화 상자가 나타납니다.



2. 대화 상자의 아래에 있는 **비밀번호 초기화** 체크 상자를 선택합니다.
3. **비밀번호 초기화 코드 가져오기**를 클릭합니다. **비밀번호 초기화 코드 가져오기** 대화 상자가 나타납니다.



4. **장치 ID** 목록 상자에서 장치를 선택합니다.
5. **가져오기**를 클릭합니다.
6. **파일로 저장**을 클릭하여 이 코드를 저장합니다.

4. BioStar 관리하기

- 이 코드를 이메일에 첨부하여 슈프리마(support@supremainc.com)에 보냅니다. 슈프리마의 기술지원 담당자로부터 비밀번호 초기화 코드를 메일로 전송 받습니다.
- 비밀번호 초기화 코드를 받으면, 장치 잠금 대화 상자를 연 후, **비밀번호 초기화** 체크 상자를 선택합니다.
- 비밀번호 초기화 코드를 이용해 비밀번호 초기화**를 클릭합니다. 비밀번호 초기화 대화 상자가 나타납니다.



- 초기화 코드 파일 열기를 클릭한 후 슈프리마로부터 받은 파일을 선택합니다.
- 파일을 연 후, **쓰기**를 클릭합니다. 장치의 잠금 비밀번호가 초기화(비밀번호 없음)됩니다.

주의: 2.x 장치(BioStation 2, BioStation A2, BioStation L2, BioEntry W2)는 이 기능을 지원하지 않습니다.

4.5 사용자 관리하기

BioStar 를 이용하면, 사용자를 삭제하거나 사용자를 다른 부서로 이동하거나 사용자 정보 항목을 임의로 변경할 수 있습니다. 또한 보고서 일괄 편집 또는 기타 다른 목적을 위하여 사용자 데이터를 내보내거나 가져올 수 있습니다.

4.5.1 사용자 삭제하기

필요한 경우 BioStar 시스템에서 사용자를 손쉽게 삭제할 수 있습니다.

사용자 삭제하기

- 단축 메뉴 창에서 **사용자**를 클릭합니다.
- 사용자의 이름을 마우스 오른쪽 버튼으로 클릭합니다.
- 사용자 삭제**를 클릭합니다.
- 예**를 클릭합니다.

4.5.1.1 커맨드 카드를 이용하여 개별 사용자 삭제하기

커맨드 카드를 가지고 있다면 BioEntry Plus, BioEntry W, Xpass 및 Xpass S2 장치에서 직접 개별 사용자를 삭제할 수 있습니다. 커맨드 카드 발급에 관한 자세한 내용은 3.2.6.1 과 3.2.8.1 을 참조하십시오.

BioEntry Plus 및 BioEntry W 장치에서 커맨드 카드를 이용하여 사용자를 삭제하려면 다음의 절차를 따릅니다.

4. BioStar 관리하기

1. 삭제 카드(커맨드 카드)를 BioEntry Plus 또는 BioEntry W 장치에 가까이 가져갑니다.
2. 인증이 필요하다면, 관리자가 자신의 지문으로 인증을 받아야 계속 진행할 수 있습니다.
3. 삭제하려는 사용자의 출입 카드를 장치에 댄 후 (장치의 요청에 따라) 사용자의 지문을 입력하게 합니다.

Xpass 및 Xpass S2 장치에서 커맨드 카드를 이용하여 사용자를 삭제하려면 다음의 절차를 따릅니다.

1. 삭제 카드(커맨드 카드)를 Xpass 나 Xpass S2 장치에 댕니다.
2. 인증이 필요하다면, 관리자가 자신의 카드로 인증을 받아야 계속 진행할 수 있습니다.
3. 삭제하려는 사용자의 출입 카드를 장치에 댕니다.
4. 삭제 카드(커맨드 카드)를 장치에 다시 한번 댕니다.

4.5.1.2 커맨드 카드를 이용하여 모든 사용자 삭제하기

커맨드 카드를 가지고 있다면 BioEntry Plus, BioEntry W, Xpass 및 Xpass S2 장치에서 직접 모든 사용자를 삭제할 수 있습니다. 커맨드 카드 발급에 관한 자세한 내용은 3.2.6.1 과 3.2.8.1 을 참조하십시오.

BioEntry Plus 및 BioEntry W 장치에서 커맨드 카드를 이용하여 모든 사용자 삭제하려면 다음의 절차를 따릅니다.

1. 모두 삭제 카드(커맨드 카드)를 BioEntry Plus 또는 BioEntry W 장치에 가까이 가져갑니다.
2. 인증이 필요하다면, 관리자가 자신의 지문으로 인증을 받아야 계속 진행할 수 있습니다.
3. 모두 삭제 카드를 장치에 다시 한번 댕니다.

Xpass 및 Xpass S2 장치에서 커맨드 카드를 이용하여 모든 사용자 삭제하려면 다음의 절차를 따릅니다.

1. 모두 삭제 카드(커맨드 카드)를 Xpass 나 Xpass S2 장치에 댕니다.
2. 인증이 필요하다면, 관리자가 자신의 카드로 인증을 받아야 계속 진행할 수 있습니다.
3. 모두 삭제 카드를 장치에 다시 한번 댕니다.

4.5.2 사용자를 다른 부서로 이동하기

다른 부서로 사용자 이동하기

1. 단축 메뉴 창에서 **사용자**를 클릭합니다.
2. 탐색 창에서 부서 최상위 단계인 **사용자**를 마우스 오른쪽 버튼으로 클릭합니다.
3. **부서 추가**를 클릭합니다.
4. 부서의 이름을 입력합니다.
5. 이동하고자 하는 사용자를 원하는 부서에 끌어다 놓습니다.

참고: 부서는 최대 4 개의 단계까지 추가할 수 있습니다.

4. BioStar 관리하기

4.5.3 사용자 정의 항목 설정하기

BioStar에서는 사용자의 정보 항목을 임의로 변경할 수 있습니다. 이것을 이용하면 사용자 정보의 기본 항목을 변경하거나 새로운 정보 항목을 추가할 수 있습니다.

4.5.3.1 새로운 정보 항목 추가하기

새로운 정보 항목 추가하기

1. 메뉴 표시줄에서 **옵션 > 사용자 > 사용자 정의 항목 설정**을 클릭합니다. **사용자 정의 항목 설정** 대화 상자가 나타납니다.

순서	항목명	형식	자료
1	ID	Edit	
2	시작일	날짜	
3	만료일시	날짜	
4	인증 모드	콤보박스	
5	직급	콤보박스	순남;사장;부장;차장;과장;대리;사원
6	핸드폰번호	Edit	
7	성별	콤보박스	남자;여자
8	성명	날짜	

2. **순서** 상자의 아래 화살표를 클릭하여 목록에서 이 항목이 표시되는 순서를 선택합니다. 사용하고 있지 않은 번호를 선택하십시오.
3. **형식** 목록 상자에서 항목의 형식을 선택합니다. 숫자만 입력할 수 있도록 하려면 **숫자만** 체크 상자를 선택합니다.
4. **항목자료** 상자에 항목의 자료(예를 들어, 콤보 박스에 표시될 여러 설정 값)를 입력하고, **항목명** 상자에 항목의 이름을 입력합니다.
5. **추가**를 클릭합니다.
6. 더 추가할 정보 항목이 있다면 2~5 단계를 반복합니다.
7. 설정을 마치면, **저장**을 클릭합니다.

4.5.3.2 기존 정보 항목 편집하기

기존 정보 항목 편집하려면 다음의 절차를 따릅니다.

1. 메뉴 표시줄에서 **옵션 > 사용자 > 사용자 정의 항목 설정**을 클릭합니다. 사용자 정의 항목 설정 대화 상자가 나타납니다(4.5.3.1 참조).
2. 목록에서 수정할 항목을 클릭합니다. 선택한 항목의 내용이 대화 상자의 윗부분에 표시됩니다.

4. BioStar 관리하기

참고: 1~4 번 항목은 필수 항목이며, 수정 및 삭제가 불가능합니다.

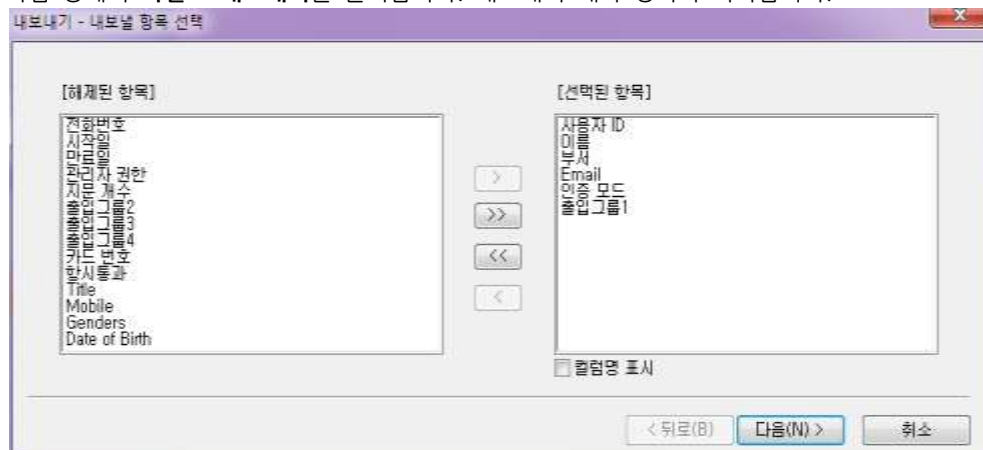
3. 필요에 맞게 데이터를 수정합니다.
4. 수정을 클릭합니다.
5. 더 수정할 정보 항목이 있다면 2~4 단계를 반복합니다.
6. 저장을 클릭합니다.

4.5.4 사용자 데이터 내보내기

사용자 데이터를 내보낼 때 사용하는 파일 형식은 CSV 이며, 이 파일은 텍스트 에디터나 MS 엑셀로 편집할 수 있습니다.

사용자 데이터 내보내기

1. 단축 메뉴 창에서 **사용자**를 클릭합니다.
2. 작업 창에서 **파일로 내보내기**를 클릭합니다. 내보내기 대화 상자가 나타납니다.



3. 해제된 항목 목록에서 파일로 내보낼 데이터 항목을 클릭한 후 > 버튼을 클릭합니다.
4. 선택 사항: 파일에서 데이터를 칼럼명과 함께 표시하려면, [선택된 항목] 아래에 있는 칼럼명 표시 체크 박스를 선택합니다.
5. 내보낼 데이터를 선택했다면, 다음을 클릭합니다.
6. 파일을 저장할 경로와 파일 이름을 파일 필드에 직접 입력하거나 또는 파일 선택을 클릭한 후 파일을 저장할 장소와 이름을 지정합니다.
7. 다음을 클릭합니다.
8. 내보내기를 클릭합니다.
9. 내보내기가 완료되면, 마침을 클릭합니다.

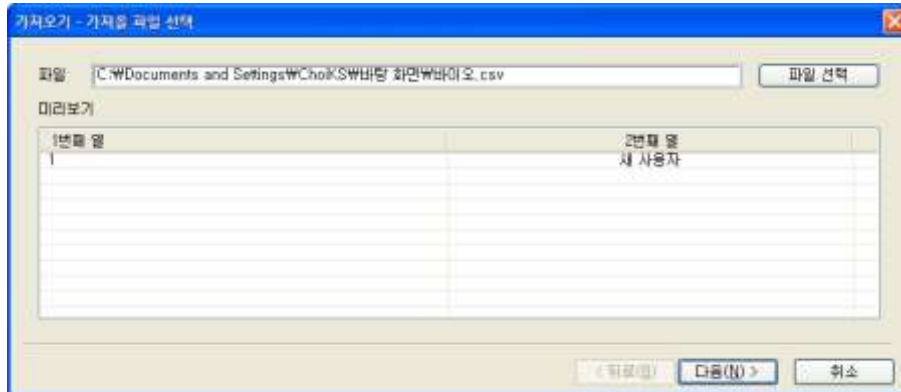
4. BioStar 관리하기

4.5.5 사용자 데이터 가져오기

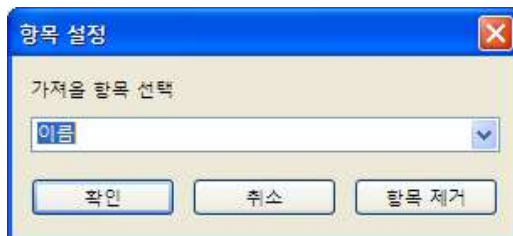
CSV 형식으로 된 사용자 데이터를 BioStar 로 가져올 수 있습니다.

사용자 데이터 가져오기

1. 단축 메뉴 창에서 **사용자**를 클릭합니다.
2. 작업 창에서 **파일에서 가져오기**를 클릭합니다. 가져오기 대화 상자가 나타납니다.



3. 사용자 데이터가 저장된 파일의 경로와 이름을 파일 필드에 직접 입력하거나 또는 **파일 선택**을 클릭한 후 파일의 경로와 이름을 선택한 후 **열기**를 클릭합니다.
4. **다음**을 클릭합니다. 각 데이터 값이 목록에 표시되고, 사용자 정보 항목의 값은 기본적으로 **사용 안함**으로 설정되어 있습니다.
5. 사용자 정보 항목 옆에 있는 셀을 클릭합니다. **항목 설정** 대화 상자가 나타납니다.



6. 아래 회살표를 클릭하여 목록에서 데이터 값을 어떤 필드 이름 아래에 둘 것인지 선택한 후 **확인**을 클릭합니다.

참고: BioStar 에서는 최대 4 개의 부서 계층이 표시 됩니다. CSV 파일에서는 슬래시('/')를 사용하여 부서 계층을 구분합니다.

7. 5~6 단계를 반복하여 각 데이터 값을 어떤 필드 이름 아래에 둘 것인지 설정합니다.
8. 데이터 값과 필드 이름을 모두 연결했다면 **다음**을 클릭합니다.
만약 BioStar 에서 내보내기를 한 CSV 칼럼 형식이 변경되지 않았다면, **자동선택** 버튼을 사용하면 순차적으로 자동 연결을 해주기 때문에 5~7 단계를 생략할 수 있습니다.
9. **가져오기**를 클릭합니다.
10. 데이터 값을 기존의 계정에 있는 필드 이름에 연결했다면, BioStar 가 기존의 데이터에 덮어쓸 것인지 묻습니다. 덮어쓰려면 **예** 또는 **모두 예**를 클릭하고, 덮어쓰지 않으려면 **아니오** 또는 **모두 아니오**를 선택합니다.
11. **마침**을 클릭합니다.

4. BioStar 관리하기

4.6 근태 관리하기

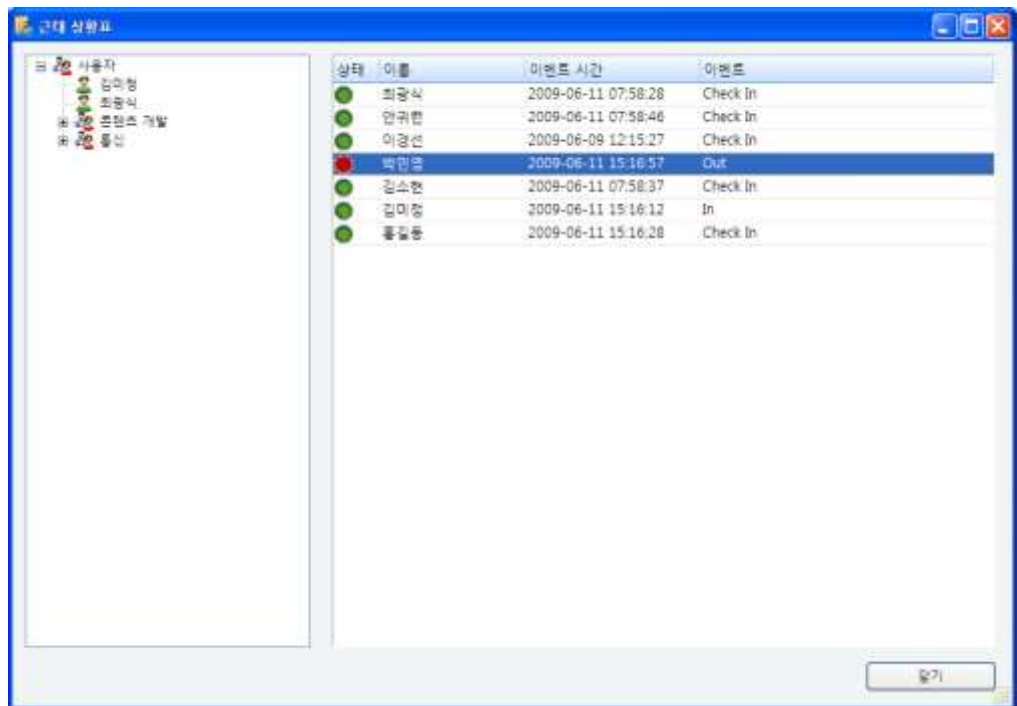
BioStar 를 이용하면 사용자들의 근태 상황을 관리 감독할 수 있으며 근태 보고서를 생성하여 이를 수정하거나 다른 파일로 저장할 수 있습니다.

4.6.1 근태 상황 확인하기

근태 상황표는 사용자의 최후 근태 이벤트를 표시합니다. 근태 상황표를 이용하면 최근에 일어난 근태 이벤트를 확인할 수 있으며, 사용자들의 출결 상태를 한눈에 알아볼 수 있습니다. 근태 상황표에 표시되는 사용자들의 출입 상태는 슈프리마 출입통제 단말기의 근태기능을 이용해야만 올바르게 표시됩니다.

근태 상황 확인하기

1. 단축 메뉴 창에서 **근태**를 클릭합니다.
2. 작업 창에서 **근태 상황표**를 클릭합니다. **근태 상황표** 창이 열립니다.



3. 왼편의 목록에서 **사용자** 또는 부서의 이름이나 사용자의 이름을 클릭합니다. 선택한 항목에 따라 모든 사용자의 출결 상태, 부서에 속한 모든 사용자의 출결 상태, 또는 한 개인의 출결 상태가 오른편에 목록에 표시됩니다.
4. 확인을 마치면 **닫기**를 클릭합니다.

참고: 근태 상황표는 BioStar 표준 버전에서만 지원됩니다.

4. BioStar 관리하기

4.6.2 근태 보고서 생성하기

근태 보고서를 생성하면 BioStar 시스템을 통해 수집된 사용자들의 모든 근태 이벤트를 확인할 수 있습니다. 이렇게 생성된 근태 결과를 최종적으로 수정하거나 인쇄하여, 급료를 계산하는 것과 같이 여러 목적에 맞게 활용할 수 있습니다.

근태 보고서 생성하기

1. 단축 메뉴 창에서 근태를 클릭합니다.
2. 작업 창에서 보고서를 클릭합니다. 보고서 창이 열립니다.



3. 보고서 종류 영역에서 보고서의 종류를 선택합니다.
 - 일일 보고서: 날짜별로 근태 이벤트에 대한 보고서를 생성합니다.
 - 개인별 보고서: 사용자 ID 별로 근태 이벤트에 대한 보고서를 생성합니다.
 - 결과 보고서: 근태 결과의 종류를 목록에서 선택하여 해당 결과만 포함하는 근태 이벤트를 표시합니다.
 - 보고서 변경 이력: 편집된 항목만 표시합니다.
 - 일일 집계 보고서: 날짜별로 근태 결과를 집계하여 근무 종류별 근무 시간, 총 근무 시간, 근태 결과별 사용자의 수를 간략하게 표시합니다.
 - 종합 보고서: 사용자별로 근태 이벤트를 집계하여 근태 이벤트의 발생시간, 각 이벤트의 발생 횟수, 근무 시간 등을 간략하게 표시합니다.

참고: 일일 보고서와 개인별 보고서에서 hh:mm(명) 또는 hh:mm(일) 등 표시 값의 (명)/(일) 부분을 생략하고 hh:mm 형식으로 간략하게 표시하려면, 옵션 > 근태 > 포맷을 클릭한 후, 명/일 표시를 클릭하십시오.

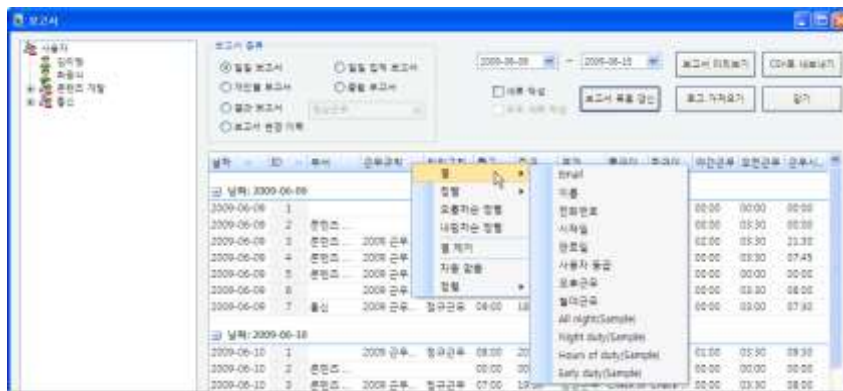
4. BioStar 관리하기

- Option 영역에서 세부 옵션을 설정합니다.
 - 명/날짜 표시: 보고서 데이터에 '명/날짜'를 표시할지 여부를 선택합니다.
 - 시간 형식(1.0h): 시간을 10 진법으로 표시합니다. 예를 들어, '1 시간 7 분'을 10 진법으로 변환하면 '1.11'로 표시됩니다.
 - In/Out 보고서: 인증을 하고 출입한 기록을 10 회까지 표시합니다.
 - 용지 크기: A4 와 Letter 크기의 용지를 지원합니다.
- 오른쪽 상단에서 근태 데이터의 날짜의 범위를 입력합니다.
- 보고서 목록 갱신을 클릭합니다. 근태 데이터가 표시됩니다.

데이터의 제목 행을 클릭하면 데이터 값의 정렬 순서를 바꿀 수 있습니다. 데이터 열의 제목 행을 클릭한 채로 이동하면 데이터 열의 위치를 바꿀 수 있습니다. 데이터의 제목 행을 마우스 오른쪽 버튼으로 클릭하면 메뉴가 나타나는데, 이 메뉴를 이용하여 데이터 열을 추가하거나 제거할 수 있으며 데이터의 정렬 순서를 바꿀 수 있습니다.

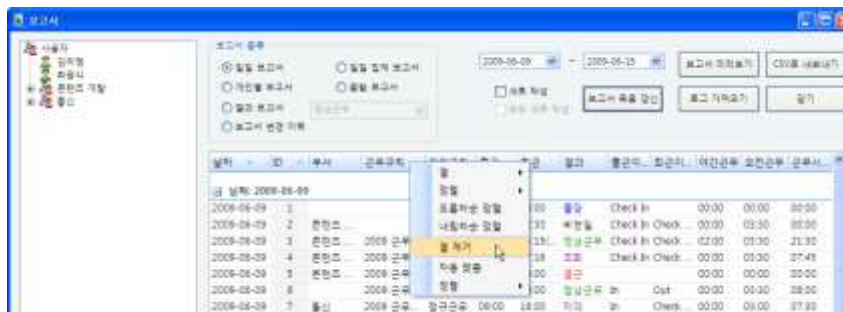
근태 보고서에 데이터 열 추가하기

- 데이터 열의 제목 행을 마우스 오른쪽 버튼으로 클릭합니다.
- 열을 클릭한 후 서브메뉴 목록에서 추가하려는 데이터 열을 클릭합니다.



근태 보고서에서 데이터 열 삭제하기

- 제거하기를 원하는 데이터 열의 제목 행을 마우스 오른쪽 버튼으로 클릭합니다.
- 열 제거를 클릭합니다.



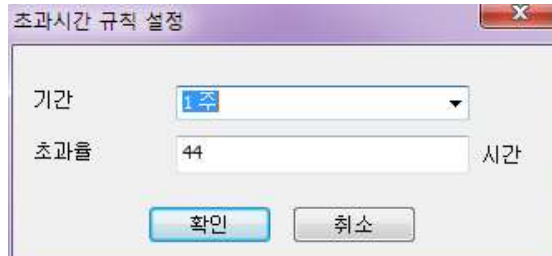
참고: 로그 가져오기를 클릭하면 BioStar 시스템에 연결된 장치로부터 데이터를 수집합니다. 보고서 목록 갱신을 클릭하면 수정한 데이터를 원래 상태로 복구합니다. 수정한 데이터 복구에 관한 자세한 내용은 4.5.3 을 참조하십시오.

4. BioStar 관리하기

보고서에서 초과 근무 시간 표시하기

사용자가 지정된 시간을 초과하여 근무한 경우, 보고서에서 연장 근무한 시간을 확인할 수 있습니다. 정규 근무 시간으로 인정하는 시간을 주 단위(1 주, 2 주, 4 주)로 지정할 수 있습니다.

1. **옵션 > 근태 > 초과시간 규칙 설정**을 클릭합니다. **초과시간 규칙 설정** 대화 상자가 나타납니다.



2. **기간** 목록 상자에서 기준이 되는 기간을 선택합니다.
3. **초과율** 필드에서 기간에 해당하는 정규 근무 시간을 입력합니다. 이 시간을 초과하여 근무한 사용자가 있다면, 보고서에서 초과로 근무한 시간을 확인할 수 있습니다.
4. **확인**을 클릭합니다.

참고: 보고서에서 초과 근무 시간을 정상적으로 표시하려면 기간을 설정할 때 시작일을 일요일로 선택해야 합니다.

4.6.3 근태 보고서 수정하기

근태 결과 보고서나 급여 계산을 위한 목적으로 관리자나 운영자는 근태 이벤트 데이터를 수정할 수 있습니다. 근태 이벤트 데이터를 수정할 수 있는 방법에는 2 가지가 있습니다. 첫 번째는 근태 보고서의 데이터 셀을 클릭한 후 원하는 값을 입력하여 수정하는 방법입니다. 이 방법은 보고서에 표시되는 데이터를 수정하는 것으로 출입통제 단말기에서 수집한 데이터 자체가 수정되지는 않습니다. 이렇게 수정된 데이터는 근태 보고서에서 회색으로 표시되며, 원래 데이터로 복구하려면 **새로 작성** 체크 상자를 선택한 후 **보고서 목록 갱신**을 클릭합니다.

두 번째 방법은 각 단말기에서 가져온 데이터를 수정하는 방법입니다. 이러한 수정 방법을 상세 편집이라 합니다. 이 방법으로 수정한 데이터는 모두 **새로 작성** 체크 상자(**새로 작성** 체크 상자를 선택해야 선택 가능)를 클릭한 후, **보고서 목록 갱신**을 클릭하여 원래 상태로 복구할 수 있습니다.

4. BioStar 관리하기

이벤트 데이터 편집하기

1. 4.5.2의 설명을 따라 근태 보고서를 생성합니다.
2. 데이터 셀을 마우스 오른쪽 버튼으로 클릭한 후 **상세 편집**을 클릭합니다. **상세 편집** 대화 상자가 나타납니다.

The dialog box titled '상세 편집' (Detailed Edit) contains the following information:

기준날짜	2009-06-09	이름	이경선
사용자 ID	3	결과	정상근무

이벤트 날짜	이벤트 시간	이벤트	장치
2009-06-09	08:15:27	Check In	12641[61.83.152....
2009-06-10	05:15:27	Check Out	12641[61.83.152....

이벤트 속성

날짜	당일	시간	오후 4:00:00
이벤트	Check In	장치	12641[61.83.152

이 설정을 변경한 뒤에 '모두 새로 작성'을 체크하게 되면 수정한 내용이 초기화 됩니다.

Buttons: 이벤트 추가, 이벤트 수정, 이벤트 삭제

3. 이벤트를 수정하려면, 목록에서 수정하려는 이벤트를 선택한 다음 **이벤트 속성** 영역에서 각 항목을 수정한 후 **이벤트 수정**을 클릭합니다. 이벤트를 추가하려면, **이벤트 속성** 영역에서 각 항목을 입력한 후 **이벤트 추가**를 클릭합니다. 이벤트를 삭제하려면, 목록에서 삭제하려는 이벤트를 선택한 후 **이벤트 삭제**를 클릭합니다.
 - **날짜**: 이벤트가 발생한 날(당일, 명일)을 선택합니다.
 - **이벤트**: 이벤트의 종류를 선택합니다.
 - **시간**: 이벤트가 발생한 시간을 입력합니다.
 - **장치**: 이벤트가 발생한 단말기를 선택합니다.
4. 수정을 마치면 오른쪽 상단의 나가기 버튼(X)를 클릭하여 **상세 편집** 대화 상자를 닫습니다.
5. **상세 편집** 대화 상자를 닫으면 수정 사항이 근태 보고서에 반영됩니다.

참고: 근태 보고서 화면에서 데이터의 제목 행을 클릭하면 데이터 값의 정렬 순서를 바꿀 수 있습니다. 데이터 열의 제목 행을 클릭한 채로 이동하면 데이터 열의 위치를 바꿀 수 있습니다.

4.6.4 근태 보고서 인쇄 및 내보내기

근태 보고서 인쇄 또는 내보내기

1. 4.5.2의 설명을 따라 근태 보고서를 생성합니다.
2. 필요하다면 4.5.3의 설명을 따라 보고서의 데이터를 수정합니다.

4. BioStar 관리하기

3. 보고서 미리보기를 클릭합니다. 미리보기 창이 나타납니다.

2009-06-08												
번호	이름	부서	근무규격	출발규격	출근	퇴근	결과	출근(연속)	퇴근(연속)	대조근무	오전근무	근무시간
1	최영식		2019 근무일	DailySchedule13:10	14:02		결근	Check In		00:00	00:00	00:00
2	안규현	문안초	2019 근무일	DailySchedule14:02	00:00		결근			00:00	00:00	00:00
3	이정선	문안초	2019 근무일	DailySchedule14:02	00:00		결근			00:00	00:00	00:00
4	박한영	문안초	2019 근무일	DailySchedule14:02	00:00		결근			00:00	00:00	00:00
5	김소현	문안초	2019 근무일	DailySchedule14:02	00:00		결근			00:00	00:00	00:00
6	김지영		08:00	00:00			복원일			00:00	00:00	00:00
7	홍길동	통산	2019 근무일	정유근무	08:00	00:00	결근			00:00	00:00	00:00

4. 보고서를 인쇄하려면 도구표시줄의 보고서 인쇄 아이콘을 클릭합니다.
5. 보고서 데이터를 다른 파일로 내보내려면, 도구표시줄의 보고서 내보내기 아이콘을 클릭합니다. 다음과 같은 형식의 파일로 저장할 수 있습니다.
- Adobe Acrobat (PDF)
 - Crystal Report (RPT)
 - HTML 3.2 또는 4.0
 - Microsoft Excel 97-2000 (XLS)
 - Microsoft Excel 97-2000 -데이터에 한함 (XLS)
 - Microsoft Word (RTF)
 - Microsoft Word - 편집가능(RTF)
 - ODC
 - XML
 - 구분된 값 (CSV)
 - 레코드 스타일 - 공백 없는 열(REC)
 - 레코드 스타일 - 공백 포함 열(REC)
 - 보고서 정의(TXT)
 - 서식 있는 텍스트 형식(RTF)
 - 탭으로 구분된 텍스트(TTX)
 - Text (TXT)

참고: 도구표시줄의 검색 아이콘(쌍안경)을 클릭하여 원하는 단어를 보고서에서 검색할 수 있습니다.

4. BioStar 관리하기

4.7 장치 관리하기

필요하다면, BioStar 시스템에서는 장치를 손쉽게 제거할 수 있으며, BioStar 프로그램에서 장치의 펌웨어를 직접 교체할 수 있습니다. 장치를 제거할 때에는 제거하려는 장치에 새로운 정보가 있는지 확인하고, 있다면 먼저 BioStar 서버에 이 정보를 전송합니다.

4.7.1 장치 제거하기

BioStar 시스템에서 장치를 제거하려면, 단축 메뉴 창에서 **장치**를 클릭합니다. 그런 다음 장치의 이름을 마우스 오른쪽 버튼으로 클릭한 후 **장치 제거**를 클릭합니다.

4.7.2 장치의 펌웨어 업그레이드하기

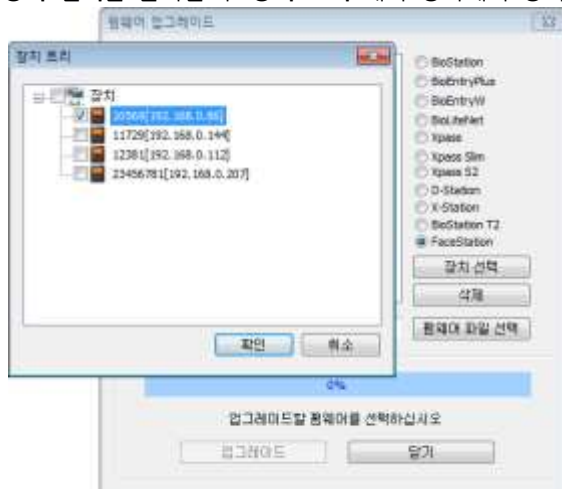
때때로 장치의 펌웨어를 최신의 펌웨어로 업그레이드할 필요가 있습니다.

펌웨어 업그레이드하기

1. 메뉴 표시줄에서 **옵션 > 장치 > 펌웨어 업그레이드**를 클릭합니다.



2. 펌웨어 업그레이드 대화 상자가 나타납니다.
3. 펌웨어를 업그레이드하려는 장치의 종류 버튼을 선택합니다.
4. 장치 선택을 클릭한 후 장치 트리 대화 상자에서 장치를 선택합니다.



5. 확인을 클릭하여 장치 트리 대화 상자를 닫습니다.
6. 펌웨어 파일 선택을 클릭합니다.

4. BioStar 관리하기

7. 펌웨어 파일을 선택한 후 열기를 클릭합니다.
8. 업그레이드를 클릭합니다.
9. 펌웨어 업그레이드가 완료되면, 장치가 재시동될 때까지 기다렸다가 닫기를 클릭합니다.

4.7.3 장치 펌웨어 다운그레이드하기

장치의 펌웨어를 현재 버전보다 낮은 버전의 펌웨어로 교체하면 장치가 올바르게 작동하지 않을 수 있습니다. 장치의 펌웨어를 다운그레이드하기 전에 슈프리마 기술지원팀(support@suprema.co.kr), 제품 공급사, 제품 판매처에 반드시 문의하시기 바랍니다.

4.8 지문 암호화 사용하기

기본적으로 지문 암호화 옵션은 꺼져 있습니다. 대부분의 경우 암호화 옵션을 사용할 필요가 없습니다. 그러나 보안을 좀더 강화하려 한다면 암호화 옵션을 사용할 수도 있습니다. 지문 암호화 옵션을 사용하면 암호화 키를 관리해야 하기 때문에, 고급 사용자가 실행하는 것이 좋습니다.

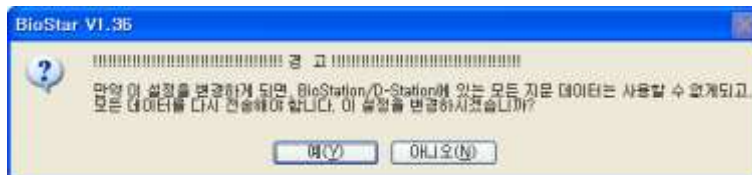
지문 암호화를 실행하면, 모든 지문 템플릿은 암호화되어 전달되고 저장됩니다. BioStar 는 3 종류의 지문 템플릿(슈프리마 고유 형식, ISO 19794-2 형식, ANSI378 형식)을 사용합니다. 지문 암호화를 실행하면 이전에 저장된 모든 템플릿은 더 이상 사용할 수 없습니다. 그렇기 때문에 사용자를 등록하기 전에 암호화를 실행하는 것이 좋습니다.

암호화 실행하기

1. 메뉴 표시줄에서 **옵션 > 지문**을 클릭합니다. **지문 설정** 대화 상자가 나타납니다.



2. 지문 설정 영역에서 **바이오 정보 보호 가이드 적용** 체크 상자를 선택합니다. 경고 메시지가 나타납니다.



3. **예**를 클릭하여 경고를 수락합니다.

4. BioStar 관리하기

- 2 단계에서 슈프리마 고유 형식(지문 템플릿 암호화)를 선택했다면 지문 암호화 키를 변경할 수 있습니다.

- 지문 암호화 키 변경을 클릭합니다. 암호화 키 변경 대화 상자가 나타납니다.



- 새 암호화 키 상자에 새 암호화 키를 입력합니다.
 - 새 암호화 키 확인 상자에 키를 한 번 더 입력합니다.
 - 변경을 클릭합니다.
- 저장을 클릭합니다. 장치 창의 지문 탭에서 변경된 옵션을 확인할 수 있습니다.

4.9 지문 템플릿 형식 변경하기

BioStar 는 3 종류의 지문 템플릿 형식(슈프리마 고유 형식, ISO 19794-2 형식, ANSI378 형식)을 지원합니다. 기본적으로 슈프리마 고유 형식이 사용됩니다. 지문 형식 옵션을 변경하면 이전에 저장된 모든 지문을 사용할 수 없게 됩니다. 그러므로 사용자의 지문을 등록하기 전에 지문 형식 옵션을 미리 선택해 두는 것이 좋습니다.

주의: 사용자 지문 포맷 변경 및 암호화는 사용자 지문 등록 전에 설정해야 합니다. 만약 지문 등록된 상태에서 지문 포맷 변경 및 암호화 작업을 수행하는 경우에는 반드시 사용자 설정 화면을 모두 닫은 상태에서 진행하십시오. 또한, 사용자 설정화면이 선택된 상태에서 변경한 경우에는 BioStar Client 를 반드시 재시작하고 사용하시기 바랍니다.

지문 형식 옵션 변경하기

- 메뉴 표시줄에서 **옵션 > 지문**을 클릭합니다. 지문 설정 대화 상자가 나타납니다.
- 슈프리마 고유 형식을 사용하려면 **바이오 정보 보호 가이드 적용**을, ISO 19794-2 형식을 사용하려면 **ISO 템플릿 형식 사용(SIF)**을, ANSI378 형식을 사용하려면 **ANSI 템플릿 형식 사용**을 선택합니다.
- 경고문을 읽은 후 계속하려면 **예**를 클릭합니다.
- 저장**을 클릭합니다.

사용자 설정

이 장에서는 BioStar 소프트웨어에서 사용할 수 있는 설정에 대해서 설명합니다. BioStar 를 이용하면 장치의 기능, 출입문과 구역, 사용자 계정의 설정을 변경하여 출입 통제 시스템을 좀더 정밀하게 제어할 수 있으며 상황에 따라 설정을 변경할 수도 있습니다.

5.1 장치 설정 변경하기

BioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, Xpass S2 및 X-Station 의 설정은 기본적으로 거의 비슷하며 기능에 따라 약간 다릅니다. BioStation 2, BioStation A2, BioStation L2, BioEntry W2 는 BioStar 2 를 기본으로 지원하는 장치이며, BioStar 2 와 설정이 다를 수 있습니다.

이 절에서는 이 장치들을 설정하는 방법에 대해서 각각 따로 설명할 것입니다. 아래에서 설명하는 탭을 화면에 띄우려면 단축 메뉴 창의 **장치**를 클릭한 후 장치의 이름을 클릭해야 합니다.

5.1.1 BioStation 설정 변경하기

이 절에서는 BioStation 에서 사용할 수 있는 설정에 대해서 설명합니다. 이러한 설정을 변경하여 현재 처해있는 상황이나 운영상의 필요에 맞게 BioStation 의 기능을 변경하시기 바랍니다.

5. 사용자 설정

5.1.1.1 동작모드 탭

동작모드 탭에서 BioStation 의 시간을 변경할 수 있으며 동작 모드와 관련된 다양한 설정을 변경할 수 있습니다.



- **BioStation 시간**
 - 날짜: 장치에서 표시할 날짜를 직접 설정합니다.
 - 시간: 장치에서 표시할 시간을 직접 설정합니다.
 - 현재 PC 시간으로 동기화: BioStar 클라이언트 프로그램이 설치되어 있는 로컬 PC 의 날짜와 시간을 가져와 바로 아래 날짜와 시간 스피너 상자에 표시합니다. 시간 적용을 클릭하면, 장치의 날짜와 시간이 로컬 PC 의 날짜와 시간으로 설정됩니다.
 - 시간 가져오기: 현재 장치에서 표시되고 있는 시간을 가져옵니다.
 - 시간 적용: 장치의 시간을 설정한 시간으로 변경합니다.
- **1:1 동작 모드 설정:** 이 영역에서는 일정에 따라 각각 다른 인증 모드가 적용되도록 설정할 수 있습니다. 예를 들어, 근무 시간에는 일반적인 인증 모드를 적용하고 근무 시간 이외에는 좀더 엄격한 인증모드를 적용할 수 있습니다. 장치에 설정된 인증 모드를 적용할지 아니면 개별 사용자에게 설정된 인증 모드를 적용할지도 여기에서 설정할 수 있습니다(5.4.1 참조). 사용자의 인증 모드를 개별적으로 설정하지 않았다면, 장치에 설정된 인증 모드가 적용됩니다.
 - ID/카드 + 지문: 인증을 위해 장치가 ID 와 지문 또는 카드와 지문을 요구하도록 설정합니다.
 - ID/카드 + 비밀번호: 인증을 위해 장치가 ID 와 비밀번호 또는 카드와 비밀번호를 요구하도록 설정합니다.
 - ID/카드 + 지문/비밀번호: 인증을 위해 장치가 ID와 지문, ID와 비밀번호, 카드와 지문, 또는 카드와 비밀번호를 요구하도록 설정합니다.
 - 카드만 사용: 인증을 위해 장치가 카드만 요구하도록 설정합니다.
 - ID/카드 + 지문 +비밀번호: 인증을 위해 장치가 ID 와 지문과 비밀번호 또는 카드와 지문과 비밀번호를 요구하도록 설정합니다. (항상적용, 사용안함, 사용자가 설정한 출입시간)
- **Mifare 설정 (BioStation MiFARE 에서만 사용 가능)**
 - Mifare 사용 안함: MiFARE 카드를 이용한 인증을 금지합니다.
 - 템플릿 온 카드 사용: 인증할 때에 MiFARE 카드에 저장된 지문 정보를 사용합니다.

5. 사용자 설정

- **Mifare 레이아웃 보기:** 장치에서 사용하고 있는 MIFARE 레이아웃을 확인합니다. MIFARE 레이아웃을 편집하는 방법에 관한 자세한 내용은 3.6.4.7 을 참조하십시오.
- **카드 ID 포맷**
 - **포맷:** 카드 ID 데이터를 어떤 방식으로 읽어 들일 것인가를 설정합니다. **일반**을 선택하면 카드 ID 데이터를 일반적인 형식으로 처리합니다. **Wiegand** 를 선택하면 위갠드 형식 설정에 따라 카드 ID 데이터를 처리합니다.
 - **Byte Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. **MSB** 는 큰 단위의 바이트에서 작은 단위의 바이트 순, **LSB** 는 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.
 - **Bit Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 비트를 처리할지 선택합니다. **MSB** 는 최상위 비트에서 최하위 비트 순, **LSB** 는 최하위 비트에서 최상위 비트 순으로 처리합니다.
- **기타 옵션**
 - **1:N 동작시간:** 지문만 사용 인증 모드를 적용할 일정(**항상적용, 사용안함, 사용자가 설정한 출입시간**)을 설정합니다.
 - **1:N 동작모드:** 지문 센서를 입력 모드로 동작시키는 방법(**자동, OK 나 근태기능키, 사용안함**)을 설정합니다.
 - **이중 인증 방식 사용:** 인증을 위해 장치가 두 사람(일반 사용자와 관리자)의 지문이나 카드를 요구하도록 설정합니다(**항상적용, 사용안함, 사용자가 설정한 출입시간**). 15 초 이내에 두 번째 사용자의 지문을 인증하지 않으면 인증이 무효가 됩니다
 - **단축 ID 매칭:** 1:N 인증 시도 시 입력한 ID 로 시작하는 사용자들에 대해서 인증을 시도합니다. 예를 들어, 111 을 입력하고 지문을 대면 ID 가 111 로 시작하는 사용자들에 대해서 인증을 시도하므로 속도가 빠릅니다. 단 서버 매칭을 사용하는 경우는 지원되지 않으며, BioStation 펌웨어 1.7 이상에서만 지원합니다.
 - **인터폰:** 장치에서 인터폰의 사용 여부를 설정할 수 있습니다(**사용 안함, 사용**).
 - 이중 인증 모드에서 관리자를 반드시 포함하는 설정 옵션을 지원합니다. 이중 인증 모드 운영 시에는 일반 사용자 인증 후 15 초 이내에 반드시 관리자가 인증해야 출입문의 릴레이가 켜집니다. 이 옵션을 사용하지 않는 경우 기존과 동일하게 일반 사용자나 관리자 여부와 관계 없이 다른 두 사용자가 15 초 이내에 인증하면 출입문의 릴레이가 켜지게 됩니다.
주의: 기능은 펌웨어 버전 BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다
- **Wiegand Card Bypass 사용:** BioStar 의 Wiegand 설정에 따라 인증 성공 여부와 상관 없이 CSN 을 내보내는 기능으로, 출입문 제어 기능이 없는 Dummy 장치로 사용하고자 할 때 유용한 기능입니다. 카드가 입력되면 장치에서는 별도의 인증 처리 없이 바로 Wiegand 로 카드 ID 를 출력하게 됩니다.
주의: 이 기능은 펌웨어 버전 BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.

5. 사용자 설정

5.1.1.2 지문 탭

지문 탭에서 BioStation 의 지문 인증 설정을 변경할 수 있습니다.



그림 5.1

- **지문**
 - **보안 등급:** 지문을 인증할 때 사용할 보안 등급을 설정합니다(보통, 안전, 가장 안전). 보안 등급을 높일수록 본인 거부율(본인의 지문이 확실한데도 장치가 인식하지 못하는 확률)도 같이 증가합니다.
 - **영상 품질 기준:** 지문의 품질 등급(낮음, 보통, 높음)을 설정합니다. 지문의 품질이 설정한 품질 등급보다 낮으면 시스템이 거부합니다.
 - **센서 감도:** 지문 스캐너의 민감도(이[최소]-기[최대])를 설정합니다. 센서의 민감도를 높이면 높일수록 더욱 정밀하게 지문을 스캔할 수 있지만, 지문의 화상이 거칠어지기 쉽습니다.
 - **1:N 지연 시간:** 지문을 인증하는 동안 지문 입력을 대기하는 시간(0 초 - 10 초)을 설정합니다. 이렇게 지연 시간을 설정함으로써 사용자가 지문 스캐너에서 손가락을 떼지 않더라도 같은 지문이 계속해서 인증되는 것을 방지할 수 있습니다.
 - **1:N 인식 속도:** 지문의 일치 여부를 판별하는 데 걸리는 시간을 줄이려면 인식 속도(자동, 보통, 빠름, 가장 빠름)를 조절합니다. 자동을 선택하면 장치에 등록된 총 지문 템플릿의 수에 따라 자동으로 판별 속도가 결정됩니다.
 - **등록 지문 영상:** BioStation 의 화면에 지문을 보일 것인지 말 것인지(보임, 보이지 않음)를 선택합니다.
 - **지문 입력 시간:** 지문 입력을 끝마쳐야 하는 시간(1 초 - 20 초)을 설정합니다. 정해진 시간 안에 지문을 입력하지 않으면 인증이 실패하게 됩니다.
 - **인증 제한 시간:** 지문의 일치 여부를 판별할 때 장치가 작업을 그만두는 시간(무제한, 1 초 - 10 초)을 설정합니다.
 - **서버 매칭:** 지문이 일치하는지를 장치에서 판별하지 않고 BioStar 서버에서 판별하도록 설정합니다. 이 옵션을 선택하면, 장치는 지문의 일치 여부를 판별하기 위해 지문 템플릿이나 카드 ID 정보를 서버에 보냅니다. 사용자의 수가 너무 많아 개별 장치에 모든 정보를 저장할 수 없거나 또는 보안상의 이유로 개별 장치에 정보를 보관할 수 없을 때 이 옵션을 사용하면 편리합니다.
 - **위조 지문 검사:** 위조 지문 공격을 방지하기 위하여 위조 지문을 검사할지(사용) 검사하지 않을지(사용 안함) 설정합니다.
- **지문 중복 검사:** 입력된 지문이 이미 등록된 지문인지 장치가 검사합니다. 장치가 입력된 지문을 이미 등록되어 있는 것으로 판단하면 등록 과정을 취소합니다.
- **지문 옵션 정보:** 전체 지문 템플릿 설정을 표시합니다. 지문 템플릿에 관한 자세한 내용은 4.9 를 참조하십시오.

5. 사용자 설정

5.1.1.3 네트워크 탭

네트워크 탭에서 BioStation의 네트워크 설정과 서버 설정을 변경할 수 있습니다.

[TCP/IP 설정] 네트워크 종류: 이더넷 포트: 1470

무선랜: 프리셋 1번 설정 변경

IP: DHCP 사용 DHCP 사용 안함

IP 주소: 61 . 83 . 152 . 175 게이트웨이: 61 . 83 . 152 . 129

서브넷: 255 . 255 . 255 . 128 연결 허용: 4

서버: 사용 사용 안함 서버와 자동으로 시간 동기화

IP 주소: 서버 포트: 1480 SSL: 사용 안함

[시리얼 설정]

RS485: 모드: 사용 안함 속도: 115200

RS232: 속도: 115200

USB 연결: USB 연결 허용 USB 연결 잠금

- TCP/IP 설정
 - 네트워크 종류: 랜의 종류(사용 안함, 이더넷, 무선 LAN 사용)를 선택합니다.
 - 포트: 장치가 사용할 포트를 지정합니다.
 - 무선 랜: 미리 설정된 무선 랜 구성을 선택합니다. 네트워크 종류에서 무선 랜을 선택해야 이 옵션을 설정할 수 있습니다
 - 설정 변경: 무선 랜을 설정하려면 클릭합니다. 무선 랜의 설정 방법은 3.2.4 를 참조하십시오.
 - DHCP 사용: 동적 호스트 구성 프로토콜(DHCP)을 사용합니다.
 - DHCP 사용 안함: 동적 호스트 구성 프로토콜(DHCP)을 사용하지 않습니다.
 - IP 주소: 장치의 IP 주소를 입력합니다.
 - 서브넷: 장치의 서브넷 주소를 입력합니다.
 - 게이트웨이: 네트워크의 게이트웨이를 입력합니다.
 - 연결 허용: 허용할 최대 연결 수를 지정합니다.
- 서버 설정
 - 사용: 서버 모드(장치를 BioStar 서버에 연결)를 사용합니다.
 - 사용 안함: 서버 모드를 사용하지 않습니다.
 - IP 주소: BioStar 서버의 IP 주소를 입력합니다.
 - 서버 포트: BioStar 가 사용하는 포트를 입력합니다.
 - SSL: 서버 연결에 사용되는 SSL 의 상태를 표시합니다.
 - 서버와 자동으로 시간 동기화: 장치의 시간을 서버의 시간과 동기화합니다. 장치에서 1 시간마다 서버 시간을 폴링하여, 서버의 시간과 5 초 이상 차이가 나면, 서버의 시간과 동기화합니다.
- RS485
 - 모드: RS485 로 연결된 장치의 모드(사용 안함, 호스트, 슬레이브, PC 연결 모드)를 설정합니다. RS485 모드에 관한 자세한 내용은 3.2.1 과 3.2.2 를 참조하십시오.
 - 속도: RS485 로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.
- RS232: RS232 로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.
- USB 설정: BioStation 에 장착된 USB 포트를 활성화합니다.

5. 사용자 설정

5.1.1.4 출입그룹 탭

출입그룹 탭에서 BioStation의 인증 제한 설정과 기본 출입그룹을 변경할 수 있습니다.

그림 5.2

- **인증 제한 설정**
 - **인증 간격(분)**: 다시 출입할 수 있는 권한을 얻는 데까지 필요한 시간(분 단위)을 설정합니다. 사용자가 어느 구역에 입장하였으면, 지정된 시간 안에는 그 구역 안으로 다시 입장할 수 없습니다.
 - **옵션 1~4**: 인증 제한 설정을 적용하려면 체크 상자를 선택한 후 이 설정을 적용할 시간을 입력합니다.
 - **최대 인증 허용 횟수**: 지정된 인증 제한 시간 안에 허용할 최대 입장 수를 설정합니다.
- **기본 출입 그룹 설정**: 다른 출입그룹에 포함되지 않은 새로운 사용자에게 적용할 기본 출입그룹을 선택합니다.

5.1.1.5 입력 탭

입력 탭에는 BioStation에 지정된 입력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 입력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Input 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 입력 설정을 구성하는 방법에 관한 자세한 내용은 3.10.3.2를 참조하십시오.

- **장치**: 설정을 추가하거나 수정할 BioStation(또는 Secure I/O)을 선택합니다.
- **포트**: 입력 포트(입력 0, 입력 1, Tamper)를 선택합니다. Secure I/O에서는 입력 0, 입력 1, 입력 2, 입력 3을 선택할 수 있습니다.

5. 사용자 설정

- **스위치:** 버튼을 클릭하여 입력 스위치의 보통 상태(N/O: 평상시 열림, N/C: 평상시 닫힘)를 설정합니다.
- **기능:** 입력을 받았을 때 취할 동작을 선택합니다.
 - **사용 안함:** 입력 포트를 감시하지 않습니다.
 - **일반 입력:** 지정된 동작을 실행하기 위해 입력 포트를 감시합니다. (Output 설정 대화 상자에서 지정된 이벤트를 확인하려면 5.1.1.6 을 참조하십시오.)
 - **비상 문 열림:** 이 장치가 제어하고 있는 출입문을 엽니다. 일반적인 출입문 열림 시간은 무시되며, 관리자가 출입문/구역 감시 탭을 통해서 "문 닫기" 명령을 실행하기 전까지는 출입문이 열린 채로 남아 있습니다(4.4.1 참조).
 - **모든 경보 해제:** 이 장치와 연결된 모든 경보를 해제합니다.
 - **장치 재 시작:** 장치를 재시동합니다.
 - **장치 잠금:** 장치가 잠깁니다. 잠긴 장치는 BioStar 서버와 통신할 수 없으며 또한 지문이나 카드 입력을 처리할 수 없습니다. 통신을 재연결하려면, 관리자가 BioStation 의 마스터 비밀번호를 입력하거나 BioEntry Plus 및 BioEntry W 장치에서 직접 인증을 해야 합니다.
 - BioStar 1.8v 에서 LED 녹색, LED 적색, 부저 입력, 출입 허가, 출입 거부 기능이 추가되었으며, BioStation (FW 1.93v), BioStation T2 (FW 1.3v), FaceStation (FW 1.3v), BioEntry Plus (FW 1.6v), BioEntry W (FW 1.2v), BioLite Net (FW 1.4v), Xpass (FW 1.3v) 에서만 지원됩니다.
- **동작시간:** 입력 신호를 감시할 일정(사용안함, 항상적용)을 설정합니다.
- **입력시간(ms):** 지정된 동작을 발생시키기 위해 필요한 입력 신호의 지속 시간(1000 분의 1 초)을 입력합니다.

5.1.1.6 출력 탭

출력 탭에는 BioStation 에 적용되는 출력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 출력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 이 때, 반드시 Output 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 출력 설정을 구성하는 방법에 관한 자세한 내용은 3.10.3.1 을 참조하십시오.

5. 사용자 설정

The screenshot shows the 'Output 설정' (Output Settings) window. At the top, there are dropdowns for '장치' (Device) set to '12647' and '포트' (Port) set to '릴레이 0'. Below this are two sections for alarm events. The first section, '알람 동작 개시 이벤트', has a list box on the left and configuration fields on the right: '이벤트' (Event) set to '인증 성공', '장치' (Device) set to '12647', '신호파형' (Signal Type) set to 'Signal1', and '우선순위' (Priority) set to '1'. The second section, '알람 멈출 이벤트', has similar configuration fields: '이벤트' (Event) set to '인증 성공', '장치' (Device) set to '12647', and '우선순위' (Priority) set to '1'. Both sections have '추가' (Add), '삭제' (Delete), and '모두 삭제' (Delete All) buttons. At the bottom of the window are '저장' (Save) and '취소' (Cancel) buttons.

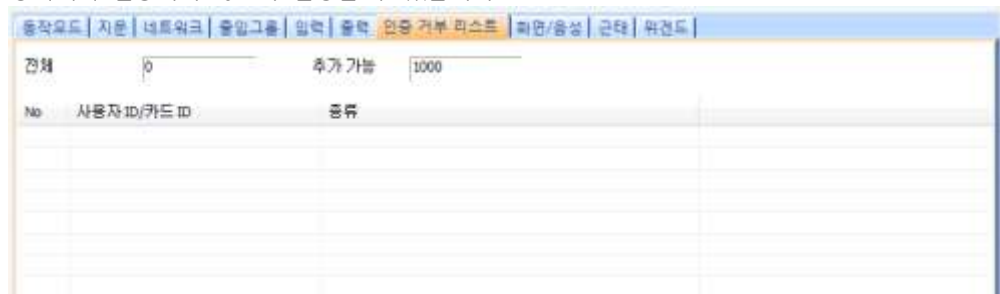
- **장치:** 설정을 추가하거나 수정할 장치의 종류를 선택합니다.
- **포트:** 출력 포트(릴레이 0)를 선택합니다. Secure I/O 에서는 릴레이 0, 릴레이 1 을 선택할 수 있습니다.
- **알람 동작 개시 이벤트:** 옵션을 설정하고 **추가**를 클릭하여 알람 동작 개시 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람을 발생시킵니다.
 - **이벤트:** 알람을 발생시킬 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
 - **장치:** 알람을 발생시키기 위해 감시할 장치를 선택합니다.
 - **신호파형:** 메뉴 표시줄의 **옵션 > 이벤트 > Output 포트 설정**을 통해서 이미 설정한 신호파형 중에서 하나를 선택합니다.

5. 사용자 설정

- **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선순위 2 의 알람 동작 개시 이벤트는 오직 우선순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.
- **알람 멈춤 이벤트:** 옵션을 설정하고 **추가**를 클릭하여 알람 멈춤 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람이 멈춥니다.
- **이벤트:** 알람을 멈추게 할 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
- **장치:** 알람을 멈추게 하기 위해 감시할 장치를 선택합니다.
- **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선순위 2 의 알람 동작 개시 이벤트는 오직 우선순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.

5.1.1.7 인증 거부 리스트 탭

인증 거부 리스트 탭에서 사용자 ID 나 카드 번호를 등록하여 사용자의 출입 시도 시 장치에서 인증되지 않도록 설정할 수 있습니다.



- **전체:** 인증 거부 목록에 등록된 사용자 ID 나 카드의 총 수를 표시합니다.
- **추가가능:** 등록할 수 있는 사용자 ID 나 카드의 수를 표시합니다.

참고: 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있습니다.

5.1.1.8 화면/음성 탭

화면/음성 탭에서 BioStation 의 화면 설정과 소리 설정을 변경할 수 있습니다. 변경한 설정을 적용하려면 반드시 탭의 아래에 있는 **적용**을 클릭해야 합니다. **다른장치 적용**을 클릭하여 다른 장치에 같은 설정을 적용할 수 있습니다.

5. 사용자 설정

- **화면/음성 설정**
 - 언어: 화면에 표시할 언어(한글, 영문, 사용자 정의)를 선택합니다.
 - 하단정보: 부가적인 정보(시간, 사용 안함)가 BioStation 의 화면 하단에 표시되도록 설정합니다.
 - 메뉴 타임아웃: 대기 화면으로 되돌아갈 시간(무제한, 10 초, 20 초, 30 초)을 설정합니다.
 - 개인 인증 화면: BioStation 화면에 인증 성공 메시지를 표시할지(사용) 표시하지 않을지(사용 안함) 설정합니다. 사용자 창에서 인증 성공 메시지를 추가할 수 있습니다. 사진 및 개인인증화면 편집을 클릭하여, 표시 횟수와 표시 기간을 설정한 후, 인증 성공 메시지 필드에 글을 입력한 다음, 저장을 클릭합니다.
 - 구성 파일: BioStar 프로그램에서 사용할 언어 파일(변경 안함, 영어 구성 파일, 한국어 구성 파일, 사용자 정의)을 설정합니다. 영어나 한국어 이외의 언어 파일을 사용하려면, 사용자 정의를 선택한 후 줄임표(...)를 클릭한 다음, 언어 파일을 지정합니다.
 - 배경 화면: BioStation 에 사용할 배경화면의 종류(로고, 공지사항, 슬라이드쇼)를 설정합니다. 지원되는 파일 종류는 JPG, GIF, BMP, PNG 이며 320×240 픽셀을 초과해서는 안됩니다. 로고나 공지사항에 사용되는 그림은 오직 한번에 하나의 그림만 사용할 수 있습니다. 반면, 슬라이드쇼는 (지정된 시간 간격으로) 최대 16 개의 그림을 표시할 수 있습니다.
 - 공지사항: BioStation 화면에 표시할 공지사항을 추가합니다. 공지사항을 추가했다면, 적용을 클릭하여 현재 선택된 장치에 적용하거나 또는 다른 장치 적용을 클릭하여 다른 모든 장치에 적용할 수 있습니다.
 - 음량: BioStation 의 음량(0~100%)을 설정합니다.
 - 메시지 타임아웃: 인증 실패 메시지나 인증 성공 메시지가 표시될 시간을 설정합니다.
- **배경화면 변경**: 이 체크 상자를 선택하여 새로운 배경화면을 장치에 저장할 수 있습니다. 추가를 클릭한 후 새로운 그림 파일을 지정해서 추가합니다.
- **효과음 변경**: 이 체크 상자를 선택하여 각 이벤트에 임의의 소리를 적용할 수 있습니다. 목록에 있는 이벤트를 클릭한 다음, 추가를 클릭한 후 새로운 소리 파일을 지정해서 추가합니다.

5. 사용자 설정

5.1.1.9 근태 탭

근태 탭에서 BioStation 장치의 근태 키 입력 방식을 설정할 수 있습니다. 설정을 저장하려면 장치 창의 하단에 있는 **적용**을 클릭해야 합니다. **다른장치 적용**을 클릭하여 다른 장치에 현재 장치의 설정을 동일하게 적용할 수 있습니다.

동작모드
지문
네트워크
출입그룹
입력
출력
인증 거부 리스트
화면/음성
근태
위젯드

근태 키 입력 방식 사용자 선택 ▼

보고서 근태키	내용	자동적용 시간	고정	문열림	이벤트 종류
F1	In	사용안함	사용	사용	들어옴
F2	Out	사용안함	사용 안함	사용 안함	나감
F3	In Duty	사용안함	사용 안함	사용	나감
F4	Out Duty	사용안함	사용 안함	사용 안함	나감

관리

BioStation 기능키 F1 ▼ 고정 이벤트

화면 표시 문구 문열림

자동 모드 적용 시간 ▼

이벤트 종류 사용 안함 ▼

지각/조퇴 처리 안함 결과에만 적용

이 이벤트 이후부터 근무시간에 포함

추가

수정

삭제

모두 삭제

- **근태 키 입력 방식:** 장치에 적용할 근태 키 입력 방식을 선택합니다.
 - **사용 안함:** 사용자는 장치에서 근태 이벤트를 기록할 수 없습니다.
 - **사용자 선택:** 사용자는 근태 이벤트를 기록하려고 할 때마다 목적에 맞는 근태 기능키를 눌러야 합니다.
 - **선택 후 유지:** 한 사용자가 특정 근태 기능키를 누를 경우 다른 근태 기능키를 누를 때까지 그 기능키가 유지됩니다.
 - **자동 설정:** 설정된 출입시간 일정에 맞게 BioStation 장치가 자동으로 근태 기능을 표시합니다.
 - **이벤트 고정:** BioStation 장치는 사용자가 설정한 근태 기능만 표시합니다.
- **관리:** 근태 기능에 사용할 키를 선택하고 어떤 근태 이벤트를 할당할지 설정합니다.
 - **BioStation 기능키:** 아래 화살표를 클릭하여 목록에서 근태 기능에 사용할 키(F1~F4, 1~9, CALL, 0, ESC)를 선택합니다. **이벤트 고정**방식을 선택하였다면, 오른쪽에 있는 **고정 이벤트**체크 상자를 선택합니다.
 - **화면 표시 문구:** BioStation 화면에 표시할 근태 기능에 맞는 문구를 입력합니다.
 - **자동 모드 적용 시간:** **자동 설정**방식을 선택한 경우 아래 화살표를 클릭하여 목록에서 장치에 적용할 출입시간을 선택합니다. 선택한 시간에 맞추어 설정된 기능을 표시합니다. 출입시간을 추가하는 방법에 관해서는 3.7.1 을 참조하십시오.
 - **이벤트 종류:** 선택한 키에 할당할 이벤트의 종류(**사용 안함**, **출근**, **퇴근**, **들어옴**, **나감**)를 선택합니다. **출근** 또는 **퇴근**을 선택한 경우 **지각/조퇴 처리 안함** 체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면 사용자의 실제 출퇴근시간에 관계없이 항상 정시에 출퇴근한 것으로 기록합니다. 근태 보고서의 결과에만 정시에 출퇴근한 것으로 기록하고 실제 근무 시간은 올바르게 계산하려면 **결과에만 적용** 체크 상자를 선택합니다. **나감**을 선택한 경우에는 **이 이벤트 이후부터 근무시간에 포함** 체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면, 사용자가 근무상의 이유로

5. 사용자 설정

밖으로 나가는 것으로 간주하여 실제 근무 시간보다 빨리 나갔다고 하더라도 정상적으로 모든 시간을 근무한 것으로 기록합니다.

5.1.1.10 위갠드 탭

위갠드 탭에서 BioStation 에서 사용할 Wiegand 형식을 설정할 수 있습니다.

BioStation 에서 위갠드 기능을 사용하려면 **Wiegand 입력**과 **Wiegand 출력**을 설정합니다.

Wiegand 설정 마법사를 실행하려면 **포맷 변경**을 클릭합니다. 위갠드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.

- **Wiegand 모드:** 카드 ID 데이터를 읽을 때 사용할 위갠드 모드(**일반모드**, **확장모드**)를 선택합니다. 일반모드를 선택하면 BioStation 에 연결된 RF 장치는 BioStation 의 일부로 인식됩니다. 확장모드를 선택하면 BioStation 에 연결된 RF 장치는 독립된 장치로 인식됩니다. 확장모드를 이용할 경우 RF 장치는 자신의 ID 로 로그를 남길 뿐 아니라 출입문을 구성할 수 있으며 구역에 포함될 수 있습니다.
- **Wiegand 입력:** 위갠드 입력을 통해 받아들이는 ID 데이터를 어떻게 해석하여 처리할지 선택합니다.
 - **사용안함:** 위갠드 입력 신호를 받아들이지 않습니다.
 - **Wiegand (카드):** 위갠드 입력을 통해 들어오는 ID 데이터를 카드 ID 로 해석하여 처리합니다.
 - **Wiegand (사용자):** 위갠드 입력을 통해 들어오는 ID 데이터를 사용자 ID 로 해석하여 처리합니다.
- **Wiegand 출력:** 위갠드 출력을 통해 어떤 신호를 내보낼지 선택합니다.
 - **사용안함:** 위갠드 출력 신호를 내보내지 않습니다.
 - **Wiegand (카드):** 인증에 성공한 사용자의 카드 ID 를 위갠드 출력 신호로 내보냅니다.
 - **Wiegand (사용자):** 인증에 성공한 사용자의 사용자 ID 를 위갠드 출력 신호로 내보냅니다.

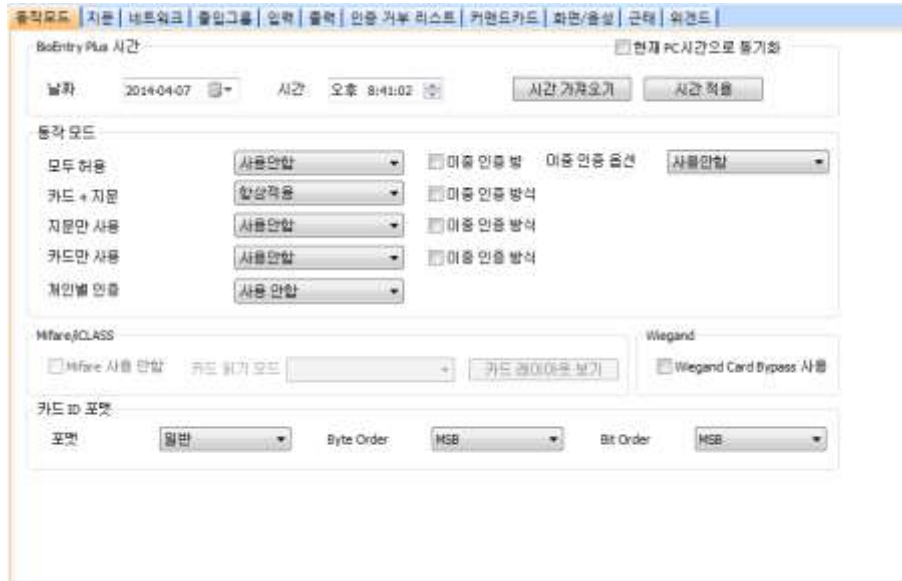
5.1.2 BioEntry Plus 및 BioEntry W 설정 변경하기

이 절에서는 BioEntry Plus 및 BioEntry W 에서 사용할 수 있는 설정에 대해서 설명합니다. 이러한 설정을 변경하여 현재 처해있는 상황이나 운영상의 필요에 맞게 BioEntry Plus 및 BioEntry W 의 기능을 변경할 수 있습니다.

5.1.2.1 동작모드 탭

동작모드 탭에서 BioEntry Plus 및 BioEntry W 의 시간을 변경할 수 있으며 동작 모드와 관련된 다양한 설정을 변경할 수 있습니다.

5. 사용자 설정



- BioEntry Plus 시간/BioEntry W 시간

- 날짜: 장치에서 표시할 날짜를 직접 설정합니다.
- 시간: 장치에서 표시할 시간을 직접 설정합니다.
- 이중 인증 모드에서 Admin User 를 반드시 포함하는 설정 옵션을 지원합니다. 이중 인증 모드 운영 시에는 Normal User 인증 후 15 초 이내에 반드시 Admin User 가 인증해야 Door Relay 가 켜집니다. 이 옵션을 사용하지 않는 경우 기존과 동일하게 Normal User 나 Admin User 여부와 관계 없이 다른 두 사용자가 15 초 이내에 인증하면 Door Relay 가 켜지게 됩니다.

주의: 이 기능은 펌웨어 버전 BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다

- Wiegand Card Bypass 사용: BioStar 의 Wiegand 설정에 따라 인증 성공 여부와 상관 없이 CSN 을 내보내는 기능으로, BioStar 제품군 장치를 타사 ACU 와 Wiegand 로 연동하여 인증 여부를 판단하고 출입문 제어 기능이 없는 Dummy 장치로 사용하고자 할 때 필요한 기능입니다. 카드가 입력되면 장치에서는 별도의 인증 처리 없이 바로 Wiegand 로 카드 ID 를 출력하게 됩니다.

주의: 이 기능은 펌웨어 버전 BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.)

5. 사용자 설정

- 현재 PC 시간으로 동기화: BioStar 클라이언트 프로그램이 설치되어 있는 로컬 PC의 날짜와 시간을 가져와 바로 아래 날짜와 시간 스피너 상자에 표시합니다. 시간 적용을 클릭하면, 장치의 날짜와 시간이 로컬 PC의 날짜와 시간으로 설정됩니다.
- 시간 가져오기: 현재 장치에서 표시되고 있는 시간을 가져옵니다.
- 시간 적용: 장치의 시간을 설정한 시간으로 변경합니다.
- 동작 모드 설정: 아래의 모든 옵션에서 이중 인증 방식 적용 체크 상자를 선택하면, 출입을 인증 받기 위해서는 두 사람이 동시에 인증을 해야 합니다.
 - 모두 허용: 모든 종류의 인증 방식을 허용합니다.
 - 카드 + 지문: 인증을 위해 장치가 카드와 지문을 요구하도록 설정합니다.
 - 지문만 사용: 인증을 위해 장치가 지문만 요구하도록 설정합니다.
 - 카드만 사용: 인증을 위해 장치가 카드만 요구하도록 설정합니다. (항상적용, 사용안함, 사용자가 설정한 출입시간)
참고: 이중 인증 방식 사용은 인증을 위해 장치가 두 사람의 지문이나 카드를 요구하도록 설정합니다.
 - 개인별 인증: 개인에게 설정된 인증 방식을 사용하여 인증하도록 설정합니다. (사용안함, 사용)
- Mifare/iCLASS(특정 모델에서 사용 가능함)
- BioEntry PlusMiFARE 장치
 - 카드 사용 안함: MiFARE 카드를 이용한 인증을 금지합니다.
 - 카드 읽기 모드: 카드 인증 모드의 종류를 설정합니다(MiFARE 템플릿 또는 MiFARE CSN 만).
 - Mifare 레이아웃 보기: 장치에서 사용하고 있는 MiFARE 레이아웃을 확인합니다. MiFARE 레이아웃을 편집하는 방법에 관한 자세한 내용은 3.6.4.6을 참조하십시오.
- BioEntry PlusiCLASS 장치
 - 카드 사용 안함: iCLASS 또는 FeliCa 카드를 이용한 인증을 금지합니다.
 - 카드 읽기 모드: 카드 인증 모드의 종류를 설정합니다(iCLASS 템플릿, iCLASS CSN, FeliCa CSN 만)
 - 카드 레이아웃 보기: 장치에서 사용하고 있는 iCLASS 레이아웃을 편집합니다. MiFARE 레이아웃을 편집하는 방법에 관한 자세한 내용은 3.6.4.7을 참조하십시오.
- 카드 ID 포맷
 - 포맷: 카드 ID 데이터를 어떤 방식으로 읽어 들일 것인가를 설정합니다. 일반을 선택하면 카드 ID 데이터를 일반적인 형식으로 처리합니다. Wiegand를 선택하면 위갠드 형식 설정에 따라 카드 ID 데이터를 처리합니다.
 - Byte Order: 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. MSB를 선택하면 큰 단위의 바이트에서 작은 단위의 바이트 순으로 처리합니다. LSB를 선택하면 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.
 - Bit Order: 카드 ID 데이터를 처리할 때 어떤 순서로 비트를 처리할지 선택합니다. MSB를 선택하면 최상위 비트에서 최하위 비트 순으로 처리합니다. LSB를 선택하면 최하위 비트에서 최상위 비트 순으로 처리합니다.

5.1.2.2 지문 탭

지문 탭에서 BioEntry Plus 및 BioEntry W의 지문 인증 설정을 변경할 수 있습니다.

5. 사용자 설정

홈 | 지문 | 네트워크 | 출입그룹 | 입력 | 출력 | 인증 거부 리스트 | 카렌트카드 | 화면/음성 | 군데 | 위젯도

지문

보안 등급	보통	1:N 인식 속도	자동
지문 입력 시간	10 초	인증 제한 시간	3 초
서버 매칭	사용	위조 지문 검사	사용 안함

지문 옵션 정보

템플릿 형식: 슈퍼리마템플릿 형식

- 지문
 - 보안 등급: 지문을 인증할 때 사용할 보안 등급(보통, 안전, 가장 안전)을 설정합니다. 보안 등급을 높일수록 본인 거부율(본인의 지문이 확실한데도 장치가 인식하지 못하는 확률)도 같이 증가합니다.
 - 지문 입력 시간: 지문 입력을 끝마쳐야 하는 시간(1 초-20 초)을 설정합니다. 정해진 시간 안에 지문을 입력하지 않으면 인증이 실패하게 됩니다.
 - 서버 매칭: 지문이 일치하는지를 장치에서 판별하지 않고 BioStar 서버에서 판별하도록 설정합니다. 이 옵션을 선택하면, 장치는 지문의 일치 여부를 판별하기 위해 지문 템플릿이나 카드 ID 정보를 서버에 보냅니다. 사용자의 수가 너무 많아 개별 장치에 모든 정보를 저장할 수 없거나 또는 보안상의 이유로 개별 장치에 정보를 보관할 수 없을 때 이 옵션을 사용하면 편리합니다.
 - 1:N 인식 속도: 지문의 일치 여부를 판별하는 데 걸리는 시간을 줄이려면 인식 속도(자동, 보통, 빠르게, 아주 빠르게)를 조절합니다. 자동을 선택하면 장치에 등록된 총 지문 템플릿의 수에 따라 자동으로 판별 속도가 결정됩니다.
 - 인증 제한 시간: 지문의 일치 여부를 판별할 때 장치가 작업을 그만두는 시간(무제한, 1 초 - 10 초)을 설정합니다.
 - 위조 지문 검사: 위조 지문 공격을 방지하기 위하여 위조 지문을 검사할지(사용) 검사하지 않을지(사용 안함) 설정합니다.

5. 사용자 설정

5.1.2.3 네트워크 탭

네트워크 탭에서 BioEntry Plus 및 BioEntry W 의 네트워크 설정과 서버 설정을 변경할 수 있습니다.



- **TCP/IP**
 - **DHCP 사용:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용합니다.
 - **DHCP 사용 안함:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용하지 않습니다.
 - **IP 주소:** 장치의 IP 주소를 입력합니다.
 - **Sunet:** 장치의 서브넷 주소를 입력합니다.
 - **Gateway:** 네트워크의 게이트웨이를 입력합니다.
 - **포트:** 장치가 사용할 포트를 지정합니다.
- **서버 설정**
 - **사용:** 서버 모드를 사용하려면 버튼을 클릭합니다.
 - **사용 안함:** 서버 모드를 사용하지 않으려면 버튼을 클릭합니다.
 - **IP 주소:** BioStar 서버의 IP 주소를 입력합니다.
 - **서버와 자동으로 시간 동기화:** 장치의 시간을 서버의 시간과 동기화합니다. 장치에서 1 시간마다 서버 시간을 폴링하여, 서버의 시간과 5 초 이상 차이가 나면, 서버의 시간과 동기화합니다.
- **100 Base-T 지원:** 이 옵션을 사용하여 네트워크에 연결하면 장치에서 빠른 속도를 이용할 수 있습니다. 이 옵션을 선택하면, 장치가 이더넷 네트워크에 연결될 때 지원되는 속도를 확인한 후 더 빠른 속도를 지원하는 방식으로 연결합니다. 이 옵션을 사용하지 않으면, 10Base-T 속도로 이더넷 네트워크에 연결합니다.
 - **사용:** 네트워크에서 지원하는 경우 100Base-T 속도로 연결합니다.
 - **사용 안함:** 100Base-T 속도를 사용하지 않습니다.
- **RS485**
 - **모드:** RS485 로 연결된 장치의 모드(사용 안함, 호스트, 슬레이브, PC 연결 모드)를 설정합니다.
 - **속도:** RS485 로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.
- **MTU Size 설정 지원**

5. 사용자 설정

- Black Fin 계열의 단말기는 MTU Size 설정을 지원합니다. 지원 패킷 사이즈는 1078-1514 이며, 기본값은 1514 입니다.

주의: 본 기능은 펌웨어 버전 BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.

5.1.2.4 출입그룹 탭

출입그룹 탭에서 BioEntry Plus 및 BioEntry W 의 인증 제한 설정과 기본 출입그룹을 변경할 수 있으며 T&A 기능을 설정할 수 있습니다.

- **인증 제한 설정**
 - **인증 간격(분):** 다시 출입할 수 있는 권한을 얻는 데까지 필요한 시간(분 단위)을 설정합니다. 사용자가 어느 구역에 입장하였으면, 지정된 시간 안에는 그 구역 안으로 다시 입장할 수 없습니다.
 - **옵션 1~4:** 인증 제한 설정을 적용하려면 체크 상자를 선택한 후 이 설정을 적용할 시간을 입력합니다.
 - **최대 인증 허용 횟수:** 지정된 인증 제한 시간 안에 허용할 최대 입장 수를 설정합니다.
- **기본 출입 그룹 설정:** 다른 출입그룹에 포함되지 않은 새로운 사용자에게 적용할 기본 출입그룹을 선택합니다.

5.1.2.5 입력 탭

입력 탭에는 BioEntry Plus 및 BioEntry W 에 지정된 입력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 입력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Input 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 입력 설정을 구성하는 방법에 관한 자세한 내용은 3.10.3.2 를 참조하십시오.

5. 사용자 설정



그림 5.3

- **장치:** 설정을 추가하거나 수정할 BioEntry Plus 또는 BioEntry W(또는 Secure I/O)를 선택합니다.
- **포트:** 입력 포트(입력 0, 입력 1, Tamper)를 선택합니다. Secure I/O 에서는 입력 0, 입력 1, 입력 2, 입력 3 을 선택할 수 있습니다.
- **스위치:** 버튼을 클릭하여 입력 스위치의 보통 상태(N/O: 평상시 열림, N/C: 평상시 닫힘)를 설정합니다.
- **기능:** 입력을 받았을 때 취할 동작을 선택합니다:
 - **사용 안함:** 입력 포트를 감시하지 않습니다.
 - **일반 입력:** 지정된 동작을 실행하기 위해 입력 포트를 감시합니다. (Output 설정 대화 상자에서 지정한 이벤트를 확인하려면 5.1.2.6 을 참조하십시오.)
 - **비상 문 열림:** 이 장치가 제어하고 있는 출입문을 엽니다. 일반적인 출입문 열림 시간은 무시되며, 관리자가 출입문/구역 감시 탭을 통해서 "문 닫기" 명령을 실행하기 전까지는 출입문이 열린 채로 남아 있습니다(4.4.1 참조).
 - **모든 경보 해제:** 이 장치와 연결된 모든 경보를 해제합니다.
 - **장치 재 시작:** 장치를 껐다가 다시 시작합니다.
 - **장치 잠금:** BioStar 와 장치 사이의 통신을 금지합니다. 통신을 다시 연결하려면, 관리자가 BioStation 의 마스터 비밀번호를 입력하거나 또는 BioEntry Plus 및 BioEntry W 장치에서 직접 인증을 해야 합니다.
 - BioStar 1.8v 에서 LED 녹색, LED 적색, 부저 입력, 출입 허가, 출입 거부 기능이 추가되었으며, BioStation (FW 1.93v), BioStation T2 (FW 1.3v), FaceStation (FW 1.3v), BioEntry Plus (FW 1.6v), BioEntry W (FW 1.2v), BioLite Net (FW 1.4v), Xpass (FW 1.3v) 에서만 지원됩니다.
- **동작시간:** 입력 신호를 감시할 일정(사용안함, 항상적용)을 설정합니다.
- **입력시간(ms):** 지정한 동작을 발생시키기 위해 필요한 입력 신호의 지속 시간(1000 분의 1 초)을 입력합니다.

5.1.2.6 출력 탭

출력 탭에는 BioEntry Plus 및 BioEntry W 에 지정된 출력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 출력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Output 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 출력 설정을 구성하는 방법에 관한 자세한 내용은 3.10.3.1 을 참조하십시오.

5. 사용자 설정



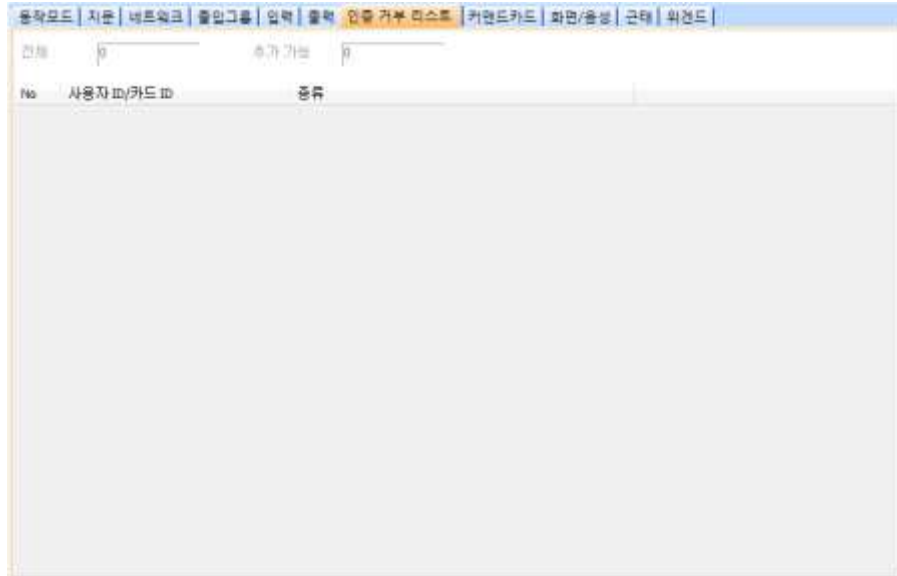
그림 5.4

- **장치:** 설정을 추가하거나 수정할 장치의 종류를 선택합니다.
- **포트:** 출력 포트(릴레이 0)를 선택합니다. Secure I/O 에서는 릴레이 0, 릴레이 1 을 선택할 수 있습니다.
- **알람 동작 개시 이벤트:** 옵션을 설정하고 **추가**를 클릭하여 알람 동작 개시 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람을 발생시킵니다.
 - **이벤트:** 알람을 발생시킬 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
 - **장치:** 알람을 발생시키기 위해 감시할 장치를 선택합니다.
 - **신호파형:** 메뉴 표시줄의 **옵션 > 이벤트 > Output 포트 설정**을 통해서 이미 설정한 신호파형 중에서 하나를 선택합니다.
 - **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선순위 2 의 알람 동작 개시 이벤트는 오직 우선순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.
- **알람 멈춤 이벤트:** 옵션을 설정하고 **추가**를 클릭하여 알람 멈춤 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람이 멈춥니다.
 - **이벤트:** 알람을 멈추게 할 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
 - **장치:** 알람을 멈추기 위해 감시할 장치를 선택합니다.
 - **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선순위 2 의 알람 동작 개시 이벤트는 오직 우선순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.

5. 사용자 설정

5.1.2.7 인증 거부 리스트 탭

인증 거부 리스트 탭에서 사용자 ID 나 카드 번호를 등록하여 사용자의 출입 시도 시 장치에서 인증되지 않도록 설정할 수 있습니다.



- **전체:** 인증 거부 목록에 등록된 사용자 ID 나 카드의 총 수를 표시합니다.
- **추가가능:** 등록할 수 있는 사용자 ID 나 카드의 수를 표시합니다.

참고: 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있습니다.

5. 사용자 설정

5.1.2.8 커맨드카드 탭

커맨드카드 탭에서 커맨드 카드를 발급할 수 있습니다. 커맨드 카드 발급에 관한 자세한 내용은 3.2.6.1 을 참조하십시오.



- **카드 ID:** 카드 ID 를 직접 입력하거나 또는 **카드 읽기**를 클릭한 후 장치에 카드를 올려놓으면 카드 ID 가 자동적으로 입력됩니다.
- **커맨드 종류:** 발급할 커맨드 카드의 종류(등록 카드, 삭제 카드, 모두 삭제 카드)를 선택합니다.

5.1.2.9 화면/음성 탭

화면/음성 탭에서 이벤트에 따라 LED 와 Buzzer 동작을설정할 수 있습니다.설정 한 후 이벤트 별로 저장 버튼을 클릭해야 저장이 됩니다.



- **이벤트:** 설정을 적용할 이벤트를 선택합니다.
- **LED:** 선택한 이벤트 발생 시 LED 의 행동 패턴을 설정합니다.
 - **횟수:** 선택한 이벤트 발생 시 LED 의 반복 사이클을 설정합니다. 0 을 입력하면 무한 반복되며 -1 을 입력하면 LED 가 작동하지 않습니다.

5. 사용자 설정

- **색상:** 최대 3 개의 LED 색상을 선택합니다. 위에서 아래의 순서대로 LED의 색상이 바뀌면서 반복됩니다. 숫자 필드에는 각 색상이 지속되는 시간을 밀리초 단위로 입력합니다.
- **Buzzer:** 선택한 이벤트 발생 시 경고음의 패턴을 설정합니다.
 - **횟수:** 경고음의 반복 횟수를 설정합니다. 0 을 입력하면 계속 경고음이 발생하며 -1 을 입력하면 경고음이 발생하지 않습니다.
 - **음량:** 경고음의 크기(Low /Middle /High)를 설정합니다. 위에서 아래의 순서로 선택한 음량 크기대로 경고음이 반복됩니다. 숫자 필드에는 각 경고음이 지속되는 시간을 밀리초 단위로 입력합니다.
 - **페이드아웃:** 경고음 소리가 점차 작아집니다.

5.1.2.10 위갠드 탭

위갠드 탭에서 BioEntry Plus 및 BioEntry W에서 사용할 위갠드 형식을 설정할 수 있습니다.

BioEntry Plus 및 BioEntry W에서 위갠드 기능을 사용하려면 **Wiegand Input** 과 **Wiegand Out** 을 설정합니다. Wiegand 설정 마법사를 실행하려면 **포맷 변경**을 클릭합니다. 위갠드 형식에 관한 자세한 내용은 3.2.16을 참조하십시오.

Wiegand 모드: 카드 ID 데이터를 읽을 때 사용할 위갠드 모드(**일반모드**, **확장모드**)를 선택합니다. 일반모드를 선택하면 BioStation에 연결된 RF 장치는 BioStation의 일부로 인식됩니다. 확장모드를 선택하면 BioStation에 연결된 RF 장치는 독립된 장치로 인식됩니다. 확장모드를 이용할 경우 RF 장치는 자신의 ID로 로그를 남길 뿐 아니라 출입문을 구성할 수 있으며 구역에 포함될 수 있습니다.

- **Wiegand 입력:** 위갠드 입력을 통해 받아들이는 ID 데이터를 어떻게 해석하여 처리할지 선택합니다.
 - **사용안함:** 위갠드 입력 신호를 받아들이지 않습니다.
 - **Wiegand (카드):** 위갠드 입력을 통해 들어오는 ID 데이터를 카드 ID로 해석하여 처리합니다.

5. 사용자 설정

- **Wiegand (사용자):** 위갠드 입력을 통해 들어오는 ID 데이터를 사용자 ID 로 해석하여 처리합니다.
- **Wiegand 출력:** 위갠드 출력을 통해 어떤 신호를 내보낼지 선택합니다.
- **사용안함:** 위갠드 출력 신호를 내보내지 않습니다.
- **Wiegand (카드):** 인증에 성공한 사용자의 카드 ID 를 위갠드 출력 신호로 내보냅니다.
- **Wiegand (사용자):** 인증에 성공한 사용자의 사용자 ID 를 위갠드 출력 신호로 내보냅니다.

5.1.3 BioLite Net 설정 변경하기

이 절에서는 BioLite Net 에서 사용할 수 있는 설정에 대해서 설명합니다. 이러한 설정을 변경하여 현재 처해있는 상황이나 운영상의 필요에 맞게 BioLite Net 의 기능을 변경할 수 있습니다.

5.1.3.1 동작모드 탭

동작모드 탭에서 BioLite Net 의 시간을 변경할 수 있으며 동작 모드와 관련된 다양한 설정을 변경할 수 있습니다.

- **BioLiteNet 시간**
 - **날짜:** 달력에서 장치에서 표시할 날짜를 설정합니다.
 - **시간:** 장치에서 표시할 시간을 설정합니다.
 - **현재 PC 시간으로 동기화:** BioStar 클라이언트 프로그램이 설치되어 있는 로컬 PC 의 날짜와 시간을 가져와 바로 아래 날짜와 시간 스피너 상자에 표시합니다. 시간 적용을 클릭하면, 장치의 날짜와 시간이 로컬 PC 의 날짜와 시간으로 설정됩니다.
 - **시간 가져오기:** 현재 장치에서 표시되고 있는 시간을 가져옵니다.
 - **시간 적용:** 장치의 시간을 설정한 시간으로 변경합니다.
- **센서 모드:** 센서 사용 시간대를 설정합니다.
 - **항상 적용:** 항상 센서가 대기하도록 하는 시간대를 설정합니다.
 - **ID 입력시:** ID 를 우선 입력 받은 후 센서가 대기하는 시간대를 설정합니다.
 - **OK Key 입력시:** OK Key 를 입력 받은 후 센서가 대기하는 시간대를 설정합니다.(항상적용, 사용안함, 사용자가 설정한 출입시간)
- **동작 모드:** 아래의 모든 옵션에서 이중 인증 방식 적용 체크 상자를 선택하면, 출입을 인증 받기 위해서는 두 사람이 동시에 인증을 해야 합니다.
 - **지문:** 인증을 위해 장치가 지문만 요구하도록 설정합니다.
 - **패스워드:** 인증을 위해 장치가 패스워드만 요구하도록 설정합니다.
 - **지문 또는 패스워드:** 인증을 위해 장치가 지문 또는 패스워드를 요구하도록 설정합니다.
 - **지문과 패스워드:** 인증을 위해 장치가 지문과 패스워드를 요구하도록 설정합니다.
 - **카드:** 인증을 위해 장치가 카드만 요구하도록 설정합니다. (항상적용, 사용안함, 사용자가 설정한 출입시간)
참고: 이중 인증 방식 사용은 인증을 위해 장치가 두 사람의 지문이나 카드를 요구하도록 설정합니다.
 - **개인별 인증:** 개인에게 설정된 인증 방식을 사용하여 인증하도록 설정합니다. (사용 안함, 사용)
- **Mifare**
 - **Mifare 사용 안함:** MiFARE 카드를 이용한 인증을 금지합니다.

5. 사용자 설정

- **템플릿 온 카드 사용:** 인증할 때에 MiFARE 카드에 저장된 지문 정보를 사용합니다.
- **Mifare 레이아웃 보기:** 장치에서 사용하고 있는 MiFARE 레이아웃을 확인합니다. MiFARE 레이아웃을 편집하는 방법에 관한 자세한 내용은 3.6.4.6 을 참조하십시오.
- **카드 ID 포맷**
 - **포맷:** 카드 ID 데이터를 어떤 방식으로 읽을지 설정합니다. **일반**을 선택하면 카드 ID 데이터를 일반적인 형식으로 처리합니다. **Wiegand** 를 선택하면 위갠드 형식 설정에 따라 카드 ID 데이터를 처리합니다.
 - **Byte Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. **MSB** 를 선택하면 큰 단위의 바이트에서 작은 단위의 바이트 순으로 처리합니다. **LSB** 를 선택하면 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.
 - **Bit Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 비트를 처리할지 선택합니다. **MSB** 를 선택하면 최상위 비트에서 최하위 비트 순으로 처리합니다. **LSB** 를 선택하면 최하위 비트에서 최상위 비트 순으로 처리합니다.
 - 이중 인증 모드에서 Admin User 를 반드시 포함하는 설정 옵션을 지원합니다. 이중 인증 모드 운영 시에는 Normal User 인증 후 15 초 이내에 반드시 Admin User 가 인증해야 Door Relay 가 켜집니다. 이 옵션을 사용하지 않는 경우 기존과 동일하게 Normal User 나 Admin User 여부와 관계 없이 다른 두 사용자가 15 초 이내에 인증하면 Door Relay 가 켜지게 됩니다.
주의: 이 기능은 펌웨어 버전 BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.
 - Wiegand Card Bypass 사용: BioStar 의 Wiegand 설정에 따라 인증 성공 여부와 상관 없이 CSN 을 내보내는 기능으로, BioStar 제품군 장치를 타사 ACU 와 Wiegand 로 연동하여 인증 여부를 판단하고 출입문 제어 기능이 없는 Dummy 장치로 사용하고자 할 때 필요한 기능입니다. 카드가 입력되면 장치에서는 별도의 인증 처리 없이 바로 Wiegand 로 카드 ID 를 출력하게 됩니다.
주의: 이 기능은 펌웨어 버전 BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.

5.1.3.2 지문 탭

지문 탭에서 BioLite Net 의 지문 인증 설정을 변경할 수 있습니다.

The screenshot shows the '지문' (Fingerprint) settings tab. The top navigation bar includes '동작모드', '지문', '네트워크', '출입그룹', '입력', '출력', '인증 거부 리스트', '화면/음성', '근태', and 'Wiegand'. The main settings area includes:

- 보안 등급:** 보통 (dropdown)
- 지문 입력 시간:** 10 초 (dropdown)
- 서버 매칭:** 사용 안함 (dropdown)
- 1N 인식 속도:** 자동 (dropdown)
- 인증 제한 시간:** 3 초 (dropdown)
- 위조 지문 검사:** 사용 안함 (dropdown)

Below these settings is a section for '지문 옵션 정보' (Fingerprint Option Info) with a checkbox for 'ISO 템플릿 사용' (Use ISO Template) which is currently unchecked.

그림 5.5

- **지문**
 - **보안 등급:** 지문을 인증할 때 사용할 보안 등급(보통, 안전, 가장 안전)을 설정합니다. 보안 등급을 높일수록 본인 거부율(본인의 지문이 확실한데도 장치가 인식하지 못하는 확률)도 같이 증가합니다.
 - **지문 입력 시간:** 지문 입력을 끝마쳐야 하는 시간(1 초-20 초)을 설정합니다. 정해진 시간 안에 지문을 입력하지 않으면 인증이 실패하게 됩니다.

5. 사용자 설정

- **서버 매칭:** 지문이 일치하는지를 장치에서 판별하지 않고 BioStar 서버에서 판별합니다. 장치는 지문의 일치 여부를 판별하기 위해 지문 템플릿이나 카드 ID 정보를 서버에 보냅니다. 사용자의 수가 너무 많아 개별 장치에 모든 정보를 저장할 수 없거나 또는 보안상의 이유로 개별 장치에 정보를 보관할 수 없을 때 이 옵션을 사용하면 편리합니다.
- **1:N 인식 속도:** 지문의 일치 여부를 판별하는 데 걸리는 시간을 줄이려면 인식 속도(자동, 보통, 빠르게, 아주 빠르게)를 조절합니다. **자동**을 선택하면 장치에 등록된 총 지문 템플릿의 수에 따라 자동으로 판별 속도가 결정됩니다.
- **인증 제한 시간:** 지문의 일치 여부를 판별할 때 장치가 작업을 그만두는 시간(무제한, 1 초 - 10 초)을 설정합니다.
- **위조 지문 검사:** 위조 지문 공격을 방지하기 위하여 위조 지문을 검사할지(사용) 검사하지 않을지(사용 안함) 설정합니다.
- **지문 옵션 정보:** 전체 지문 템플릿 설정을 표시합니다. 지문 템플릿에 관한 자세한 내용은 4.9 를 참조하십시오.

5.1.3.3 네트워크 탭

네트워크 탭에서 BioLite Net의 네트워크 설정과 서버 설정을 변경할 수 있습니다.

- **MTU Size 설정 지원**
 - Black Fin 계열 단말기는 MTU Size 설정을 지원합니다. 지원 패킷 사이즈는 1078~1514이며, 기본값은 1514입니다.
(이 기능은 펌웨어 버전 BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.)
- **TCP/IP**
 - **DHCP 사용:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용합니다.
 - **DHCP 사용 안함:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용하지 않습니다.
 - **IP 주소:** 장치의 IP 주소를 입력합니다.
 - **Sunet:** 장치의 서브넷 주소를 입력합니다.
 - **Gateway:** 네트워크의 게이트웨이를 입력합니다.
 - **포트:** 장치가 사용할 포트를 지정합니다.
- **서버 설정**
 - **사용:** 서버 모드를 사용합니다.
 - **사용 안함:** 서버 모드를 사용하지 않습니다.
 - **IP 주소:** BioStar 서버의 IP 주소를 입력합니다.
 - **서버와 자동으로 시간 동기화:** 장치의 시간을 서버의 시간과 동기화합니다. 장치에서 1 시간마다 서버 시간을 폴링하여, 서버의 시간과 5 초 이상 차이가 나면, 서버의 시간과 동기화합니다.
- **100 Base-T 지원:** 이 옵션을 사용하여 네트워크에 연결하면 장치에서 빠른 속도를 이용할 수 있습니다. 이 옵션을 선택하면, 장치가 이더넷 네트워크에 연결될 때 지원되는 속도를 확인한 후 더 빠른 속도를 지원하는 방식으로 연결합니다. 이 옵션을 사용하지 않으면, 10Base-T 속도로 이더넷 네트워크에 연결합니다.
 - **사용:** 네트워크에서 지원하는 경우 100Base-T 속도로 연결합니다.
 - **사용 안함:** 100Base-T 속도를 사용하지 않습니다.

5. 사용자 설정

- RS485
 - 모드: RS485 로 연결된 장치의 모드(사용 안함, 호스트, 슬레이브, PC 연결 모드)를 설정합니다.
 - 속도: RS485 로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.

5.1.3.4 출입그룹 탭

출입그룹 탭에서 BioLite Net의 인증 제한 설정과 기본 출입그룹을 변경할 수 있습니다.

그림 5.6

- 인증 제한 설정
 - 인증 간격(분): 다시 출입할 수 있는 권한을 얻는 데까지 필요한 시간(분 단위)을 설정합니다. 사용자가 어느 구역에 입장하였으면, 지정된 시간 안에는 그 구역 안으로 다시 들어갈 수 없습니다.
 - 옵션 1~4: 인증 제한 설정을 적용하려면 체크 상자를 선택한 후 이 설정을 적용할 시간을 입력합니다.
 - 최대 인증 허용 횟수: 지정된 인증제한 시간 안에 허용할 최대 입장수를 설정합니다.
 - 기본 출입 그룹 설정: 다른 출입그룹에 포함되지 않은 새로운 사용자에게 적용할 기본 출입그룹을 선택합니다.

5. 사용자 설정

5.1.3.5 입력 탭

입력 탭에는 BioLite Net 에 지정된 입력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 입력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Input 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 입력 설정을 구성하는 방법에 관한 자세한 내용은 3.10.3.2 를 참조하십시오.



그림 5.7

- **장치:** 설정을 추가하거나 수정할 BioLite Net(또는 Secure I/O)를 선택합니다.
- **포트:** 입력 포트(입력 0, 입력 1, Tamper)를 선택합니다. Secure I/O 에서는 입력 0, 입력 1, 입력 2, 입력 3 을 선택할 수 있습니다.
- **스위치:** 버튼을 클릭하여 입력 스위치의 보통 상태(N/O: 평상시 열림, N/C: 평상시 닫힘)를 설정합니다.
- **기능:** 입력을 받았을 때 취할 동작을 선택합니다:
 - **사용 안함:** 입력 포트를 감시하지 않습니다.
 - **일반 입력:** 지정된 동작을 실행하기 위해 입력 포트를 감시합니다. (Output 설정 대화 상자에서 지정한 이벤트를 확인하려면 5.1.3.6 을 참조하십시오.)
 - **비상 문 열림:** 이 장치가 제어하고 있는 출입문을 엽니다. 일반적인 출입문 열림 시간은 무시되며, 관리자가 출입문/구역 감시 탭을 통해서 "문 닫기" 명령을 실행하기 전까지는 출입문이 열린 채로 남아 있습니다(4.4.1 참조).
 - **모든 경보 해제:** 이 장치와 연결된 모든 경보를 해제합니다.
 - **장치 재 시작:** 장치를 껐다가 다시 시작합니다.
 - **장치 잠금:** BioStar 와 장치 사이의 통신을 금지합니다. 통신을 다시 연결하려면, 관리자가 BioLite Net 의 마스터 비밀번호를 입력하거나 또는 BioLite Net 에서 직접 인증을 받아야 합니다.
 - BioStar 1.8v 에서 LED 녹색, LED 적색, 부저 입력, 출입 허가, 출입 거부 기능이 추가되었으며, BioStation (FW 1.93v), BioStation T2 (FW 1.3v), FaceStation (FW 1.3v), BioEntry Plus (FW 1.6v), BioEntry W (FW 1.2v), BioLite Net (FW 1.4v), Xpass (FW 1.3v) 에서만 지원됩니다.
- **동작시간:** 입력 신호를 감시할 일정(사용안함, 항상적용)을 설정합니다.
- **입력시간(ms):** 지정한 동작을 발생시키기 위해 필요한 입력 신호의 지속 시간(1000 분의 1 초)을 입력합니다.

5. 사용자 설정

5.1.3.6 출력 탭

출력 탭에는 BioLite Net 에 지정된 출력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 출력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 **Output 설정** 대화 상자에서 관련 옵션을 지정해야 합니다. 출력 설정을 구성하는 방법에 관한 자세한 내용은 3.10.3.1 을 참조하십시오.



그림 5.8

- **장치:** 설정을 추가하거나 수정할 장치의 종류를 선택합니다.
- **포트:** 출력 포트(릴레이 0)를 선택합니다. Secure I/O 에서는 **릴레이 0** 또는 **릴레이 1** 을 선택할 수 있습니다.
- **알람 동작 개시 이벤트:** 옵션을 설정하고 **추가** 를 클릭하여 알람 동작 개시 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람을 발생시킵니다.
 - **이벤트:** 알람을 발생시킬 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
 - **장치:** 알람을 발생시키기 위해 감시할 장치를 선택합니다.
 - **신호파형:** 메뉴 표시줄의 **옵션 > 이벤트 > Output 포트 설정** 을 통해서 이미 설정한 신호파형 중에서 하나를 선택합니다.
 - **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선순위 2 의 알람 동작 개시 이벤트는 오직 우선순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.
- **알람 멈춤 이벤트:** 옵션을 설정하고 **추가** 를 클릭하여 알람 멈춤 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람이 멈춥니다.
 - **이벤트:** 알람을 멈추게 할 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
 - **장치:** 알람을 멈추기 위해 감시할 장치를 선택합니다.
 - **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를

5. 사용자 설정

들어, 우선순위 2의 알람 동작 개시 이벤트는 오직 우선순위 1이나 2의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.

5.1.3.7 인증 거부 리스트 탭

인증 거부 리스트 탭에서 사용자 ID 나 카드 번호를 등록하여 사용자의 출입 시도 시 장치에서 인증되지 않도록 설정할 수 있습니다.

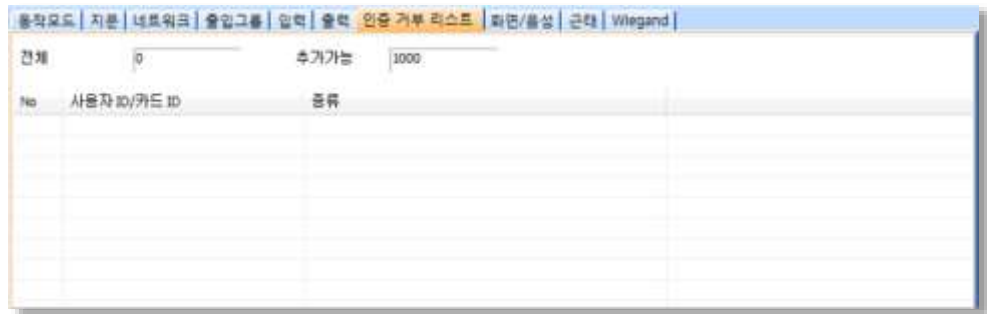


그림 5.9

- **전체:** 인증 거부 목록에 등록된 사용자 ID 나 카드의 총 수를 표시합니다.
- **추가가능:** 등록할 수 있는 사용자 ID 나 카드의 수를 표시합니다.

참고: 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있습니다.

5.1.3.8 화면/음성 탭

화면/음성 탭에서 BioLite Net 에서 발생하는 이벤트나 상태에 따라 LED 와 Buzzer 를 설정하여 작동상태를 표시할 수 있습니다. 설정 한 후 이벤트 별로 저장 버튼을 클릭해야 저장이 됩니다. 또한 화면에 표시할 언어 및 구성 파일을 설정할 수 있습니다.



그림 5.10

- **이벤트:** 설정을 적용할 이벤트를 선택합니다.
- **LED:** 선택한 이벤트 발생 시 LED의 행동 패턴을 설정합니다.
 - **횟수:** 선택한 이벤트 발생 시 LED의 반복 사이클을 설정합니다. 0을 입력하면 무한 반복되며 -1을 입력하면 LED가 작동하지 않습니다.

5. 사용자 설정

- 색상: 최대 3 개의 LED 색상을 선택합니다. 위에서 아래 순서대로 LED 의 색상이 바뀌면서 반복됩니다. 숫자 필드에는 각 색상이 지속되는 시간을 밀리초 단위로 입력합니다.
- **Buzzer:** 선택한 이벤트 발생 시 경고음의 패턴을 설정합니다.
 - 횟수: 경고음의 반복 횟수를 설정합니다. 0 을 입력하면 계속 경고음이 발생하며 -1 을 입력하면 경고음이 발생하지 않습니다.
 - 음량: 경고음의 크기(Low /Middle /High)를 설정합니다. 위에서 아래의 순서로 선택한 음량 크기대로 경고음이 반복됩니다. 숫자 필드에는 각 경고음이 지속되는 시간을 밀리초 단위로 입력합니다.
 - 페이드아웃: 경고음의 소리가 점차 작아집니다.
- 언어: 화면에 표시할 언어(한글, 영문, 사용자 정의)를 선택합니다
- 구성파일: BioLite Net 에서 사용할 언어 파일을 선택합니다. 영어나 한국어 이외의 언어 파일을 사용하려면, 줄임표(...)를 클릭한 다음, 언어 파일을 지정합니다.

5.1.3.9 근태 탭

근태 탭에서 BioLite Net 장치의 근태 키 입력 방식을 설정할 수 있습니다. 설정을 저장하려면 장치 창의 하단에 있는 **적용**을 클릭해야 합니다. **다른장치 적용**을 클릭하여 다른 장치에 현재 장치의 설정을 동일하게 적용할 수 있습니다.



그림 5.11

- **근태 키 입력 방식:** 장치에 적용할 근태 키 입력 방식을 선택합니다.
 - **사용 안함:** 이 옵션을 선택하면, 사용자는 장치에서 근태 이벤트를 기록할 수 없습니다.
 - **사용자 선택:** 이 옵션을 선택하면, 사용자는 근태 이벤트를 기록하려고 할 때마다 목적에 맞는 근태 기능키를 눌러야 합니다.
 - **선택 후 유지:** 이 옵션을 선택하면, 한 사용자가 특정 근태 기능키를 누를 경우 다른 근태 기능키를 누를 때까지 그 기능키가 유지됩니다.
 - **자동 설정:** 이 옵션을 선택하면, 설정된 출입시간 일정에 맞게 BioLite Net 장치가 자동으로 근태 기능을 표시합니다.
 - **이벤트 고정:** 이 옵션을 선택하면, BioLite Net 장치는 사용자가 설정한 근태 기능만 표시합니다.
- **관리:** 근태 기능에 사용할 키를 선택하고 어떤 근태 이벤트를 할당할지 설정합니다.

5. 사용자 설정

- **BioLite** 기능키: 아래 화살표를 클릭하여 목록에서 근태 기능에 사용할 키(<x1, >x1~>x15)를 선택합니다. **이벤트 고정** 방식을 선택하였다면, 오른쪽에 있는 **고정 이벤트체크** 상자를 선택합니다.
- **화면 표시 문구**: BioLite Net 화면에 표시할 근태 기능에 맞는 문구를 입력합니다.
- **자동 모드 적용 시간**: **자동 설정** 방식을 선택한 경우 아래 화살표를 클릭하여 목록에서 장치에 적용할 출입시간을 선택합니다. 선택한 시간에 맞추어 설정된 기능을 표시합니다. 출입시간의 추가 방법은 3.7.1 을 참조하십시오.
- **이벤트 종류**: 선택한 키에 할당할 이벤트의 종류(**사용 안함, 출근, 퇴근, 들어옴, 나감**)를 선택합니다. **출근** 또는 **퇴근**을 선택한 경우 **지각/조퇴 처리 안함** 체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면 사용자의 실제 출퇴근 시간에 관계없이 항상 정시에 출퇴근한 것으로 기록합니다.
근태 보고서의 결과에만 정시에 출퇴근한 것으로 기록하고 실제 근무 시간은 올바르게 계산하려면 **결과에만 적용체크** 상자를 선택합니다. **나감**을 선택한 경우에는 **이 이벤트 이후부터 근무시간에 포함체크** 상자를 선택할 수 있습니다. 이 옵션을 선택하면, 사용자가 근무상의 이유로 밖으로 나가는 것으로 간주하여 실제 근무 시간보다 빨리 나갔다고 하더라도 정상적으로 모든 시간을 근무한 것으로 기록합니다.

5.1.3.10 위갠드 탭

위갠드 탭에서 BioLite Net 에서 사용할 위갠드 형식을 설정할 수 있습니다. BioLite Net 에서 위갠드 기능을 사용하려면 **Wiegand 입력** 또는 **Wiegand 출력**을 설정합니다. Wiegand 설정 마법사를 실행하려면 **포맷 변경**을 클릭합니다. 위갠드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.

- **Wiegand 모드**: 카드 ID 데이터를 읽을 때 사용할 위갠드 모드(**일반모드, 확장모드**)를 선택합니다. 일반모드를 선택하면 BioLite Net 에 연결된 RF 장치는 BioLite Net 의 일부로 인식됩니다. 확장모드를 선택하면 BioLite Net 에 연결된 RF 장치는 독립된 장치로 인식됩니다. 확장모드를 이용할 경우 RF 장치는 자신의 ID 로 로그를 남길 뿐 아니라 출입문을 구성할 수 있으며 구역에 포함될 수 있습니다.
- **Wiegand 입력**: 위갠드 입력을 통해 받아들이는 ID 데이터를 어떻게 해석하여 처리할지 선택합니다.
 - **사용안함**: 위갠드 입력 신호를 받아들이지 않습니다.
 - **Wiegand (카드)**: 위갠드 입력을 통해 들어오는 ID 데이터를 카드 ID 로 해석하여 처리합니다.
 - **Wiegand (사용자)**: 위갠드 입력을 통해 들어오는 ID 데이터를 사용자 ID 로 해석하여 처리합니다.
- **Wiegand 출력**: 위갠드 출력을 통해 어떤 신호를 내보낼지 선택합니다.
 - **사용안함**: 위갠드 출력 신호를 내보내지 않습니다.
 - **Wiegand (카드)**: 인증에 성공한 사용자의 카드 ID 를 위갠드 출력 신호로 내보냅니다.
 - **Wiegand (사용자)**: 인증에 성공한 사용자의 사용자 ID 를 위갠드 출력 신호로 내보냅니다.

참고: Wiegand 입력과 Wiegand 출력은 BioStation 과는 달리 두 개중 하나만 선택하여 사용할 수 있습니다.

5. 사용자 설정

5.1.4 Xpass 설정 변경하기

이 절에서는 Xpass 에서 사용할 수 있는 설정에 대해서 설명합니다.

5.1.4.1 동작모드 탭

동작모드 탭에서 Xpass 의 시간을 변경할 수 있으며 동작 모드와 관련된 다양한 설정을 변경할 수 있습니다.

- **Xpass 시간**
 - 날짜: 장치에서 표시할 날짜를 직접 설정합니다.
 - 시간: 장치에서 표시할 시간을 직접 설정합니다.
 - 현재 PC 시간으로 동기화: BioStar 클라이언트 프로그램이 설치되어 있는 로컬 PC 의 날짜와 시간을 가져와 바로 아래 날짜와 시간 스피너 상자에 표시합니다. 시간 적용을 클릭하면, 장치의 날짜와 시간이 로컬 PC 의 날짜와 시간으로 설정됩니다.
 - 시간 가져오기: 현재 장치에서 표시되고 있는 시간을 가져옵니다.
 - 시간 적용: 장치의 시간을 설정한 시간으로 변경합니다.
- **동작 모드**: 아래의 옵션에서 이중 인증 방식 적용 체크 상자를 선택하면, 출입을 인증 받기 위해서는 두 사람이 동시에 인증을 해야 합니다.
 - 카드만 사용: 인증을 위해 장치가 카드만 요구하도록 설정합니다(**항상적용, 사용안함, 사용자가 설정한 출입시간**).
 - 서버 매칭: 카드가 일치하는지를 장치에서 판별하지 않고 BioStar 서버에서 판별하도록 설정합니다. 이 옵션을 선택하면, 장치는 카드의 일치 여부를 판별하기 위해 카드 ID 정보를 서버에 보냅니다. 사용자의 수가 너무 많아 개별 장치에 모든 정보를 저장할 수 없거나 또는 보안상의 이유로 개별 장치에 정보를 보관할 수 없을 때 이 옵션을 사용하면 편리합니다(**사용 안함, 사용**).
- **Mifare**
 - Mifare 사용 안함: MiFARE 카드를 이용한 인증을 금지합니다.
 - 데이터 카드 사용: 인증할 때에 MiFARE 카드에 저장된 사용자 데이터를 사용합니다. 지문 템플릿 정보는 제공되지 않습니다.
 - Mifare 레이아웃 보기: 장치에서 사용하고 있는 MiFARE 레이아웃을 확인합니다. MiFARE 레이아웃의 편집 방법은 3.6.4.7 을 참조하십시오.
- **카드 ID 포맷**
 - 포맷: 카드 ID 데이터를 어떤 방식으로 읽어 들일 것인가를 설정합니다. **일반**을 선택하면 카드 ID 데이터를 일반적인 형식으로 처리합니다. **Wiegand** 를 선택하면 위겐드 형식 설정에 따라 카드 ID 데이터를 처리합니다.
 - Byte Order: 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. **MSB** 를 선택하면 큰 단위의 바이트에서 작은 단위의 바이트 순으로 처리합니다. **LSB** 를 선택하면 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.
 - Bit Order: 카드 ID 데이터를 처리할 때 어떤 순서로 비트를 처리할지 선택합니다. **MSB** 를 선택하면 최상위 비트에서 최하위 비트 순으로 처리합니다. **LSB** 를 선택하면 최하위 비트에서 최상위 비트 순으로 처리합니다.
 - 이중 인증 모드에서 Admin User 를 반드시 포함하는 설정 옵션을 지원합니다. 이중 인증 모드 운영 시에는 Normal User 인증 후 15 초 이내에 반드시 Admin User 가 인증해야 Door Relay 가 켜집니다. 이 옵션을 사용하지 않는 경우 기존과 동일하게

5. 사용자 설정

Normal User 나 Admin User 여부와 관계 없이 다른 두 사용자가 15 초 이내에 인증하면 Door Relay 가 켜지게 됩니다.

주의: 이 기능은 펌웨어 버전 BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.

- Wiegand Card Bypass 사용: BioStar 의 Wiegand 설정에 따라 인증 성공 여부와 상관 없이 CSN 을 내보내는 기능으로, BioStar 제품군 장치를 타사 ACU 와 Wiegand 로 연동하여 인증 여부를 판단하고 출입문 제어 기능이 없는 Dummy 장치로 사용하고자 할 때 필요한 기능입니다. 카드가 입력되면 장치에서는 별도의 인증 처리 없이 바로 Wiegand 로 카드 ID 를 출력하게 됩니다.

주의: 이 기능은 펌웨어 버전 BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.

5.1.4.2 네트워크 탭

네트워크 탭에서 Xpass 의 네트워크 설정과 서버 설정을 변경할 수 있습니다.

- **TCP/IP**
 - **DHCP 사용:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용합니다.
 - **DHCP 사용 안함:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용하지 않습니다.
 - **IP 주소:** 장치의 IP 주소를 입력합니다.
 - **Sunet:** 장치의 서브넷 주소를 입력합니다.
 - **Gateway:** 네트워크의 게이트웨이를 입력합니다.
 - **포트:** 장치가 사용할 포트를 지정합니다.
- **MTU Size 설정 지원**
 - Black Fin 계열의 단말기는 MTU Size 설정을 지원합니다. 지원 패킷 사이즈는 1078-1514 이며, 기본값은 1514 입니다.
 - 주의:** 이 기능은 펌웨어 버전 BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.
- **서버**
 - **사용:** 서버 모드를 사용하려면 버튼을 클릭합니다.
 - **사용 안함:** 서버 모드를 사용하지 않습니다.
 - **IP 주소:** BioStar 서버의 IP 주소를 입력합니다.
 - **서버와 자동으로 시간 동기화:** 장치의 시간을 서버의 시간과 동기화합니다. 장치에서 1 시간마다 서버 시간을 폴링하여, 서버의 시간과 5 초 이상 차이가 나면, 서버의 시간과 동기화합니다.
- **100 Base-T 지원:** 이 옵션을 사용하여 네트워크에 연결하면 장치에서 빠른 속도를 이용할 수 있습니다. 이 옵션을 선택하면, 장치가 이더넷 네트워크에 연결될 때 지원되는 속도를 확인한 후 더 빠른 속도를 지원하는 방식으로 연결합니다. 이 옵션을 사용하지 않으면, 10Base-T 속도로 이더넷 네트워크에 연결합니다.
 - **사용:** 네트워크에서 지원하는 경우 100Base-T 속도로 연결합니다.
 - **사용 안함:** 100Base-T 속도를 사용하지 않습니다.
- **RS485**
 - **모드:** RS485 로 연결된 장치의 모드(**사용 안함, 호스트, 슬레이브, PC 연결 모드**)를 설정합니다.
 - **속도:** RS485 로 연결된 장치의 전송 속도(**9600-115200**)를 설정합니다.

5. 사용자 설정

5.1.4.3 출입그룹 탭

출입그룹 탭에서 Xpass 의 인증 제한 설정과 기본 출입그룹을 변경할 수 있으며 근태 모드를 설정할 수 있습니다.

인증 제한 설정

- **인증 간격(분):** 다시 출입할 수 있는 권한을 얻는 데까지 필요한 시간(분 단위)을 설정합니다. 사용자가 어느 구역에 입장하였으면, 지정된 시간 안에는 그 구역 안으로 다시 들어갈 수 없습니다.
- **제한 옵션 1~4:** 인증 제한 설정을 적용하려면 체크 상자를 선택한 후 이 설정을 적용할 시간을 입력합니다.
- **최대 인증 허용 횟수:** 지정된 인증 제한 시간 안에 허용할 최대 입장 수를 설정합니다.
- **기본 출입 그룹 설정:** 다른 출입그룹에 포함되지 않은 새로운 사용자에게 적용할 기본 출입그룹을 선택합니다.

5.1.4.4 입력 탭

입력 탭에는 Xpass 에 지정된 입력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 입력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Input 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 입력 설정의 구성 방법은 3.10.3.2 를 참조하십시오.



그림 5.12

- **장치:** 설정을 추가하거나 수정할 Xpass(또는 Secure I/O)를 선택합니다.
- **포트:** 입력 포트(입력 0, 입력 1, Tamper)를 선택합니다. Secure I/O 에서는 입력 0, 입력 1, 입력 2, 입력 3 을 선택할 수 있습니다.
- **스위치:** 버튼을 클릭하여 입력 스위치의 보통 상태(N/O: 평상시 열림, N/C: 평상시 닫힘)를 설정합니다.
- **기능:** 입력을 받았을 때 취할 동작을 선택합니다:
 - **사용 안함:** 입력 포트를 감시하지 않습니다.
 - **일반 입력:** 지정된 동작을 실행하기 위해 입력 포트를 감시합니다. (Output 설정 대화 상자에서 지정한 이벤트를 확인하려면 5.1.4.5 을 참조하십시오.)
 - **비상 문 열림:** 이 장치가 제어하고 있는 출입문을 엽니다. 일반적인 출입문 열림 시간은 무시되며, 관리자가 출입문/구역 감시 탭을 통해서 "문 닫기" 명령을 실행하기 전까지는 출입문이 열린 채로 남아 있습니다(4.4.1 참조).

5. 사용자 설정

- 모든 경보 해제: 이 장치와 연결된 모든 경보를 해제합니다.
- 장치 재 시작: 장치를 껐다가 다시 시작합니다.
- 장치 잠금: BioStar 와 장치 사이의 통신을 금지합니다. 통신을 다시 연결하려면, 관리자가 Xpass 의 마스터 비밀번호를 입력하거나 또는 Xpass 장치에서 직접 인증을 해야 합니다.
- BioStar 1.8v 에서 LED 녹색, LED 적색, 부저 입력, 출입 허가, 출입 거부 기능이 추가되었으며, BioStation (FW 1.93v), BioStation T2 (FW 1.3v), FaceStation (FW 1.3v), BioEntry Plus (FW 1.6v), BioEntry W (FW 1.2v), BioLite Net (FW 1.4v), Xpass (FW 1.3v) 에서만 지원됩니다.
- 동작시간: 입력 신호를 감시할 일정(사용안함, 항상적용)을 설정합니다.
- 입력시간(ms): 지정한 동작을 발생시키기 위해 필요한 입력 신호의 지속 시간(1000 분의 1 초)을 입력합니다.

5.1.4.5 출력 탭

출력 탭에는 Xpass 에 지정된 출력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 출력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 **Output 설정** 대화 상자에서 관련 옵션을 지정해야 합니다. 출력 설정을 구성하는 방법에 관한 자세한 내용은 3.10.3.1 을 참조하십시오.



그림 5.13

- **장치:** 설정을 추가하거나 수정할 장치의 종류를 선택합니다.
- **포트:** 출력 포트(릴레이 0)를 선택합니다. Secure I/O 에서는 릴레이 0, 릴레이 1 을 선택할 수 있습니다.
- **알람 동작 개시 이벤트:** 옵션을 설정하고 **추가**를 클릭하여 알람 동작 개시 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람을 발생시킵니다.
 - **이벤트:** 알람을 발생시킬 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
 - **장치:** 알람을 발생시키기 위해 감시할 장치를 선택합니다.
 - **신호파형:** 메뉴 표시줄의 **옵션 > 이벤트 > Output 포트 설정**을 통해서 이미 설정한 신호파형 중에서 하나를 선택합니다.

5. 사용자 설정

- **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선순위 2 의 알람 동작 개시 이벤트는 오직 우선순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.
- **알람 멈춤 이벤트:** 옵션을 설정하고 **추가**를 클릭하여 알람 멈춤 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람이 멈춥니다.
- **이벤트:** 알람을 멈추게 할 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
- **장치:** 알람을 멈추기 위해 감시할 장치를 선택합니다.
- **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선순위 2 의 알람 동작 개시 이벤트는 오직 우선순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.

5.1.4.6 인증거부리스트

BioStar 1.8부터 인증거부 리스트를 Xpass에서도 지원 합니다.
(이 기능은 펌웨어 버전 Xpass 1.3 이상 지원됩니다.)

5.1.4.7 커맨드카드 탭

커맨드카드 탭에서 커맨드 카드를 발급할 수 있습니다. 커맨드 카드 발급에 관한 자세한 내용은 3.2.8.1 을 참조하십시오.

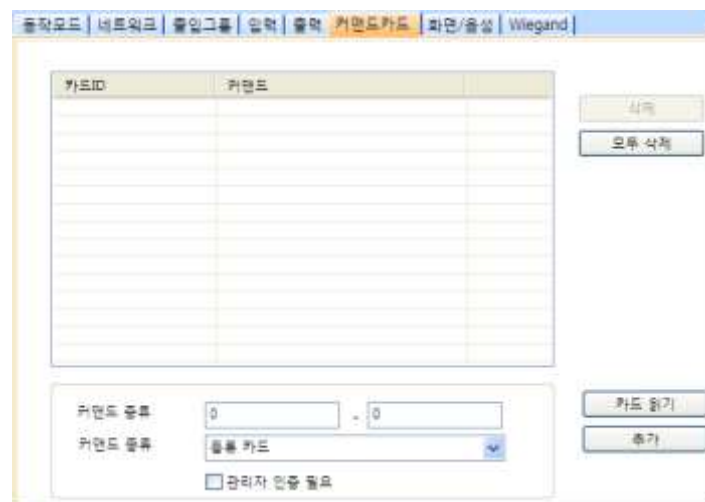


그림 5.14

- **카드 ID:** 카드 ID 를 직접 입력하거나 또는 **카드 읽기**를 클릭한 후 장치에 카드를 올려놓으면 카드 ID 가 자동적으로 입력됩니다.
- **커맨드 종류:** 발급할 커맨드 카드의 종류(등록 카드, 삭제 카드, 모두 삭제 카드)를 선택합니다.

5. 사용자 설정

5.1.4.8 화면/음성 탭

화면/음성 탭에서 Xpass 에서 발생하는 이벤트나 상태에 따라 LED 와 Buzzer 를 설정하여 작동상태를 표시할 수 있습니다. 설정 한 후 이벤트 별로 저장 버튼을 클릭해야 저장이 됩니다.

동작모드 | 네트워크 | 출입그룹 | 입력 | 출력 | 커맨드카드 | 화면/음성 | Wiegand

Output 신호

이벤트: 일반 상태

LED

횟수: 0 (-1 : 사용안함, 0: 반복)

파란색: 2000 msec, 0 msec

하늘색: 2000 msec, 0 msec

없음: 0 msec, 0 msec

Buzzer

횟수: -1 (-1 : 사용안함, 0: 반복)

없음: 0 msec, 0 msec, 페이드아웃

없음: 0 msec, 0 msec, 페이드아웃

없음: 0 msec, 0 msec, 페이드아웃

그림 5.15

- **이벤트:** 설정을 적용할 이벤트를 선택합니다.
- **LED:** 선택한 이벤트 발생 시 LED의 행동 패턴을 설정합니다.
 - **횟수:** 선택한 이벤트 발생 시 LED의 반복 사이클을 설정합니다. 0을 입력하면 무한 반복되며 -1을 입력하면 LED가 작동하지 않습니다.
 - **색상:** 최대 3개의 LED 색상을 선택합니다. 위에서 아래 순서대로 LED의 색상이 바뀌면서 반복됩니다. 숫자 필드에는 각 색상이 지속되는 시간을 밀리초 단위로 입력합니다.
- **Buzzer:** 선택한 이벤트 발생 시 경고음의 패턴을 설정합니다.
 - **횟수:** 경고음의 반복 횟수를 설정합니다. 0을 입력하면 계속 경고음이 발생하며 -1을 입력하면 경고음이 발생하지 않습니다.
 - **음량:** 경고음의 크기(Low /Middle /High)를 설정합니다. 위에서 아래의 순서로 선택한 음량 크기대로 경고음이 반복됩니다. 숫자 필드에는 각 경고음이 지속되는 시간을 밀리초 단위로 입력합니다.
 - **페이드아웃:** 경고음의 소리가 점차 작아집니다.

5. 사용자 설정

5.1.4.9 위갠드 탭

위갠드 탭에서 Xpass 에서 사용할 위갠드 형식을 설정할 수 있습니다. Xpass 에서 위갠드 기능을 사용하려면 **Wiegand Input** 과 **Wiegand Out** 을 설정합니다. Wiegand 설정 마법사를 실행하려면 **포맷 변경**을 클릭합니다. 위갠드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.

- **Wiegand 모드:** 카드 ID 데이터를 읽을 때 사용할 위갠드 모드(**일반모드**, **확장모드**)를 선택합니다. 일반모드를 선택하면 Xpass 에 연결된 RF 장치는 Xpass 의 일부로 인식됩니다. 확장모드를 선택하면 Xpass 에 연결된 RF 장치는 독립된 장치로 인식됩니다. 확장모드를 이용할 경우 RF 장치는 자신의 ID 로 로그를 남길 뿐 아니라 출입문을 구성할 수 있으며 구역에 포함될 수 있습니다.
- **Wiegand 입력:** 위갠드 입력을 통해 받아들이는 ID 데이터를 어떻게 해석하여 처리할지 선택합니다.
 - **사용안함:** 위갠드 입력 신호를 받아들이지 않습니다.
 - **Wiegand (카드):** 위갠드 입력을 통해 들어오는 ID 데이터를 카드 ID 로 해석하여 처리합니다.
 - **Wiegand (사용자):** 위갠드 입력을 통해 들어오는 ID 데이터를 사용자 ID 로 해석하여 처리합니다.
- **Wiegand 출력:** 위갠드 출력을 통해 어떤 신호를 내보낼지 선택합니다.
 - **사용안함:** 위갠드 출력 신호를 내보내지 않습니다.
 - **Wiegand (카드):** 인증에 성공한 사용자의 카드 ID 를 위갠드 출력 신호로 내보냅니다.
 - **Wiegand (사용자):** 인증에 성공한 사용자의 사용자 ID 를 위갠드 출력 신호로 내보냅니다.

5.1.5 Xpass S2 설정 변경하기

이 절에서는 Xpass S2 에서 사용할 수 있는 설정에 대해서 설명합니다. 이러한 설정을 변경하여 현재 처해있는 상황이나 운영상의 필요에 맞게 Xpass S2 의 기능을 변경할 수 있습니다.

5.1.5.1 동작모드 탭

동작모드 탭에서 Xpass S2 의 시간을 변경할 수 있으며 동작 모드와 관련한 다양한 설정을 변경할 수 있습니다.

- **Xpass S2 시간**
 - **날짜:** 장치에 표시할 날짜를 설정합니다.
 - **시간:** 장치에서 표시할 시간을 설정합니다.
 - **현재 PC 시간으로 동기화:** BioStar 클라이언트 프로그램이 설치되어 있는 로컬 PC 의 날짜와 시간을 가져와 바로 아래 날짜와 시간 스피너 상자에 표시합니다. 시간 적용을 클릭하면, 장치의 날짜와 시간이 로컬 PC 의 날짜와 시간으로 설정됩니다.
 - **시간 가져오기:** 현재 장치에서 표시되고 있는 시간을 가져옵니다.
 - **시간 적용:** 장치의 시간을 설정한 시간으로 변경합니다.

5. 사용자 설정

- 동작 모드: 아래의 옵션에서 이중 인증 방식 적용 체크 상자를 선택하면, 출입을 인증 받기 위해서는 두 사람이 동시에 인증을 해야 합니다.
 - **카드만 사용**: 인증을 위해 장치가 카드만 요구하도록 설정합니다(**항상적용, 사용안함, 사용자가 설정한 출입시간**).
 - **서버 매칭**: 카드가 일치하는지를 장치에서 판별하지 않고 BioStar 서버에서 판별하도록 설정합니다. 이 옵션을 선택하면, 장치는 카드의 일치 여부를 판별하기 위해 카드 ID 정보를 서버에 보냅니다. 사용자의 수가 너무 많아 개별 장치에 모든 정보를 저장할 수 없거나 또는 보안상의 이유로 개별 장치에 정보를 보관할 수 없을 때 이 옵션을 사용하면 편리합니다(**사용 안함, 사용**).
- **Mifare**: Mifare 템플릿 카드는 지원되지 않습니다.
- 카드 ID 포맷
 - **포맷**: 카드 ID 데이터를 어떤 방식으로 읽어 들일 것인가를 설정합니다. 일반을 선택하면 카드 ID 데이터를 일반적인 형식으로 처리합니다. Wiegand 를 선택하면 위간드 형식 설정에 따라 카드 ID 데이터를 처리합니다.
 - **Byte Order**: 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. MSB 를 선택하면 큰 단위의 바이트에서 작은 단위의 바이트 순으로 처리합니다. LSB 를 선택하면 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.
 - **Bit Order**: 카드 ID 데이터를 처리할 때 어떤 순서로 비트를 처리할지 선택합니다. MSB 를 선택하면 최상위 비트에서 최하위 비트 순으로 처리합니다. LSB 를 선택하면 최하위 비트에서 최상위 비트 순으로 처리합니다.

5.1.5.2 네트워크 탭

네트워크 탭에서 Xpass S2의 네트워크 설정과 서버 설정을 변경할 수 있습니다.

- **TCP/IP**
 - **DHCP 사용**: 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용합니다.
 - **DHCP 사용 안함**: 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용하지 않습니다.
 - **IP 주소**: 장치의 IP 주소를 입력합니다.
 - **Sunet**: 장치의 서브넷 주소를 입력합니다.
 - **Gateway**: 네트워크의 게이트웨이를 입력합니다.
 - **포트**: 장치가 사용할 포트를 지정합니다.
- **서버**
 - **사용**: 서버 모드를 사용합니다.
 - **사용 안함**: 서버 모드를 사용하지 않습니다.
 - **IP 주소**: BioStar 서버의 IP 주소를 입력합니다.
 - **서버와 자동으로 시간 동기화**: 장치의 시간을 서버의 시간과 동기화합니다. 장치에서 1 시간마다 서버 시간을 폴링하여, 서버의 시간과 5 초 이상 차이가 나면, 서버의 시간과 동기화합니다.
- **100 Base-T 지원**: 이 옵션을 사용하여 네트워크에 연결하면 장치에서 빠른 속도를 이용할 수 있습니다. 이 옵션을 선택하면, 장치가 이더넷 네트워크에 연결될 때 지원되는 속도를 확인한 후 더 빠른 속도를 지원하는 방식으로 연결합니다. 이 옵션을 사용하지 않으면, 10Base-T 속도로 이더넷 네트워크에 연결합니다.

5. 사용자 설정

- **사용:** 네트워크에서 지원하는 경우 100Base-T 속도로 연결합니다.
- **사용 안함:** 100Base-T 속도를 사용하지 않습니다.
- **RS485**
 - **모드:** RS485 로 연결된 장치의 모드(**사용 안함, 호스트, 슬레이브, PC 연결 모드**)를 설정합니다.
 - **속도:** RS485 로 연결된 장치의 전송 속도(**9600-115200**)를 설정합니다.

5.1.5.3 출입그룹 탭

출입그룹 탭에서 Xpass S2 의 인증 제한 설정과 기본 출입그룹을 변경할 수 있으며 근태 모드를 설정할 수 있습니다.

- **인증 제한 설정**
 - **인증 간격(분):** 다시 출입할 수 있는 권한을 얻는 데까지 필요한 시간(분 단위)을 설정합니다. 사용자가 어느 구역에 입장하였으면, 지정된 시간 안에는 그 구역 안으로 다시 입장할 수 없습니다.
 - **제한 옵션 1~4:** 인증 제한 설정을 적용하려면 체크 상자를 선택한 후 이 설정을 적용할 시간을 입력합니다.
 - **최대 인증 허용 횟수:** 지정된 인증 제한 시간 안에 허용할 최대 입장 수를 설정합니다.
- **기본 출입 그룹 설정:** 다른 출입그룹에 포함되지 않은 새로운 사용자에게 적용할 기본 출입그룹을 선택합니다.

5.1.5.4 입력 탭

입력 탭에는 Xpass S2 에 지정된 입력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 입력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Input 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 입력 설정을 구성하는 방법에 관한 자세한 내용은 3.10.3.2 를 참조하십시오.

- **장치:** 설정을 추가하거나 수정할 Xpass S2 (또는 Secure I/O)를 선택합니다.
- **포트:** 입력 포트(**입력 0, 입력 1, Tamper**)를 선택합니다. Secure I/O 에서는 **입력 0, 입력 1, 입력 2, 입력 3** 을 선택할 수 있습니다.
- **스위치:** 버튼을 클릭하여 입력 스위치의 보통 상태(**N/O: 평상시 열림, N/C: 평상시 닫힘**)를 설정합니다.

5. 사용자 설정

- 기능: 입력을 받았을 때 취할 동작을 선택합니다.
 - 사용 안함: 입력 포트를 감시하지 않습니다.
 - 일반 입력: 지정된 동작을 실행하기 위해 입력 포트를 감시합니다. (Output 설정 대화 상자에서 지정한 이벤트를 확인하려면 5.1.5.5 을 참조하십시오.)
 - 비상 문 열림: 이 장치가 제어하고 있는 출입문을 엽니다. 일반적인 출입문 열림 시간은 무시되며, 관리자가 출입문/구역 감시 탭을 통해서 "문 닫기" 명령을 실행하기 전까지는 출입문이 열린 채로 남아 있습니다(4.4.1 참조).
 - 모든 경보 해제: 이 장치와 연결된 모든 경보를 해제합니다.
 - 장치 재 시작: 장치를 껐다가 다시 시작합니다.
 - 장치 잠금: BioStar 와 장치 사이의 통신을 금지합니다. 통신을 다시 연결하려면, 관리자가 Xpass S2 의 마스터 비밀번호를 입력하거나 또는 Xpass S2 장치에서 직접 인증을 해야 합니다.
- 동작시간: 입력 신호를 감시할 일정(사용안함, 항상적용)을 설정합니다.
- 입력시간(ms): 지정한 동작을 발생시키기 위해 필요한 입력 신호의 지속 시간(1000 분의 1 초)을 입력합니다.

5.1.5.5 출력 탭

출력 탭에는 Xpass S2 에 지정된 출력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 출력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Output 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 출력 설정을 구성하는 방법에 관한 자세한 내용은 3.10.3.1 을 참조하십시오.



- 장치: 설정을 추가하거나 수정할 장치의 종류를 선택합니다.
- 포트: 출력 포트(릴레이 0)를 선택합니다. Secure I/O 에서는 릴레이 0, 릴레이 1 을 선택할 수 있습니다.
- 알람 동작 개시 이벤트: 옵션을 설정하고 추가를 클릭하여 알람 동작 개시 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람을 발생시킵니다.
 - 이벤트: 알람을 발생시킬 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
 - 장치: 알람을 발생시키기 위해 감시할 장치를 선택합니다.

5. 사용자 설정

- 신호파형: 메뉴 표시줄의 **옵션 > 이벤트 > Output 포트 설정**을 통해서 이미 설정한 신호파형 중에서 하나를 선택합니다.
- 우선순위: 이벤트의 우선 순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선 순위 2 의 알람 동작 개시 이벤트는 오직 우선 순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.
- **알람 멈춤 이벤트:** 옵션을 설정하고 **추가**를 클릭하여 알람 멈춤 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람이 멈춥니다.
- 이벤트: 알람을 멈추게 할 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
- 장치: 알람을 멈추기 위해 감시할 장치를 선택합니다.
- 우선순위: 이벤트의 우선 순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선 순위 2 의 알람 동작 개시 이벤트는 오직 우선 순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.

5.1.5.6 커맨드카드 탭

커맨드카드 탭에서 커맨드 카드를 발급할 수 있습니다. 커맨드 카드 발급에 관한 자세한 내용은 3.2.8.1 을 참조하십시오.

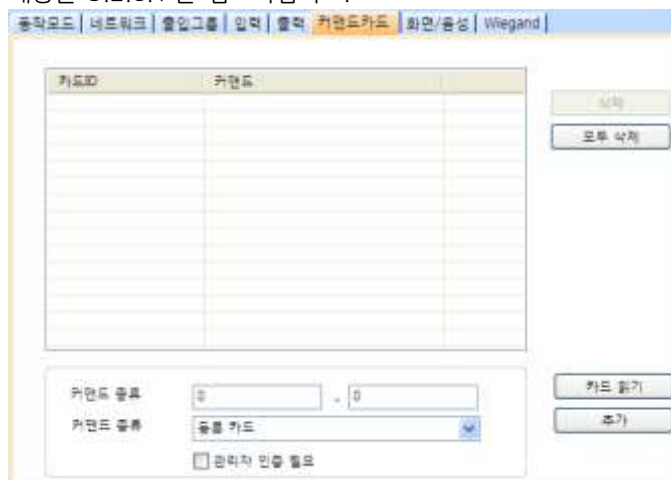


그림 5.16

- **카드 ID:** 카드 ID 를 직접 입력하거나 또는 **카드 읽기**를 클릭한 후 장치에 카드를 올려놓으면 카드 ID 가 자동적으로 입력됩니다.
- **커맨드 종류:** 발급할 커맨드 카드의 종류(등록 카드, 삭제 카드, 모두 삭제 카드)를 선택합니다.

5. 사용자 설정

5.1.5.7 화면/음성 탭

화면/음성 탭에서 Xpass S2 에서 발생하는 이벤트나 상태에 따라 LED 와 Buzzer 를 설정하여 작동상태를 표시할 수 있습니다. 설정한 후 이벤트 별로 저장 버튼을 클릭해야 저장이 됩니다.

Output 신호

이벤트: 일반 상태

LED

횟수: 0 (-1 : 사용안함, 0: 반복)

파란색: 2000 msec, 0 msec

하늘색: 2000 msec, 0 msec

없음: 0 msec, 0 msec

Buzzer

횟수: -1 (-1 : 사용안함, 0: 반복)

없음: 0 msec, 0 msec 페이드아웃

없음: 0 msec, 0 msec 페이드아웃

없음: 0 msec, 0 msec 페이드아웃

- **이벤트:** 설정을 적용할 이벤트를 선택합니다.
- **LED:** 선택한 이벤트 발생 시 LED의 행동 패턴을 설정합니다.
 - **횟수:** 선택한 이벤트 발생 시 LED의 반복 사이클을 설정합니다. 0을 입력하면 무한 반복되며 -1을 입력하면 LED가 작동하지 않습니다.
 - **색상:** 최대 3개의 LED 색상을 선택합니다. 위에서 아래 순서대로 LED의 색상이 바뀌면서 반복됩니다. 숫자 필드에는 각 색상이 지속되는 시간을 밀리초 단위로 입력합니다.
- **Buzzer:** 선택한 이벤트 발생 시 경고음의 패턴을 설정합니다.
 - **횟수:** 경고음의 반복 횟수를 설정합니다. 0을 입력하면 계속 경고음이 발생하며 -1을 입력하면 경고음이 발생하지 않습니다.
 - **음량:** 경고음의 크기(Low /Middle /High)를 설정합니다. 위에서 아래의 순서로 선택한 음량 크기대로 경고음이 반복됩니다. 숫자 필드에는 각 경고음이 지속되는 시간을 밀리초 단위로 입력합니다.
 - **페이드아웃:** 경고음의 소리가 점차 작아집니다.

5. 사용자 설정

5.1.5.8 위캔드 탭

위캔드 탭에서 Xpass S2 에서 사용할 위캔드 형식을 설정할 수 있습니다. Xpass S2 에서 위캔드 기능을 사용하려면 **Wiegand Input** 과 **Wiegand Out** 을 설정합니다. Wiegand 설정 마법사를 실행하려면 **포맷 변경**을 클릭합니다. 위캔드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.

- **Wiegand 모드:** 카드 ID 데이터를 읽을 때 사용할 위캔드 모드(**일반모드**, **확장모드**)를 선택합니다. 일반모드를 선택하면 Xpass S2 에 연결된 RF 장치는 Xpass S2 의 일부로 인식됩니다. 확장모드를 선택하면 Xpass S2 에 연결된 RF 장치는 독립된 장치로 인식됩니다. 확장모드를 이용할 경우 RF 장치는 자신의 ID 로 로그를 남길 뿐 아니라 출입문을 구성할 수 있으며 구역에 포함될 수 있습니다.
- **Wiegand 입력:** 위캔드 입력을 통해 받아들이는 ID 데이터를 어떻게 해석하여 처리할지 선택합니다.
 - **사용안함:** 위캔드 입력 신호를 받아들이지 않습니다.
 - **Wiegand (카드):** 위캔드 입력을 통해 들어오는 ID 데이터를 카드 ID 로 해석하여 처리합니다.
 - **Wiegand (사용자):** 위캔드 입력을 통해 들어오는 ID 데이터를 사용자 ID 로 해석하여 처리합니다.
- **Wiegand 출력:** 위캔드 출력을 통해 어떤 신호를 내보낼지 선택합니다.
 - **사용안함:** 위캔드 출력 신호를 내보내지 않습니다.
 - **Wiegand (카드):** 인증에 성공한 사용자의 카드 ID 를 위캔드 출력 신호로 내보냅니다.
 - **Wiegand (사용자):** 인증에 성공한 사용자의 사용자 ID 를 위캔드 출력 신호로 내보냅니다.

5.1.6 X-Station 설정 변경하기

이 절에서는 X-Station 에서 사용할 수 있는 설정에 대해서 설명합니다. 이러한 설정을 변경하여 현재 처해있는 상황이나 운영상의 필요에 맞게 X-Station 의 기능을 변경할 수 있습니다.

5.1.6.1 동작모드 탭

동작모드 탭에서 X-Station 의 시간을 변경할 수 있으며 동작 모드와 관련한 다양한 설정을 변경할 수 있습니다.

- **X-Station 시간**
 - **날짜:** 장치에 표시할 날짜를 설정합니다.
 - **시간:** 장치에서 표시할 시간을 설정합니다.
 - **현재 PC 시간으로 동기화:** BioStar 클라이언트 프로그램이 설치되어 있는 로컬 PC 의 날짜와 시간을 가져와 바로 아래 날짜와 시간 스피너 상자에 표시합니다. 시간 적용을 클릭하면, 장치의 날짜와 시간이 로컬 PC 의 날짜와 시간으로 설정됩니다.
 - **시간 가져오기:** 현재 장치에서 표시되고 있는 시간을 가져옵니다.
 - **시간 적용:** 장치의 시간을 설정한 시간으로 변경합니다.
- **1:1 동작 모드 설정:** 이 영역에서는 일정에 따라 각각 다른 인증 모드가 적용되도록 설정할 수 있습니다. 예를 들어, 근무 시간에는 일반적인 인증 모드를 적용하고 근무

5. 사용자 설정

시간 이외에는 좀더 엄격한 인증모드를 적용할 수 있습니다. 장치에 설정된 인증 모드를 적용할지 아니면 개별 사용자에게 설정된 인증 모드를 적용할지도 여기에서 설정할 수 있습니다(5.4.1 참조). 사용자의 인증 모드를 개별적으로 설정하지 않았다면, 장치에 설정된 인증 모드가 적용됩니다.

- **카드:** 인증을 위해 장치가 카드만 요구하도록 설정합니다.
- **ID/카드 + 패스워드:** 인증을 위해 장치가 ID와 패스워드를 요구하도록 설정합니다.
- **개인별 인증:** 개인에게 설정된 인증 방식을 사용하여 인증하도록 설정합니다 (**사용 안함, 사용**).
- **이중 인증 시간:** 인증을 위해 장치가 두 사람의 카드를 요구하도록 설정합니다(**항상 적용, 사용 안함**). 15 초 이내에 두 번째 사용자의 카드를 인증하지 않으면 인증이 무효가 됩니다.
- **서버 매칭:** 장치 대신에 BioStar 서버에서 카드 ID 매칭을 수행합니다. 설정 시 장치는 카드 ID 정보를 서버로 전송하여 매칭을 확인합니다. 이 설정은 장치에 저장할 수 있는 사용자보다 더 많은 사용자가 있을 때 유용합니다.
- **인증타임아웃:** 인증 시 장치가 인증 대기 상태로 돌아갈 시간을 설정합니다.
- **얼굴 검출:** 인증이 성공하였을 때 얼굴 이미지를 강제로 검출하여 출입하는 사용자의 얼굴 이미지를 확보합니다.
- **Mifare 설정**
 - **Mifare 사용 안함:** MiFARE 카드를 이용한 인증을 금지합니다.
 - **데이터 카드 사용:** 인증할 때에 MiFARE 카드에 저장된 사용자 정보를 사용합니다. 지문 정보는 제공하지 않습니다.
 - **Mifare 레이아웃 보기:** 장치에서 사용하고 있는 MiFARE 레이아웃을 확인합니다. MiFARE 레이아웃의 편집 방법은 3.6.4.7을 참조하십시오.
- **카드 ID 포맷**
 - **포맷:** 카드 ID 데이터를 어떤 방식으로 읽어 들일 것인가를 설정합니다. **일반**을 선택하면 카드 ID 데이터를 일반적인 형식으로 처리합니다. **Wiegand**를 선택하면 위간드 형식 설정에 따라 카드 ID 데이터를 처리합니다.
 - **Byte Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. **MSB**를 선택하면 큰 단위의 바이트에서 작은 단위의 바이트 순으로 처리합니다. **LSB**를 선택하면 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.
 - **Bit Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 비트를 처리할지 선택합니다. **MSB**를 선택하면 최상위 비트에서 최하위 비트 순으로 처리합니다. **LSB**를 선택하면 최하위 비트에서 최상위 비트 순으로 처리합니다.

5. 사용자 설정

5.1.6.2 카메라 탭

카메라 탭에서 X-Station의 카메라 설정을 변경할 수 있습니다. 특정 이벤트에 따라 카메라의 작동을 설정할 수 있습니다. 카메라를 작동할 이벤트를 추가하고 적용을 클릭하여 변경 사항을 저장합니다.



그림 5.17

주의: 보안을 위해 카메라 이벤트에 인증 이벤트를 추가할 것을 권장합니다. 장치와 서버간의 네트워크 부하를 줄이기 위해 최대 30 개의 이벤트만 추가하십시오.

5.1.6.3 네트워크 탭

네트워크 탭에서 X-Station의 네트워크 설정과 서버 설정을 변경할 수 있습니다.



- TCP/IP 설정
 - 네트워크 종류: 랜의 종류(사용 안함, 이더넷)를 선택합니다.
 - 포트: 장치가 사용할 포트를 지정합니다.
- IP
 - DHCP 사용: 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용합니다.
 - DHCP 사용 안함: 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용하지 않습니다.
 - IP 주소: 장치의 IP 주소를 입력합니다.
 - 서브넷: 장치의 서브넷 주소를 입력합니다.
 - 게이트웨이: 네트워크의 게이트웨이를 입력합니다.

5. 사용자 설정

- 최대 연결 갯수: 허용할 최대 연결 수를 지정합니다.
- 서버
 - 사용: 서버 모드(장치를 BioStar 서버에 연결)를 사용합니다.
 - 사용 안함: 서버 모드를 사용하지 않습니다.
 - IP 주소: BioStar 서버의 IP 주소를 입력합니다.
 - 서버 포트: BioStar 가 사용하는 포트를 입력합니다.
 - 서버와 자동으로 시간 동기화: 장치의 시간을 서버의 시간과 동기화합니다. 장치에서 1 시간마다 서버 시간을 풀링하여, 서버의 시간과 5 초 이상 차이가 나면, 서버의 시간과 동기화합니다.
- RS485
 - 모드: RS485로 연결된 장치의 모드(사용 안함, 호스트, 슬레이브)를 설정합니다. RS485 모드에 관한 자세한 내용은 3.2.1 과 3.2.2 를 참조하십시오.
 - 속도: RS485로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.

5.1.6.4 출입그룹 탭

출입그룹 탭에서 X-Station의 인증 제한 설정과 기본 출입그룹을 변경할 수 있습니다.



- 인증 제한 설정
 - 인증 간격(분): 다시 출입할 수 있는 권한을 얻는 데까지 필요한 시간(분 단위)을 설정합니다. 사용자가 어느 구역에 입장하였으면, 지정된 시간 안에는 그 구역 안으로 다시 입장할 수 없습니다.
 - 옵션 1~4: 인증 제한 설정을 적용하려면 체크 상자를 선택한 후 이 설정을 적용할 시간을 입력합니다.
 - 최대 인증 허용 횟수: 지정된 인증 제한 시간 안에 허용할 최대 입장 수를 설정합니다.
- 기본 출입 그룹 설정: 다른 출입그룹에 포함되지 않은 새로운 사용자에게 적용할 기본 출입그룹을 선택합니다.

5. 사용자 설정

5.1.6.5 인터폰 탭

X-Station의 인터폰 기능을 사용하여 출입문 안쪽에 있는 상대방과 전화 통화할 수 있습니다.

The screenshot shows the '인터폰' (Intercom) settings page. At the top, there is a navigation bar with tabs: 동작모드, 카메라, 네트워크, 출입그룹, 인터폰, 입력, 출력, 인증 거부 리스트, 화면/음성, 근태, 위전드. The '종류' (Type) dropdown is set to '바이오스타 비디오폰'. The '인터폰' section contains the following fields: '비디오 서버 IP' (192 . 168 . 1 . 172), 'VOIP 표시명' (555), 'VOIP ID' (176), '스피커 게인' (10), 'VOIP 전화번호' (174), 'VOIP 비밀번호' (176), and '마이크 게인' (6). The '비디오폰' section includes a 'Mode' dropdown set to '단일', a checked '출입문 제어' checkbox, and a '장치 비밀번호' field with four asterisks.

아날로그 인터폰, IP 인터폰, BioStar VideoPhone 등 3 가지 종류가 지원됩니다. BioStar VideoPhone 은 음성 및 영상 통화가 지원되는 인터폰으로서, X-Station V1.2 이상의 펌웨어에서만 지원됩니다. 별도로 제공되는 프로그램을 PC 에 설치해야 합니다. 프로그램 설치 및 사용 방법은 BioStar VideoPhone 사용자 매뉴얼을 참조하십시오.

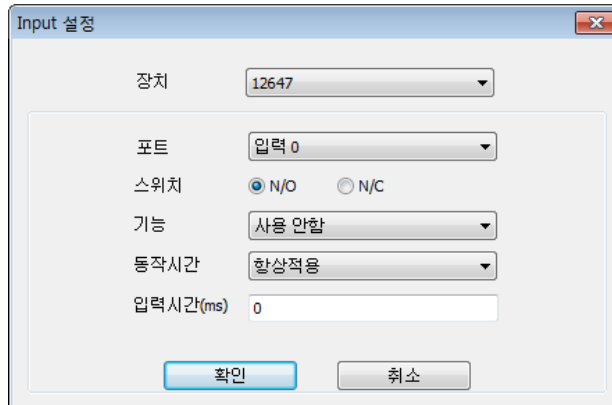
사용하고자 하는 인터폰 종류에 따라 다음 옵션을 설정할 수 있습니다.

- **인터폰**
 - **VOIP 서버 IP:** VoIP 서버의 IP 주소를 입력합니다.
 - **VOIP 표시명:** VoIP의 사용자 지정 이름을 입력합니다.
 - **VOIP 전화번호:** VoIP 전화번호를 입력합니다.
 - **VOIP ID:** VoIP 서버의 ID를 입력합니다.
 - **VOIP 비밀번호:** VoIP 서버의 비밀번호를 입력합니다.
 - **스피커 게인:** 스피커의 음량을 조절합니다(1~10).
 - **마이크 게인:** 마이크의 음량을 조절합니다(1~10).
- **비디오폰**
 - **모드:** 단일 또는 내선 2 가지 모드가 지원됩니다. 단일 모드는 장치에서 1 대의 PC와 연결 가능하며, 내선 모드는 최대 8대의 PC와 연결할 수 있습니다.
 - **장치 비밀번호:** 장치에서 설정한 비밀번호를 입력합니다. 이 비밀번호는 BioStar VideoPhone 프로그램에서 장치에 로그인하기 위해 필요합니다.
 - **출입문 제어:** PC에서 원격으로 출입문을 열 수 있도록 허용합니다.

5. 사용자 설정

5.1.6.6 입력 탭

입력 탭에는 X-Station 에 지정된 입력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 입력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Input 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 입력 설정의 구성 방법은 3.10.3.2 를 참조하십시오.



- **장치:** 설정을 추가하거나 수정할 X-Station(또는 Secure I/O)을 선택합니다.
- **포트:** Secure I/O 와 동일하게 **입력 0, 입력 1, 입력 2, 입력 3** 을 선택할 수 있습니다.
- **스위치:** 버튼을 클릭하여 입력 스위치의 보통 상태(**N/O**: 평상시 열림, **N/C**: 평상시 닫힘)를 설정합니다.
- **기능:** 입력을 받았을 때 취할 동작을 선택합니다:
 - **사용 안함:** 입력 포트를 감시하지 않습니다.
 - **일반 입력:** 지정된 동작을 실행하기 위해 입력 포트를 감시합니다. (Output 설정 대화 상자에서 지정한 이벤트를 확인하려면 5.1.6.7 을 참조하십시오.)
 - **비상 문 열림:** 이 장치가 제어하고 있는 출입문을 엽니다. 일반적인 출입문 열림 시간은 무시되며, 관리자가 출입문/구역 감시 탭을 통해서 "문 닫기" 명령을 실행하기 전까지는 출입문이 열린 채로 남아 있습니다(4.4.1 참조).
 - **모든 경보 해제:** 이 장치와 연결된 모든 경보를 해제합니다.
 - **장치 재 시작:** 장치를 껐다가 다시 시작합니다.
 - **장치 잠금:** 장치가 잠깁니다. 잠긴 장치는 BioStar 서버와 통신할 수 없으며 또한 지문이나 카드 입력을 처리할 수 없습니다. 통신을 다시 연결하려면, 관리자가 X-Station 에서 직접 인증을 해야 합니다.
- **동작시간:** 입력 신호를 감시할 일정(**사용안함, 항상적용**)을 설정합니다.
- **입력시간(ms):** 지정한 동작을 발생시키기 위해 필요한 입력 신호의 지속 시간(1000 분의 1 초)을 입력합니다.

5. 사용자 설정

5.1.6.7 출력 탭

출력 탭에는 X-Station 에 적용되는 출력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 출력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Output 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 출력 설정의 구성 방법은 3.10.3.1 을 참조하십시오.



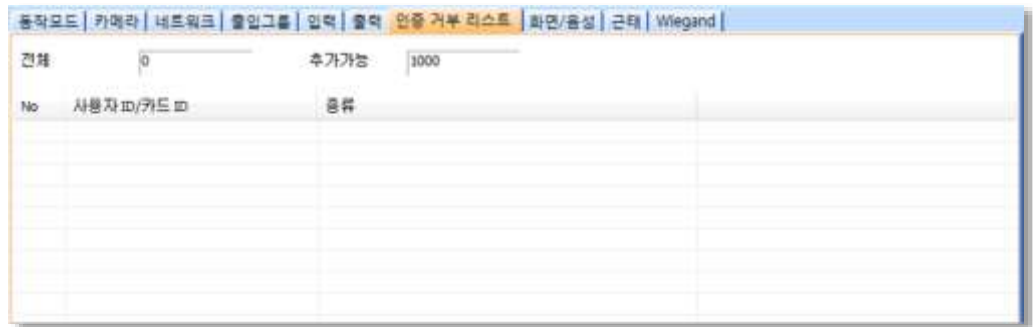
- **장치:** 설정을 추가하거나 수정할 장치의 종류를 선택합니다.
- **포트:** Secure I/O 와 동일하게 릴레이 0, 릴레이 1 을 선택할 수 있습니다.
- **알람 동작 개시 이벤트:** 옵션을 설정하고 **추가**를 클릭하여 알람 동작 개시 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람을 발생시킵니다.
 - **이벤트:** 알람을 발생시킬 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
 - **장치:** 알람을 발생시키기 위해 감시할 장치를 선택합니다.
 - **신호파형:** 메뉴 표시줄의 **옵션 > 이벤트 > Output 포트 설정**을 통해서 이미 설정한 신호파형 중에서 하나를 선택합니다.
 - **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선순위 2 의 알람 동작 개시 이벤트는 오직 우선순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.
- **알람 멈춤 이벤트:** 옵션을 설정하고 **추가**를 클릭하여 알람 멈춤 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람이 중단됩니다.
 - **이벤트:** 알람을 멈추게 할 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
 - **장치:** 알람을 멈추게 하기 위해 감시할 장치를 선택합니다.
 - **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를

5. 사용자 설정

들어, 우선순위 2의 알람 동작 개시 이벤트는 오직 우선순위 1이나 2의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.

5.1.6.8 인증 거부 리스트 탭

인증 거부 리스트 탭에서 사용자 ID 나 카드 번호를 등록하여 사용자의 출입 시도 시 장치에서 인증되지 않도록 설정할 수 있습니다.



- 전체: 인증 거부 목록에 등록된 사용자 ID 나 카드의 총 수를 표시합니다.
- 추가가능: 등록할 수 있는 사용자 ID 나 카드의 수를 표시합니다.

참고: 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있습니다.

5.1.6.9 화면/음성 탭

화면/음성 탭에서 X-Station의 화면 설정과 소리 설정을 변경할 수 있습니다. 변경한 설정을 적용하려면 반드시 탭의 아래에 있는 **적용**을 클릭해야 합니다. **다른장치 적용**을 클릭하여 다른 장치에 같은 설정을 적용할 수 있습니다.



- 화면/음성 설정

5. 사용자 설정

- 언어: 화면에 사용할 언어를 설정합니다.
- 메뉴 타임아웃: 대기 화면으로 되돌아갈 시간을 설정합니다.
- 백라이트 타임아웃: 화면의 조명 시간을 설정합니다.
- 테마: 화면 테마를 설정합니다.
- 구성 파일: X-Station 에서 사용할 언어 파일(변경 안함, 영어 구성 파일, 한국어 구성 파일, 사용자 정의)을 설정합니다. 영어나 한국어 이외의 언어 파일을 사용하려면, 사용자 정의를 선택한 후 줄임표(...)를 클릭한 다음, 언어 파일을 지정합니다.
- 배경 화면: X-Station 에 사용할 배경화면의 종류(로고, 공지사항)를 설정합니다. 지원되는 파일 종류는 JPG, GIF, BMP, PNG 이며 240x320 픽셀을 초과해서는 안됩니다. 로고나 공지사항에 사용되는 그림은 오직 한번에 하나의 그림만 사용할 수 있습니다.
- 공지사항: X-Station 화면에 표시할 공지사항을 추가합니다. 공지사항을 추가했다면, 적용을 클릭하여 현재 선택된 장치에 적용하거나 또는 다른장치 적용을 클릭하여 다른 모든 장치에 적용할 수 있습니다.
- 음량: X-Station 의 음량(0% - 100%)을 설정합니다.
- 메시지 타임아웃: 인증 실패 메시지나 인증 성공 메시지가 표시될 시간을 설정합니다.
- 시계 표시: 현재 시간을 장치에 표시하도록 설정합니다.
- 배경화면 변경: 이 체크 상자를 선택하여 새로운 배경화면을 장치에 저장할 수 있습니다. 추가를 클릭한 후 새로운 그림 파일을 지정해서 추가합니다.
- 효과음 변경: 이 체크 상자를 선택하여 각 이벤트에 임의의 소리를 적용할 수 있습니다. 목록에 있는 이벤트를 클릭한 다음, 추가를 클릭한 후 새로운 소리 파일을 지정해서 추가합니다.

5.1.6.10 근태 탭

근태 탭에서 X-Station 장치의 근태 키 입력 방식을 설정할 수 있습니다. 설정을 저장하려면 장치 창의 하단에 있는 적용을 클릭해야 합니다. 다른장치 적용을 클릭하여 다른 장치에 현재 장치의 설정을 동일하게 적용할 수 있습니다.

보고서 근태키	내용	자동적용 시간	고장	문열림	이벤트 종류
F1	In	No Time	사용	사용 안함	사용 안함
F2	Out	No Time	사용 안함	사용 안함	사용 안함
F3	In Duty	No Time	사용 안함	사용 안함	사용 안함
F4	Out Duty	No Time	사용 안함	사용 안함	사용 안함

관리

X-Station 기능키: F1 (고장 이벤트)

화면 표시 문구: (빈칸) (문열림)

자동 모드 적용 시간: (빈칸)

이벤트 종류: 사용 안함

자극/조퇴 처리 안함 출퇴근만 적용

이 이벤트 이후부터 근무시간에 포함

추가, 수정, 삭제, 모두 삭제

5. 사용자 설정

- 근태 키 입력 방식: 장치에 적용할 근태 키 입력 방식을 선택합니다.
 - 사용 안함: 사용자가 장치에서 근태 이벤트를 기록할 수 없습니다.
 - 사용자 선택: 사용자가 근태 이벤트를 기록하려고 할 때마다 목적에 맞는 근태 기능키를 눌러야 합니다.
 - 선택 후 유지: 한 사용자가 특정 근태 기능키를 누를 경우 다른 근태 기능키를 누를 때까지 그 기능키가 유지됩니다.
 - 자동 설정: 설정된 출입시간 일정에 맞게 X-Station 장치가 자동으로 근태 기능을 표시합니다.
 - 이벤트 고정: X-Station 은 사용자가 설정한 근태 기능만 표시합니다.
- 관리: 근태 기능에 사용할 키를 선택하고 어떤 근태 이벤트를 할당할지 설정합니다.
 - X-Station 기능키: 아래 화살표를 클릭하여 목록에서 근태 기능에 사용할 키(F1~F4, EXT01~EXT12)를 선택합니다. **이벤트 고정** 방식을 선택하였다면, 오른쪽에 있는 **고정 이벤트체크** 상자를 선택합니다.
 - 화면 표시 문구: X-Station 화면에 표시할 근태 기능에 맞는 문구를 입력합니다.
 - 자동 모드 적용 시간: **자동 설정** 방식을 선택한 경우 아래 화살표를 클릭하여 목록에서 장치에 적용할 출입시간을 선택합니다. 선택한 시간에 맞추어 설정된 기능을 표시합니다. 출입시간을 추가하는 방법에 관해서는 3.7.1 을 참조하십시오.
 - 이벤트 종류: 선택한 키에 할당할 이벤트의 종류(**사용 안함**, **출근**, **퇴근**, **들어옴**, **나감**)을 선택합니다. **출근** 또는 **퇴근**을 선택한 경우 **지각/조퇴 처리 안함** 체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면 사용자의 실제 출퇴근시간에 관계없이 항상 정시에 출퇴근한 것으로 기록합니다. 근태 보고서의 결과에만 정시에 출퇴근한 것으로 기록하고 실제 근무 시간은 올바르게 계산하려면 **결과에만 적용체크** 상자를 선택합니다. **나감**을 선택한 경우에는 **이 이벤트 이후부터 근무시간에 포함체크** 상자를 선택할 수 있습니다. 이 옵션을 선택하면, 사용자가 근무상의 이유로 밖으로 나가는 것으로 간주하여 실제 근무 시간보다 빨리 나갔다고 하더라도 정상적으로 모든 시간을 근무한 것으로 기록합니다.

5.1.6.11 위캔드 탭

위캔드 탭에서 X-Station 에서 사용할 Wiegand 형식을 설정할 수 있습니다. X-Station 에서 위캔드 기능을 사용하려면 **Wiegand 입력**과 **Wiegand 출력**을 설정합니다. Wiegand 설정 마법사를 실행하려면 **포맷 변경**을 클릭합니다. 위캔드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.



5. 사용자 설정

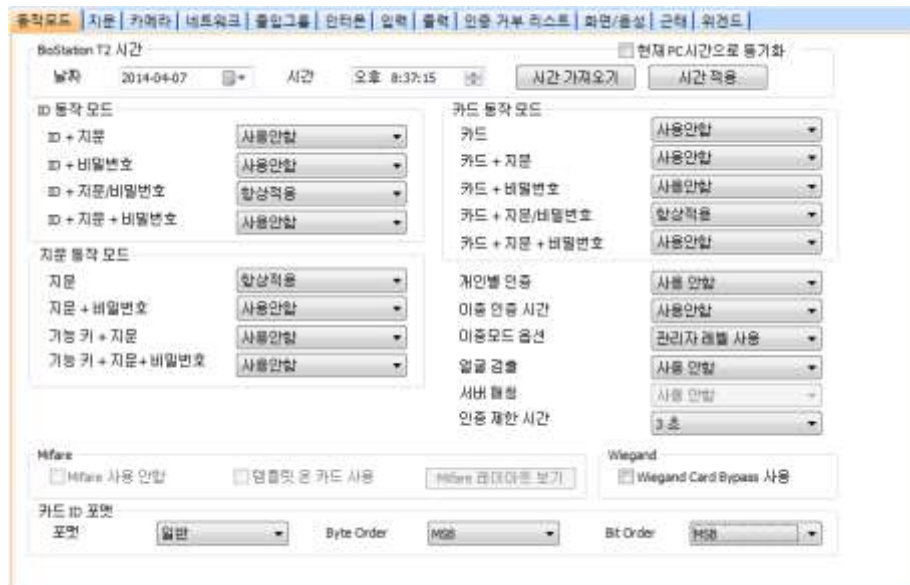
- **Wiegand 모드:** 카드 ID 데이터를 읽을 때 사용할 위겐드 모드(**일반모드**, **확장모드**)를 선택합니다. 일반모드를 선택하면 X-Station 에 연결된 RF 장치는 X-Station 의 일부로 인식됩니다. 확장모드를 선택하면 X-Station 에 연결된 RF 장치는 독립된 장치로 인식됩니다. 확장모드를 이용할 경우 RF 장치는 자신의 ID 로 로그를 남길 뿐 아니라 출입문을 구성할 수 있으며 구역에 포함될 수 있습니다.
- **Wiegand 입/출력:** 위겐드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 어떻게 처리할지 선택합니다.
 - **Wiegand (카드):** 위겐드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 카드 ID 로 처리합니다.
 - **Wiegand (사용자):** 위겐드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 사용자 ID 로 처리합니다.

5.1.7 BioStation T2 설정 변경하기

이 절에서는 BioStation T2 에서 사용할 수 있는 설정에 대해서 설명합니다. 이러한 설정을 변경하여 현재 처해있는 상황이나 운영상의 필요에 맞게 BioStation T2 의 기능을 변경할 수 있습니다.

5.1.7.1 동작모드 탭

동작모드 탭에서 BioStation T2 의 시간을 변경할 수 있으며 동작 모드와 관련한 다양한 설정을 변경할 수 있습니다.



- **BioStation T2 시간**
 - **날짜:** 장치에 표시할 날짜를 직접 설정합니다.
 - **시간:** 장치에 표시할 시간을 직접 설정합니다.
 - **현재 PC 시간으로 동기화:** BioStar 클라이언트 프로그램이 설치되어 있는 로컬 PC 의 날짜와 시간을 가져와 바로 아래 날짜와 시간 스피너 상자에 표시합니다. 시간 적용을 클릭하면, 장치의 날짜와 시간이 로컬 PC 의 날짜와 시간으로 설정됩니다.
 - **시간 가져오기:** 현재 장치에서 표시되고 있는 시간을 가져옵니다.
 - **시간 적용:** 장치의 시간을 설정한 시간으로 변경합니다.

5. 사용자 설정

- **ID 동작모드:** 이 영역에서는 일정에 따라 각각 다른 인증 모드가 적용되도록 설정할 수 있습니다. 예를 들어, 근무 시간에는 일반적인 인증 모드를 적용하고 근무 시간 이외에는 좀더 엄격한 인증모드를 적용할 수 있습니다. 장치에 설정된 인증 모드를 적용할지 아니면 개별 사용자에게 설정된 인증 모드를 적용할지도 여기에서 설정할 수 있습니다(5.4.1 참조). 사용자의 인증 모드를 개별적으로 설정하지 않았다면, 장치에 설정된 인증 모드가 적용됩니다.
 - **ID + 지문:** 인증을 위해 장치가 ID와 지문을 요구하도록 설정합니다.
 - **ID + 비밀번호:** 인증을 위해 장치가 ID와 비밀번호를 요구하도록 설정합니다.
 - **ID + 지문/비밀번호:** 인증을 위해 장치가 ID와 지문 또는 ID와 비밀번호를 요구하도록 설정합니다.
 - **ID + 지문 + 비밀번호:** 인증을 위해 장치가 ID와 지문과 비밀번호를 요구하도록 설정합니다. (항상적용, 사용안함, 사용자가 설정한 출입시간)
- **카드 동작 모드:**
 - **카드:** 인증을 위해 장치가 카드만 요구하도록 설정합니다.
 - **카드 + 지문:** 인증을 위해 장치가 카드와 지문을 요구하도록 설정합니다.
 - **카드 + 비밀번호:** 인증을 위해 장치가 카드와 비밀번호를 요구하도록 설정합니다.
 - **카드 + 지문/비밀번호:** 인증을 위해 장치가 카드와 지문 또는 카드와 비밀번호를 요구하도록 설정합니다.
 - **카드 + 지문 + 비밀번호:** 인증을 위해 장치가 카드와 지문과 비밀번호를 요구하도록 설정합니다. (항상적용, 사용안함, 사용자가 설정한 출입시간)
- **지문 동작 모드:**
 - **지문:** 인증을 위해 장치가 지문만 요구하도록 설정합니다.
 - **지문 + 비밀번호:** 인증을 위해 장치가 지문과 비밀번호를 요구하도록 설정합니다.
 - **기능 키 + 지문:** 인증을 위해 장치가 기능 키와 지문을 요구하도록 설정합니다.
 - **기능 키 + 지문 + 비밀번호:** 인증을 위해 장치가 기능 키와 지문과 비밀번호를 요구하도록 설정합니다. (항상적용, 사용안함, 사용자가 설정한 출입시간)
- **기타 옵션**
 - **개인별 인증:** 개인에게 설정된 인증 방식을 사용하여 인증하도록 설정합니다. (사용, 사용 안함)
 - **이중 인증 시간:** 인증을 위해 장치가 두 사람의 ID나 지문이나 카드를 요구하도록 설정합니다(항상 적용, 사용 안함). 15초 이내에 두 번째 사용자의 지문을 인증하지 않으면 인증이 무효가 됩니다.
 - **얼굴 검출:** 인증이 성공하였을 때 얼굴 이미지를 강제로 검출하여 출입하는 사용자의 얼굴 이미지를 확보합니다.
 - **서버 매칭:** 지문이 일치하는지를 장치에서 판별하지 않고 BioStar 서버에서 판별하도록 설정합니다. 이 옵션을 선택하면, 장치는 지문의 일치 여부를 판별하기 위해 사용자 ID나 지문 템플릿이나 카드 ID 정보를 서버에 보냅니다. 사용자의 수가 너무 많아 개별 장치에 모든 정보를 저장할 수 없거나 또는 보안상의 이유로 개별 장치에 정보를 보관할 수 없을 때 이 옵션을 사용하면 편리합니다.
 - **인증 제한 시간:** 지문의 일치 여부를 판별할 때 장치가 작업을 그만두는 시간(3초, 7초, 10초, 15초, 20초, 30초)을 설정합니다.
- **Mifare 설정**
 - **Mifare 사용 안함:** MiFARE 카드를 이용한 인증을 금지합니다.
 - **템플릿 온 카드 사용:** 인증할 때에 MiFARE 카드에 저장된 지문 정보를 사용합니다.

5. 사용자 설정

- **Mifare 레이아웃 보기:** 장치에서 사용하고 있는 MIFARE 레이아웃을 확인합니다. MIFARE 레이아웃의 편집 방법은 3.6.4.7 을 참조하십시오.
- **카드 ID 포맷**
 - **포맷:** 카드 ID 데이터를 어떤 방식으로 읽어 들일 것인가를 설정합니다. **일반**을 선택하면 카드 ID 데이터를 일반적인 형식으로 처리합니다. **Wiegand** 를 선택하면 위갠드 형식 설정에 따라 카드 ID 데이터를 처리합니다.
 - **Byte Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. **MSB** 를 선택하면 큰 단위의 바이트에서 작은 단위의 바이트 순으로 처리합니다. **LSB** 를 선택하면 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.
 - **Bit Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 비트를 처리할지 선택합니다. **MSB** 를 선택하면 최상위 비트에서 최하위 비트 순으로 처리합니다. **LSB** 를 선택하면 최하위 비트에서 최상위 비트 순으로 처리합니다.
 - 이중 인증 모드에서 Admin User 를 반드시 포함하는 설정 옵션을 지원합니다. 이중 인증 모드 운영 시에는 Normal User 인증 후 15초 이내에 반드시 Admin User 가 인증해야 Door Relay 가 켜집니다. 이 옵션을 사용하지 않는 경우 기존과 동일하게 Normal User 나 Admin User 여부와 관계 없이 다른 두 사용자가 15초 이내에 인증하면 Door Relay 가 켜지게 됩니다.
주의: 이 기능은 펌웨어 버전 BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.
 - Wiegand Card Bypass 사용: BioStar 의 Wiegand 설정에 따라 인증 성공 여부와 상관 없이 CSN 을 내보내는 기능으로, BioStar 제품군 장치를 타사 ACU 와 Wiegand 로 연동하여 인증 여부를 판단하고 출입문 제어 기능이 없는 Dummy 장치로 사용하고자 할 때 필요한 기능입니다. 카드가 입력되면 장치에서는 별도의 인증 처리 없이 바로 Wiegand 로 카드 ID 를 출력하게 됩니다.
주의: 이 기능은 펌웨어 버전 BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원 됩니다.

5.1.7.2 지문 탭

지문 탭에서 BioStation T2 의 지문 인증 설정을 변경할 수 있습니다.



5. 사용자 설정

- **지문**
 - **보안 등급:** 지문을 인증할 때 사용할 보안 등급을 설정합니다(**보통, 안전, 가장 안전**). 보안 등급을 높일수록 본인 거부율(본인의 지문이 확실한데도 장치가 인식하지 못하는 확률)도 같이 증가합니다.
 - **영상 품질 기준:** 지문의 품질 등급(**낮음, 보통, 높음**)을 설정합니다. 지문의 품질이 설정한 품질 등급보다 낮으면 시스템이 거부합니다.
 - **지문 입력 시간:** 지문 입력을 끝마쳐야 하는 시간(**1 초-20 초**)을 설정합니다. 정해진 시간 안에 지문을 입력하지 않으면 인증이 실패하게 됩니다.
 - **1:N 인식 속도:** 지문의 일치 여부를 판별하는 데 걸리는 시간을 줄이려면 인식 속도(**자동, 보통, 빠름, 가장 빠름**)를 조절합니다. **자동**을 선택하면 장치에 등록된 총 지문 템플릿의 수에 따라 자동으로 판별 속도가 결정됩니다.
 - **등록 지문 영상:** BioStation T2 의 화면에 지문을 보일 것인지 말 것인지(**보임, 보이지 않음**)를 선택합니다.
 - **위조 지문 검사:** 위조 지문 공격을 방지하기 위하여 위조 지문을 검사할지(**사용, 검사하지 않음**) 설정합니다.
- **지문 옵션 정보:** 전체 지문 템플릿 설정을 표시합니다. 지문 템플릿에 관한 자세한 내용은 4.9 를 참조하십시오.

5.1.7.3 카메라 탭

카메라 탭에서 BioStation T2 의 카메라 설정을 변경할 수 있습니다. 출입 시간대별 발생하는 이벤트에 따라 카메라의 작동을 설정할 수 있습니다. **추가**를 클릭하여 카메라를 작동할 이벤트를 추가한 후 **적용**을 클릭하여 변경 사항을 저장합니다.



주의: 보안을 위해 카메라 이벤트에 인증 이벤트를 추가할 것을 권장합니다. 장치와 서버간의 네트워크 부하를 줄이기 위해 최대 30 개의 이벤트만 추가하십시오.

5.1.7.4 네트워크 탭

네트워크 탭에서 BioStation T2 의 네트워크 설정과 서버 설정을 변경할 수 있습니다.

5. 사용자 설정



- **TCP/IP 설정**
 - **네트워크 종류:** 랜의 종류(사용 안함, 이더넷, 무선 LAN 사용)를 선택합니다.
 - **포트:** 장치가 사용할 포트를 지정합니다.
 - **무선 랜:** 미리 설정된 무선 랜 구성을 선택합니다. 네트워크 종류에서 **무선 랜**을 선택해야 이 옵션을 설정할 수 있습니다
 - **설정 변경:** 무선 랜을 설정하려면 클릭합니다. 무선 랜을 설정하는 방법에 관한 자세한 내용은 3.2.4 를 참조하십시오.
 - **DHCP 사용:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용합니다.
 - **DHCP 사용 안함:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용하지 않습니다.
 - **IP 주소:** 장치의 IP 주소를 입력합니다.
 - **서브넷:** 장치의 서브넷 주소를 입력합니다.
 - **게이트웨이:** 네트워크의 게이트웨이를 입력합니다.
 - **연결 허용:** 허용할 최대 연결 수를 지정합니다.
- **서버**
 - **사용:** 서버 모드(장치를 BioStar 서버에 연결)를 사용합니다.
 - **사용 안함:** 서버 모드를 사용하지 않습니다.
 - **IP 주소:** BioStar 서버의 IP 주소를 입력합니다.
 - **서버 포트:** BioStar 가 사용하는 포트를 입력합니다.
 - **서버와 자동으로 시간 동기화:** 장치의 시간을 서버의 시간과 동기화합니다. 장치에서 1 시간마다 서버 시간을 폴링하여, 서버의 시간과 5 초 이상 차이가 나면, 서버의 시간과 동기화합니다.
- **시리얼 설정**
 - **RS485 네트워크 모드:** RS485 로 연결된 장치의 모드(사용 안함, 호스트, 슬레이브, PC 연결 모드)를 설정합니다. RS485 모드에 관한 자세한 내용은 3.2.1 과 3.2.2 를 참조하십시오.
 - **RS485 속도:** RS485 로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.
 - **RS232 속도:** RS232 로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.
- **USB 설정:** BioStation T2 에 장착된 USB 포트를 활성화하려면 버튼을 클릭합니다.

5. 사용자 설정

- **USB:** 버튼을 클릭하여 USB 연결을 허용할지 금지할지 선택합니다.
- **USB 메모리:** 버튼을 클릭하여 USB 메모리 사용을 허용할지 금지할지 선택합니다.

5.1.7.5 출입그룹 탭

출입그룹 탭에서 BioStation T2의 인증 제한 설정과 기본 출입그룹을 변경할 수 있습니다.

The screenshot shows the 'Entrance Limit Setting' configuration page. It includes a navigation bar with tabs for '동작모드', '지문', '카메라', '네트워크', '출입그룹', '인터폰', '입력', '출력', '인증 거부 리스트', '화면/음성', '근태', and 'Wiegand'. The main content area is titled 'Entrance Limit Setting' and contains the following fields:

- 인증 간격(분):** A text input field with the value '0' and a unit dropdown set to '분'.
- 제한 옵션1-4:** Four rows, each with a checkbox, a text input field (all containing '0000'), a range separator '~', another text input field (all containing '0000'), and a label '최대 인증 허용 횟수' followed by a text input field (all containing '0').
- 기본 출입 그룹 설정:** A section with a label '기본 출입 그룹' and a dropdown menu currently set to 'Full Access'.

- **인증 제한 설정**
 - **인증 간격(분):** 다시 출입할 수 있는 권한을 얻는 데까지 필요한 시간(분 단위)을 설정합니다. 사용자가 어느 구역에 입장하였으면, 지정된 시간 안에는 그 구역 안으로 다시 입장할 수 없습니다.
 - **제한 옵션 1~4:** 인증 제한 설정을 적용하려면 체크 상자를 선택한 후 이 설정을 적용할 시간을 입력합니다.
 - **최대 인증 허용 횟수:** 지정된 인증 제한 시간 안에 허용할 최대 입장 수를 설정합니다.
- **기본 출입 그룹 설정:** 다른 출입그룹에 포함되지 않은 새로운 사용자에게 적용할 기본 출입그룹을 선택합니다.

5.1.7.6 인터폰 탭

BioStation T2의 인터폰 기능을 사용하여 출입문 안쪽에 있는 상대방과 전화 통화할 수 있습니다.

The screenshot shows the 'Interphone' configuration page. It includes the same navigation bar as the previous page. The main content area is titled 'Interphone' and contains the following fields:

- 종류:** A dropdown menu with '생성중이외' selected.
- VOIP 서버 IP:** A text input field with the value '255.255.255.255'.
- VOIP 표시명:** A text input field.
- VOIP ID:** A text input field.
- 스피커 개인:** A dropdown menu with '3D' selected.
- VOIP 전화번호:** A text input field.
- VOIP 비밀번호:** A text input field.
- 마이크 개인:** A dropdown menu with '6' selected.

아날로그 인터폰, IP 인터폰, BioStar VideoPhone 등 3 가지 종류가 지원됩니다. BioStar VideoPhone은 음성 및 영상 통화가 지원되는 인터폰으로서, BioStation T2 V1.1 이상의 펌웨어에서만 지원됩니다. 별도로 제공되는 프로그램을 PC에 설치해야 합니다. 프로그램 설치 및 사용 방법은 BioStar VideoPhone 사용자 매뉴얼을 참조하십시오.

사용하고자 하는 인터폰 종류에 따라 다음 옵션을 설정할 수 있습니다.

- **인터폰**

5. 사용자 설정

- **VOIP 서버 IP:** VoIP 서버의 IP 주소를 입력합니다.
- **VOIP 표시명:** VoIP의 사용자 지정 이름을 입력합니다.
- **VOIP 전화번호:** VoIP 전화번호를 입력합니다.
- **VOIP ID:** VoIP 서버의 ID를 입력합니다.
- **VOIP 비밀번호:** VoIP 서버의 비밀번호를 입력합니다.
- **스피커 게인:** 스피커의 음량을 조절합니다(1~10).
- **마이크 게인:** 마이크의 음량을 조절합니다(1~10).
- **비디오폰**
 - **모드:** 단일 또는 내선 2 가지 모드가 지원됩니다. 단일 모드는 장치에서 1 대의 PC와 연결 가능하며, 내선 모드는 최대 8대의 PC와 연결할 수 있습니다.
 - **장치 비밀번호:** 장치에서 설정한 비밀번호를 입력합니다. 이 비밀번호는 BioStar VideoPhone 프로그램에서 장치에 로그인하기 위해 필요합니다.
 - **출입문 제어:** PC에서 원격으로 출입문을 열 수 있도록 허용합니다.

5.1.7.7 입력 탭

입력 탭에는 BioStation T2에 지정된 입력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 입력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Input 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 입력 설정의 구성 방법은 3.10.3.2를 참조하십시오.



- **장치:** 설정을 추가하거나 수정할 BioStation T2(또는 Secure I/O)을 선택합니다.
- **포트:** Secure I/O와 동일하게 **입력 0**, **입력 1**, **입력 2**, **입력 3**을 선택할 수 있습니다.
- **스위치:** 버튼을 클릭하여 입력 스위치의 보통 상태(**N/O**: 평상시 열림, **N/C**: 평상시 닫힘)를 설정합니다.
- **기능:** 입력을 받았을 때 취할 동작을 선택합니다:
 - **사용 안함:** 입력 포트를 감시하지 않습니다.
 - **일반 입력:** 지정된 동작을 실행하기 위해 입력 포트를 감시합니다. (Output 설정 대화 상자에서 지정한 이벤트를 확인하려면 5.1.7.8을 참조하십시오.)
 - **비상 문 열림:** 이 장치가 제어하고 있는 출입문을 엽니다. 일반적인 출입문 열림 시간은 무시되며, 관리자가 출입문/구역 감시 탭을 통해서 "문 닫기" 명령을 실행하기 전까지는 출입문이 열린 채로 남아 있습니다(4.4.1 참조).
 - **모든 경보 해제:** 이 장치와 연결된 모든 경보를 해제합니다.
 - **장치 재 시작:** 장치를 재시동합니다.
 - **장치 잠금:** 장치가 잠깁니다. 잠긴 장치는 BioStar 서버와 통신할 수 없으며 또한 지문이나 카드 입력을 처리할 수 없습니다. 통신을 다시 연결하려면, 관리자가 BioStation T2에서 직접 인증해야 합니다.

5. 사용자 설정

- **동작시간:** 입력 신호를 감시할 일정(**사용안함, 항상적용**)을 설정합니다.
- **입력시간(ms):** 지정한 동작을 발생시키기 위해 필요한 입력 신호의 지속 시간(1000분의 1 초)을 입력합니다.

5.1.7.8 출력 탭

출력 탭에는 BioStation T2 에 적용되는 출력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 출력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Output 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 출력 설정의 구성 방법은 3.10.3.1 을 참조하십시오.



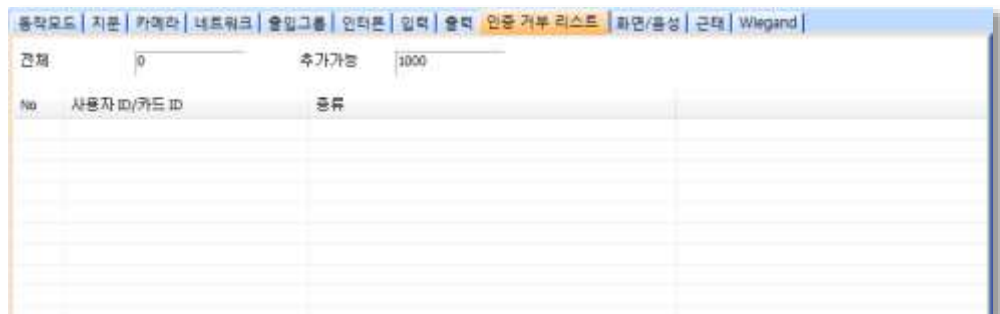
- **장치:** 설정을 추가하거나 수정할 장치의 종류를 선택합니다.
- **포트:** Secure I/O 와 동일하게 **릴레이 0, 릴레이 1** 을 선택할 수 있습니다.
- **알람 동작 개시 이벤트:** 옵션을 설정하고 **추가** 를 클릭하여 알람 동작 개시 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람을 발생시킵니다.
 - **이벤트:** 알람을 발생시킬 이벤트(**인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지**)를 선택합니다.
 - **장치:** 알람을 발생시키기 위해 감시할 장치를 선택합니다.
 - **신호파형:** 메뉴 표시줄의 **옵션 > 이벤트 > Output 포트 설정** 을 통해서 이미 설정한 신호파형 중에서 하나를 선택합니다.
 - **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선순위 2 의 알람 동작 개시 이벤트는 오직 우선순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.
- **알람 멈춤 이벤트:** 옵션을 설정하고 **추가** 를 클릭하여 알람 멈춤 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람이 중단됩니다.

5. 사용자 설정

- 이벤트: 알람을 멈추게 할 이벤트(인증 성공, 인증 실패, 협박모드 검출, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
- 장치: 알람을 멈추게 하기 위해 감시할 장치를 선택합니다.
- 우선순위: 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선순위 2 의 알람 동작 개시 이벤트는 오직 우선순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.

5.1.7.9 인증 거부 리스트 탭

인증 거부 리스트 탭에서 사용자 ID 나 카드 번호를 등록하여 사용자의 출입 시도 시 장치에서 인증되지 않도록 설정할 수 있습니다.



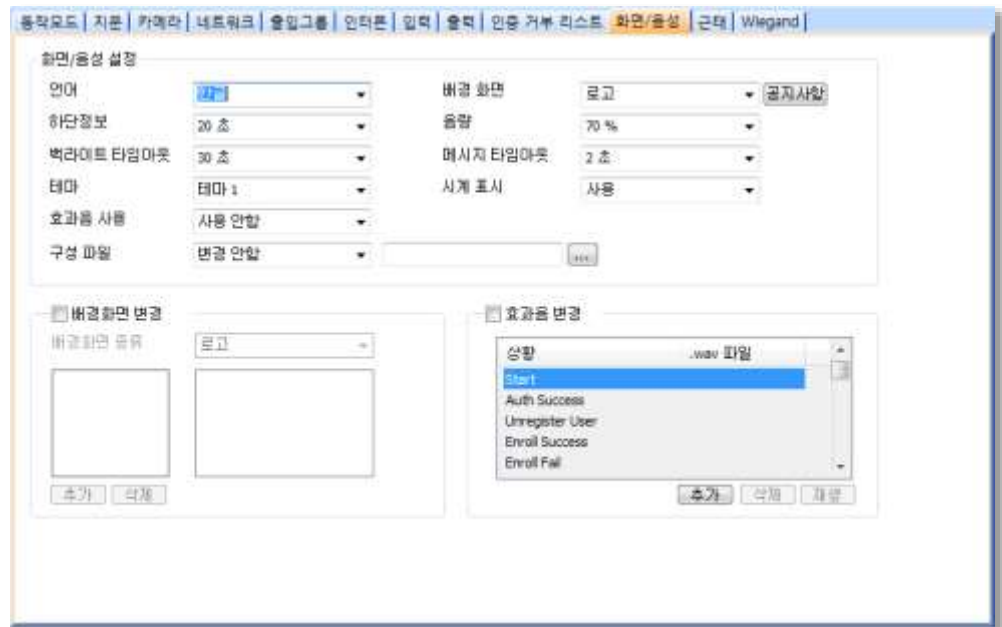
- 전체: 인증 거부 목록에 등록된 사용자 ID 나 카드의 총 수를 표시합니다.
- 추가가능: 등록할 수 있는 사용자 ID 나 카드의 수를 표시합니다.

참고: 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있습니다.

5.1.7.10 화면/음성 탭

화면/음성 탭에서 BioStation T2 의 화면 설정과 소리 설정을 변경할 수 있습니다. 변경한 설정을 적용하려면 반드시 탭의 아래에 있는 **적용**을 클릭해야 합니다. **다른장치 적용**을 클릭하여 다른 장치에 같은 설정을 적용할 수 있습니다.

5. 사용자 설정



- **화면/음성 설정**
 - 언어: 화면에 표시할 언어(한글, 영문, 사용자 정의)를 선택합니다.
 - 하단정보: 부가적인 정보가 BioStation T2 의 화면 하단에 표시될 시간(무제한, 10 초, 20 초, 30 초)을 설정합니다.
 - 백라이트 타임아웃: 화면의 조명 시간을 설정합니다.
 - 테마: 화면 테마를 설정합니다.
 - 효과음 사용: 효과음 사용 여부를 설정합니다.
 - 구성 파일: BioStation T2 에서 사용할 언어 파일(변경 안함, 영어 구성 파일, 한국어 구성 파일, 사용자 정의)을 설정합니다. 영어나 한국어 이외의 언어 파일을 사용하려면, 사용자 정의를 선택한 후 출임표(...)를 클릭한 다음, 언어 파일을 지정합니다.
 - 배경 화면: BioStation T2 에서 사용할 배경화면의 종류(로고, 공지사항, 슬라이드쇼, PDF)를 설정합니다. 지원되는 파일 종류는 JPG, GIF, BMP, PNG, PDF 이며 480×800 픽셀을 초과해서는 안됩니다. 로고나 공지사항에 사용되는 그림은 오직 한번에 하나의 그림만 사용할 수 있습니다.
 - 공지사항: BioStation T2 화면에 표시할 공지사항을 추가합니다. 공지사항을 추가했다면, 적용을 클릭하여 현재 선택된 장치에 적용하거나 또는 다른장치 적용을 클릭하여 다른 모든 장치에 적용할 수 있습니다.
 - 음량: BioStation T2 의 음량(0% - 100%)을 설정합니다.
 - 메시지 타임아웃: 인증 실패 메시지나 인증 성공 메시지가 표시될 시간을 설정합니다.
 - 시계 표시: 시계 표시 여부를 설정합니다.
- **배경화면 변경:** 이 체크 상자를 선택하여 새로운 배경화면을 장치에 저장할 수 있습니다. 추가를 클릭한 후 새로운 그림 파일을 지정해서 추가합니다.
- **효과음 변경:** 이 체크 상자를 선택하여 각 이벤트에 임의의 소리를 적용할 수 있습니다. 목록에 있는 이벤트를 클릭한 다음, 추가를 클릭한 후 새로운 소리 파일을 지정해서 추가합니다.

5. 사용자 설정

5.1.7.11 근태 탭

근태 탭에서 BioStation T2 장치의 근태 키 입력 방식을 설정할 수 있습니다. 설정을 저장하려면 장치 창의 하단에 있는 **적용**을 클릭해야 합니다. **다른장치 적용**을 클릭하여 다른 장치에 현재 장치의 설정을 동일하게 적용할 수 있습니다.

보고서 근태키	내용	자동적용 시간	고정	운영됨	이벤트 종류
F1	In	No Time	사용	사용	들어옴
F2	Out	No Time	사용 안함	사용 안함	나감
F3	In Duty	No Time	사용 안함	사용	나감
F4	Out Duty	No Time	사용 안함	사용 안함	나감

관리

BioStation T2 기능키: F1 고정 이벤트

화면 표시 문구:

자동 모드 적용 시간:

이벤트 종류: 사용 안함 운영됨

지각/조퇴 처리 안함 결과에만 적용

이 이벤트 이후부터 근무시간에 포함

추가, 수정, 삭제, 모두 삭제

- **근태 키 입력 방식:** 장치에 적용할 근태 키 입력 방식을 선택합니다.
 - **사용 안함:** 사용자가 장치에서 근태 이벤트를 기록할 수 없습니다.
 - **사용자 선택:** 사용자가 근태 이벤트를 기록하려고 할 때마다 목적에 맞는 근태 기능키를 눌러야 합니다.
 - **선택 후 유지:** 한 사용자가 특정 근태 기능키를 누를 경우 다른 근태 기능키를 누를 때까지 그 기능키가 유지됩니다.
 - **자동 설정:** 설정된 출입시간 일정에 맞게 BioStation T2 장치가 자동으로 근태 기능을 표시합니다.
 - **이벤트 고정:** BioStation T2 은 사용자가 설정한 근태 기능만 표시합니다.
- **관리:** 근태 기능에 사용할 키를 선택하고 어떤 근태 이벤트를 할당할지 설정합니다.
 - **BioStation T2 기능키:** 아래 화살표를 클릭하여 목록에서 근태 기능에 사용할 키(F1~F4, EXT01~EXT12)를 선택합니다. **이벤트 고정** 방식을 선택하였다면, 오른쪽에 있는 **고정 이벤트** 체크 상자를 선택합니다.
 - **화면 표시 문구:** BioStation T2 화면에 표시할 근태 기능에 맞는 문구를 입력합니다.
 - **자동 모드 적용 시간:** **자동 설정** 방식을 선택한 경우 아래 화살표를 클릭하여 목록에서 장치에 적용할 출입시간을 선택합니다. 선택한 시간에 맞추어 설정된 기능을 표시합니다. 출입시간을 추가하는 방법에 관해서는 3.7.1 을 참조하십시오.
 - **이벤트 종류:** 선택한 키에 할당할 이벤트의 종류(**사용 안함**, **출근**, **퇴근**, **들어옴**, **나감**)를 선택합니다. **출근** 또는 **퇴근**을 선택한 경우 **지각/조퇴 처리 안함** 체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면 사용자의 실제 출퇴근 시간에 관계없이 항상 정시에 출퇴근한 것으로 기록합니다. 근태 보고서의 결과에만 정시에 출퇴근한 것으로 기록하고 실제 근무 시간은 올바르게 계산하려면 **결과에만 적용** 체크 상자를 선택합니다. **나감**을 선택한 경우에는 **이 이벤트 이후부터 근무시간에 포함** 체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면, 사용자가 근무상의

5. 사용자 설정

이유로 밖으로 나가는 것으로 간주하여 실제 근무 시간보다 빨리 나갔다고 하더라도 정상적으로 모든 시간을 근무한 것으로 기록합니다.

5.1.7.12 위갠드 탭

위갠드 탭에서 BioStation T2 에서 사용할 Wiegand 형식을 설정할 수 있습니다. BioStation T2 에서 위갠드 기능을 사용하려면 **Wiegand 입력**과 **Wiegand 출력**을 설정합니다. Wiegand 설정 마법사를 실행하려면 **포맷 변경**을 클릭합니다. 위갠드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.



- **Wiegand 모드:** 카드 ID 데이터를 읽을 때 사용할 위갠드 모드(**일반모드**, **확장모드**)를 선택합니다. 일반모드를 선택하면 호스트 장치에 연결된 RF 장치는 호스트 장치의 일부로 인식됩니다. 확장모드를 선택하면 연결된 RF 장치가 독립된 장치로 인식됩니다. 확장모드를 이용할 경우 RF 장치는 자신의 ID 로 로그를 남길 뿐 아니라 출입문을 구성할 수 있으며 구역에 포함될 수 있습니다.
- **Wiegand 입/출력:** 위갠드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 어떻게 처리할지 선택합니다.
 - **Wiegand (카드):** 위갠드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 카드 ID 로 처리합니다.
 - **Wiegand (사용자):** 위갠드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 사용자 ID 로 처리합니다.

5.1.8 FaceStation 설정 변경하기

이 절에서는 FaceStation 에서 사용할 수 있는 설정에 대해서 설명합니다. 이러한 설정을 변경하여 현재 처해있는 상황이나 운영상의 필요에 맞게 FaceStation 의 기능을 변경할 수 있습니다.

5.1.8.1 동작모드 탭

동작모드 탭에서 FaceStation 의 시간을 변경할 수 있으며 동작 모드와 관련한 다양한 설정을 변경할 수 있습니다.

- **FaceStation 시간**

5. 사용자 설정

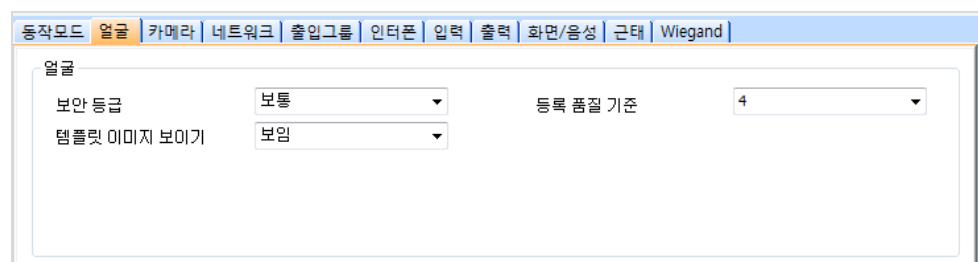
- 날짜: 장치에 표시할 날짜를 직접 설정합니다.
- 시간: 장치에 표시할 시간을 직접 설정합니다.
- 현재 PC 시간으로 동기화: BioStar 클라이언트 프로그램이 설치되어 있는 로컬 PC의 날짜와 시간을 가져와 바로 아래 날짜와 시간 스피ن 상자에 표시합니다. 시간 적용을 클릭하면, 장치의 날짜와 시간이 로컬 PC의 날짜와 시간으로 설정됩니다.
- 시간 가져오기: 현재 장치에서 표시되고 있는 시간을 가져옵니다.
- 시간 적용: 장치의 시간을 설정한 시간으로 변경합니다.
- ID 동작 모드: 이 영역에서는 일정에 따라 각각 다른 인증 모드가 적용되도록 설정할 수 있습니다. 예를 들어, 근무 시간에는 일반적인 인증 모드를 적용하고 근무 시간 이외에는 좀더 엄격한 인증모드를 적용할 수 있습니다. 장치에 설정된 인증 모드를 적용할지 아니면 개별 사용자에게 설정된 인증 모드를 적용할지도 여기에서 설정할 수 있습니다(5.4.1 참조). 사용자의 인증 모드를 개별적으로 설정하지 않았다면, 장치에 설정된 인증 모드가 적용됩니다.
 - ID + 얼굴: 인증을 위해 장치가 ID와 얼굴 인식을 요구하도록 설정합니다.
 - ID + 비밀번호: 인증을 위해 장치가 ID와 비밀번호를 요구하도록 설정합니다.
 - ID + 얼굴/비밀번호: 인증을 위해 장치가 ID와 얼굴 인식 또는 ID와 비밀번호를 요구하도록 설정합니다.
 - ID + 얼굴 + 비밀번호: 인증을 위해 장치가 ID와 얼굴 인식과 비밀번호를 요구하도록 설정합니다. (항상적용, 사용안함, 사용자가 설정한 출입시간)
- 카드 동작 모드:
 - 카드: 인증을 위해 장치가 카드만 요구하도록 설정합니다.
 - 카드 + 얼굴: 인증을 위해 장치가 카드와 얼굴 인식을 요구하도록 설정합니다.
 - 카드 + 비밀번호: 인증을 위해 장치가 카드와 비밀번호를 요구하도록 설정합니다.
 - 카드 + 얼굴/비밀번호: 인증을 위해 장치가 카드와 얼굴 인식 또는 카드와 비밀번호를 요구하도록 설정합니다.
 - 카드 + 얼굴 + 비밀번호: 인증을 위해 장치가 카드와 얼굴 인식과 비밀번호를 요구하도록 설정합니다. (항상적용, 사용안함, 사용자가 설정한 출입시간)
- 얼굴 동작 모드:
 - 얼굴: 인증을 위해 장치가 얼굴 인식만 요구하도록 설정합니다.
 - 얼굴 + 비밀번호: 인증을 위해 장치가 얼굴 인식과 비밀번호를 요구하도록 설정합니다.
 - 기능 키 + 얼굴: 인증을 위해 장치가 기능 키와 얼굴 인식을 요구하도록 설정합니다.
 - 기능 키 + 얼굴 + 비밀번호: 인증을 위해 장치가 기능 키와 얼굴 인식과 비밀번호를 요구하도록 설정합니다(항상적용, 사용안함, 사용자가 설정한 출입시간).
- 기타 옵션
 - 개인별 인증: 개인에게 설정된 인증 방식을 사용하여 인증하도록 설정합니다 (사용, 사용 안함).
 - 이중 인증 시간: 인증을 위해 장치가 두 사람의 ID나 얼굴 또는 카드를 요구하도록 설정합니다(항상 적용, 사용 안함). 15초 이내에 두 번째 사용자의 인증 정보를 않으면 인증이 무효가 됩니다.
 - 얼굴 검출: 인증이 성공하였을 때 얼굴 이미지를 강제로 검출하여 출입하는 사용자의 얼굴 이미지를 확보합니다.
 - 인증 제한 시간: 인증 정보의 일치 여부를 판별할 때 장치가 작업을 그만두는 시간(3초, 7초, 10초, 15초, 20초, 30초)을 설정합니다.
- Mifare 설정

5. 사용자 설정

- Mifare 사용 안함: MiFARE 카드를 이용한 인증을 금지합니다.
- 템플릿 온 카드 사용: FaceStation 에서는 지원되지 않습니다.
- Mifare 레이아웃 보기: FaceStation 에서는 지원되지 않습니다.
- **카드 ID 포맷**
 - **포맷:** 카드 ID 데이터를 어떤 방식으로 읽어 들일 것인가를 설정합니다. **일반**을 선택하면 카드 ID 데이터를 일반적인 형식으로 처리합니다. **Wiegand** 를 선택하면 위갠드 형식 설정에 따라 카드 ID 데이터를 처리합니다.
 - **Byte Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. **MSB** 를 선택하면 큰 단위의 바이트에서 작은 단위의 바이트 순으로 처리합니다. **LSB** 를 선택하면 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.
 - **Bit Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 비트를 처리할지 선택합니다. **MSB** 를 선택하면 최상위 비트에서 최하위 비트 순으로 처리합니다. **LSB** 를 선택하면 최하위 비트에서 최상위 비트 순으로 처리합니다.
 - 이중 인증 모드에서 Admin User 를 반드시 포함하는 설정 옵션을 지원합니다. 이중 인증 모드 운영 시에는 Normal User 인증 후 15 초 이내에 반드시 Admin User 가 인증해야 Door Relay 가 켜집니다. 이 옵션을 사용하지 않는 경우 기존과 동일하게 Normal User 나 Admin User 여부와 관계 없이 다른 두 사용자가 15 초 이내에 인증하면 Door Relay 가 켜지게 됩니다.
주의: 이 기능은 펌웨어 버전 BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.
 - Wiegand Card Bypass 사용: BioStar 의 Wiegand 설정에 따라 인증 성공 여부와 상관 없이 CSN 을 내보내는 기능으로, BioStar 제품군 장치를 타사 ACU 와 Wiegand 로 연동하여 인증 여부를 판단하고 출입문 제어 기능이 없는 Dummy 장치로 사용하고자 할 때 필요한 기능입니다. 카드가 입력되면 장치에서는 별도의 인증 처리 없이 바로 Wiegand 로 카드 ID 를 출력하게 됩니다.
주의: 이 기능은 펌웨어 버전 BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.

5.1.8.2 얼굴 탭

얼굴 탭에서 FaceStation 의 얼굴 인식 설정을 변경할 수 있습니다.

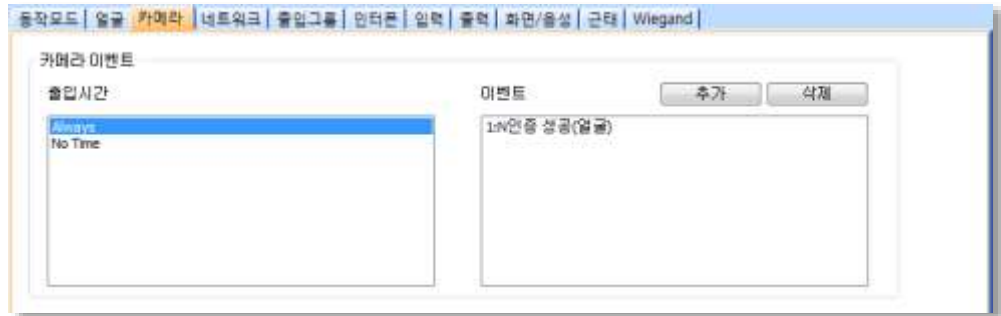


- **얼굴**
 - **보안 등급:** 얼굴 인식으로 인증할 때 사용할 보안 등급을 설정합니다(보통, 안전, 가장 안전). 보안 등급을 높일수록 본인 거부율(본인의 얼굴이 확실한데도 장치가 인식하지 못하는 확률)도 같이 증가합니다.
 - **등록 품질 기준:** 얼굴 인식 시스템의 민감도(이[최소]~9[최대])를 설정합니다. 높게 설정할수록 얼굴은 잘 인식되지만, 외부 영상 노이즈 또한 증가합니다.
 - **템플릿 이미지 보이기:** FaceStation 장치에서 사용자 템플릿 이미지를 표시하거나 표시하지 않도록 설정합니다.

5. 사용자 설정

5.1.8.3 카메라 탭

카메라 탭에서 FaceStation 의 카메라 설정을 변경할 수 있습니다. 출입시간대별로 발생하는 이벤트에 따라 카메라의 작동을 설정할 수 있습니다. **추가**를 클릭하여 카메라를 작동할 이벤트를 추가한 후 **적용**을 클릭하여 변경 사항을 저장합니다.



주의: 보안을 위해 카메라 이벤트에 인증 이벤트를 추가할 것을 권장합니다. 장치와 서버간의 네트워크 부하를 줄이기 위해 최대 30 개의 이벤트만 추가하십시오.

5.1.8.4 네트워크 탭

네트워크 탭에서 FaceStation 의 네트워크 설정과 서버 설정을 변경할 수 있습니다.



- **TCP/IP 설정**
 - **네트워크 종류:** 랜의 종류(사용 안함, 이더넷, 무선 LAN 사용)를 선택합니다.
 - **포트:** 장치가 사용할 포트를 지정합니다.
 - **무선 랜:** 미리 설정된 무선 랜 구성을 선택합니다. 네트워크 종류에서 무선 랜을 선택해야 이 옵션을 설정할 수 있습니다.
 - **설정 변경:** 무선 랜을 설정합니다. 무선 랜의 설정 방법은 3.2.4 를 참조하십시오.

5. 사용자 설정

- DHCP 사용: 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용합니다.
- DHCP 사용 안함: 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용하지 않습니다.
- IP 주소: 장치의 IP 주소를 입력합니다.
- 서브넷: 장치의 서브넷 주소를 입력합니다.
- 게이트웨이: 네트워크의 게이트웨이를 입력합니다.
- 연결 허용: 허용할 최대 연결 수를 지정합니다.
- 서버
 - 사용: 서버 모드(장치를 BioStar 서버에 연결)를 사용합니다.
 - 사용 안함: 서버 모드를 사용하지 않습니다.
 - IP 주소: BioStar 서버의 IP 주소를 입력합니다.
 - 서버 포트: BioStar 가 사용하는 포트를 입력합니다.
 - 서버와 자동으로 시간 동기화: 장치의 시간을 서버의 시간과 동기화합니다. 장치에서 1 시간마다 서버 시간을 폴링하여, 서버의 시간과 5 초 이상 차이가 나면, 서버의 시간과 동기화합니다.
- 시리얼 설정
 - RS485 네트워크 모드: RS485 로 연결된 장치의 모드(사용 안함, 호스트, 슬레이브, PC 연결 모드)를 설정합니다. RS485 모드에 관한 자세한 내용은 3.2.1 과 3.2.2 를 참조하십시오.
 - RS485 속도: RS485 로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.
 - RS232 속도: RS232 로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.
- USB 설정: FaceStation 에 장착된 USB 포트를 활성화하려면 버튼을 클릭합니다.
 - USB: 버튼을 클릭하여 USB 연결을 허용할지 금지할지 선택합니다.
 - USB 메모리: 버튼을 클릭하여 USB 메모리 사용을 허용할지 금지할지 선택합니다.

5.1.8.5 출입그룹 탭

출입그룹 탭에서 FaceStation 의 인증 제한 설정과 기본 출입그룹을 변경할 수 있습니다.



- 인증 제한 설정
 - 인증 간격(분): 다시 출입할 수 있는 권한을 얻는 데까지 필요한 시간(분 단위)을 설정합니다. 사용자가 어느 구역에 입장하였으면, 지정된 시간 안에는 그 구역 안으로 다시 들어갈 수 없습니다.
 - 제한 옵션 1~4: 인증 제한 설정을 적용하려면 체크 상자를 선택한 후 이 설정을 적용할 시간을 입력합니다.
 - 최대 인증 허용 횟수: 지정된 인증 제한 시간 안에 허용할 최대 입장 수를 설정합니다.

5. 사용자 설정

- 기본 출입 그룹 설정: 다른 출입그룹에 포함되지 않은 새로운 사용자에게 적용할 기본 출입그룹을 선택합니다.

5.1.8.6 인터폰 탭

FaceStation 의 인터폰 기능을 사용하여 출입문 안쪽에 있는 상대방과 전화 통화할 수 있습니다.

아날로그 인터폰, IP 인터폰, BioStar VideoPhone 등 3 가지 종류가 지원됩니다. BioStar VideoPhone 은 음성 및 영상 통화가 지원되는 인터폰으로서, FaceStation V1.0 이상의 펌웨어에서만 지원됩니다. 별도로 제공되는 프로그램을 PC 에 설치해야 합니다. 프로그램 설치 및 사용 방법은 BioStar VideoPhone 사용자 매뉴얼을 참조하십시오.

사용하고자 하는 인터폰 종류에 따라 다음 옵션을 설정할 수 있습니다.

- 인터폰
 - VOIP 서버 IP: VoIP 서버의 IP 주소를 입력합니다.
 - VOIP 표시명: VoIP의 사용자 지정 이름을 입력합니다.
 - VOIP 전화번호: VoIP 전화번호를 입력합니다.
 - VOIP ID: VoIP 서버의 ID 를 입력합니다.
 - VOIP 비밀번호: VoIP 서버의 비밀번호를 입력합니다.
 - 스피커 게인: 스피커의 음량을 조절합니다(1~10).
 - 마이크 게인: 마이크의 음량을 조절합니다(1~10).
- 비디오폰
 - 모드: 단일 또는 내선 2 가지 모드가 지원됩니다. 단일 모드는 장치에서 1 대의 PC 와 연결 가능하며, 내선 모드는 최대 8대의 PC 와 연결할 수 있습니다.
 - 장치 비밀번호: 장치에서 설정한 비밀번호를 입력합니다. 이 비밀번호는 BioStar VideoPhone 프로그램에서 장치에 로그인하기 위해 필요합니다.
 - 출입문 제어: PC 에서 원격으로 출입문을 열 수 있도록 허용합니다.

5.1.8.7 입력 탭

입력 탭에는 FaceStation 에 지정된 입력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 입력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Input 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 입력 설정의 구성 방법은 3.10.3.2 를 참조하십시오.

5. 사용자 설정



- **장치:** 설정을 추가하거나 수정할 FaceStation(또는 Secure I/O)을 선택합니다.
- **포트:** Secure I/O 와 동일하게 **입력 0, 입력 1, 입력 2, 입력 3** 을 선택할 수 있습니다.
- **스위치:** 버튼을 클릭하여 입력 스위치의 보통 상태(**N/O**: 평상시 열림, **N/C**: 평상시 닫힘)를 설정합니다.
- **기능:** 입력을 받았을 때 취할 동작을 선택합니다:
 - **사용 안함:** 입력 포트를 감시하지 않습니다.
 - **일반 입력:** 지정된 동작을 실행하기 위해 입력 포트를 감시합니다. (Output 설정 대화 상자에서 지정한 이벤트를 확인하려면 5.1.8.8 을 참조하십시오.)
 - **비상 문 열림:** 이 장치가 제어하고 있는 출입문을 엽니다. 일반적인 출입문 열림 시간은 무시되며, 관리자가 출입문/구역 감시 탭을 통해서 "문 닫기" 명령을 실행하기 전까지는 출입문이 열린 채로 남아 있습니다(4.4.1 참조).
 - **모든 경보 해제:** 이 장치와 연결된 모든 경보를 해제합니다.
 - **장치 재 시작:** 장치를 껐다가 다시 시작합니다.
 - **장치 잠금:** 장치가 잠깁니다. 잠긴 장치는 BioStar 서버와 통신할 수 없으며 또한 얼굴이나 카드 입력을 처리할 수 없습니다. 통신을 다시 연결하려면, 관리자가 FaceStation 에서 직접 인증을 받아야 합니다.
- **동작시간:** 입력 신호를 감시할 일정(**사용안함, 항상적용**)을 설정합니다.
- **입력시간(ms):** 지정한 동작을 발생시키기 위해 필요한 입력 신호의 지속 시간(1000 분의 1 초)을 입력합니다.

5.1.8.8 출력 탭

출력 탭에는 FaceStation 에 적용되는 출력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 출력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Output 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 출력 설정 방법은 3.10.3.1 을 참조하십시오.

5. 사용자 설정



- **장치:** 설정을 추가하거나 수정할 장치의 종류를 선택합니다.
- **포트:** Secure I/O 와 동일하게 릴레이 0, 릴레이 1 을 선택할 수 있습니다.
- **알람 동작 개시 이벤트:** 옵션을 설정하고 **추가**를 클릭하여 알람 동작 개시 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람을 발생시킵니다.
 - **이벤트:** 알람을 발생시킬 이벤트(인증 성공, 인증 실패, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
 - **장치:** 알람을 발생시키기 위해 감시할 장치를 선택합니다.
 - **신호파형:** 메뉴 표시줄의 **옵션 > 이벤트 > Output 포트 설정**을 통해서 이미 설정한 신호파형 중에서 하나를 선택합니다.
 - **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선순위 2 의 알람 동작 개시 이벤트는 오직 우선순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.
- **알람 멈춤 이벤트:** 옵션을 설정하고 **추가**를 클릭하여 알람 멈춤 이벤트 목록에 이벤트를 추가합니다. 이러한 이벤트가 발생하면 알람이 멈춥니다.
 - **이벤트:** 알람을 멈추게 할 이벤트(인증 성공, 인증 실패, Anti-passback 제한, 권한 없음, 인증 제한, 관리자 인증 성공, Tamper 검출, 문 열림, 문 닫힘, 문 강제 열림, 문 장시간 열림, 입력 #1-3 감지)를 선택합니다.
 - **장치:** 알람을 멈추게 하기 위해 감시할 장치를 선택합니다.
 - **우선순위:** 이벤트의 우선순위를 설정합니다. 동등하거나 높은 우선 순위(1 이 가장 높은 순위)를 가진 이벤트는 이전에 발생한 이벤트를 무시하고 발생하게 됩니다. 예를 들어, 우선순위 2 의 알람 동작 개시 이벤트는 오직 우선순위 1 이나 2 의 알람 멈춤 이벤트에 의해서 취소될 수 있습니다.

5. 사용자 설정

5.1.8.9 화면/음성 탭

화면/음성 탭에서 FaceStation 의 화면 설정과 소리 설정을 변경할 수 있습니다. 변경한 설정을 적용하려면 반드시 탭의 아래에 있는 **적용**을 클릭해야 합니다. **다른장치 적용**을 클릭하여 다른 장치에 같은 설정을 적용할 수 있습니다.



그림 5.18

- **화면/음성 설정**
 - 언어: 화면에 표시할 언어(한글, 영문, 사용자 정의)를 선택합니다.
 - 하단정보: 부가적인 정보가 FaceStation 의 화면 하단에 표시될 시간(무제한, 10 초, 20 초, 30 초)을 설정합니다.
 - 백라이트 타임아웃: 화면의 조명 시간을 설정합니다.
 - 테마: 화면 테마를 설정합니다.
 - 효과음 사용: 효과음 사용 여부를 설정합니다.
 - 구성 파일: FaceStation 에서 사용할 언어 파일(변경 안함, 영어 구성 파일, 한국어 구성 파일, 사용자 정의)을 설정합니다. 영어나 한국어 이외의 언어 파일을 사용하려면, 사용자 정의를 선택한 후 줄임표(...)를 클릭한 다음, 언어 파일을 지정합니다.
 - 배경 화면: FaceStation 에서 사용할 배경화면의 종류(로고, 공지사항, 슬라이드쇼, PDF)를 설정합니다. 지원되는 파일 종류는 JPG, GIF, BMP, PNG, PDF 이며 480×800 픽셀을 초과해서는 안됩니다. 로고나 공지사항에 사용되는 그림은 오직 한번에 하나의 그림만 사용할 수 있습니다.
 - 공지사항: FaceStation 화면에 표시할 공지사항을 추가합니다. 공지사항을 추가했다면, 적용을 클릭하여 현재 선택된 장치에 적용하거나 또는 다른장치 적용을 클릭하여 다른 모든 장치에 적용할 수 있습니다.
 - 음량: FaceStation 의 음량(0% - 100%)을 설정합니다.
 - 메시지 타임아웃: 인증 실패 메시지나 인증 성공 메시지가 표시될 시간을 설정합니다.
 - 시계 표시: 시계 표시 여부를 설정합니다.

5. 사용자 설정

- **배경화면 변경:** 이 체크 상자를 선택하여 새로운 배경화면을 장치에 저장할 수 있습니다. **추가**를 클릭한 후 새로운 그림 파일을 지정해서 추가합니다.
- **효과음 변경:** 이 체크 상자를 선택하여 각 이벤트에 임의의 소리를 적용할 수 있습니다. 목록에 있는 이벤트를 클릭한 다음, **추가**를 클릭한 후 새로운 소리 파일을 지정해서 추가합니다.

5.1.8.10 근태 탭

근태 탭에서 FaceStation 장치의 근태 키 입력 방식을 설정할 수 있습니다. 설정을 저장하려면 장치 창의 하단에 있는 **적용**을 클릭해야 합니다. **다른장치 적용**을 클릭하여 다른 장치에 현재 장치의 설정을 동일하게 적용할 수 있습니다.



그림 5.19

- **근태 키 입력 방식:** 장치에 적용할 근태 키 입력 방식을 선택합니다.
 - **사용 안함:** 사용자가 장치에서 근태 이벤트를 기록할 수 없습니다.
 - **사용자 선택:** 사용자가 근태 이벤트를 기록하려고 할 때마다 목록에 맞는 근태 기능키를 눌러야 합니다.
 - **선택 후 유지:** 한 사용자가 특정 근태 기능키를 누를 경우 다른 근태 기능키를 누를 때까지 그 기능키가 유지됩니다.
 - **자동 설정:** 설정된 출입시간 일정에 맞게 FaceStation 장치가 자동으로 근태 기능을 표시합니다.
 - **이벤트 고정:** FaceStation 은 사용자가 설정한 근태 기능만 표시합니다.
- **관리:** 근태 기능에 사용할 키를 선택하고 어떤 근태 이벤트를 할당할지 설정합니다.
 - **FaceStation 기능키:** 아래 화살표를 클릭하여 목록에서 근태 기능에 사용할 키(F1~F4, EXT01~EXT12)를 선택합니다. **이벤트 고정** 방식을 선택하였다면, 오른쪽에 있는 **고정 이벤트** 체크 상자를 선택합니다.
 - **화면 표시 문구:** FaceStation 화면에 표시할 근태 기능에 맞는 문구를 입력합니다.

5. 사용자 설정

- **자동 모드 적용 시간:** 자동 설정 방식을 선택한 경우 아래 화살표를 클릭하여 목록에서 장치에 적용할 출입시간을 선택합니다. 선택한 시간에 맞추어 설정된 기능을 표시합니다. 출입시간의 추가 방법은 3.7.1 을 참조하십시오.
- **이벤트 종류:** 선택한 키에 할당할 이벤트의 종류(사용 안함, 출근, 퇴근, 들어옴, 나감)를 선택합니다. 출근 또는 퇴근을 선택한 경우 **지각/조퇴 처리 안함** 체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면 사용자의 실제 출퇴근시간에 관계없이 항상 정시에 출퇴근한 것으로 기록합니다. 근태 보고서의 결과에만 정시에 출퇴근한 것으로 기록하고 실제 근무 시간은 올바르게 계산하려면 **결과에만 적용** 체크 상자를 선택합니다. 나감을 선택한 경우에는 **이 이벤트 이후부터 근무시간에 포함** 체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면, 사용자가 근무상의 이유로 밖으로 나가는 것으로 간주하여 실제 근무 시간보다 빨리 나갔다고 하더라도 정상적으로 모든 시간을 근무한 것으로 기록합니다.

5.1.8.11 위깅드 탭

위깅드 탭에서 FaceStation 에서 사용할 Wiegand 형식을 설정할 수 있습니다. FaceStation 에서 위깅드 기능을 사용하려면 **Wiegand 입력**과 **Wiegand 출력**을 설정합니다. Wiegand 설정 마법사를 실행하려면 **포맷 변경**을 클릭합니다. 위깅드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.

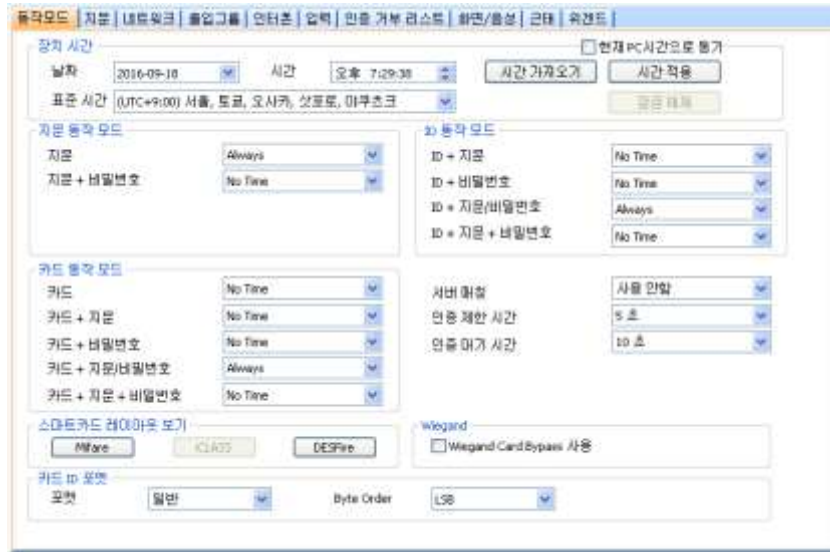
- **Wiegand 모드:** 카드 ID 데이터를 읽을 때 사용할 위깅드 모드(**일반모드**, **확장모드**)를 선택합니다. 일반모드를 선택하면 호스트 장치에 연결된 RF 장치는 호스트 장치의 일부로 인식됩니다. 확장모드를 선택하면 연결된 RF 장치가 독립된 장치로 인식됩니다. 확장모드를 이용할 경우 RF 장치는 자신의 ID 로 로그를 남길 뿐 아니라 출입문을 구성할 수 있으며 구역에 포함될 수 있습니다.
- **Wiegand 입/출력:** 위깅드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 어떻게 처리할지 선택합니다.
 - **Wiegand (카드):** 위깅드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 카드 ID 로 처리합니다.
 - **Wiegand (사용자):** 위깅드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 사용자 ID 로 처리합니다.

5.1.9 BioStation 2 설정 변경하기

5.1.9.1 동작모드 탭

동작모드 탭에서 BioStation 2의 시간을 변경할 수 있으며 동작 모드와 관련한 다양한 설정을 변경할 수 있습니다.

5. 사용자 설정



- **장치 시간**
 - 날짜: 장치에 표시할 날짜를 직접 설정합니다.
 - 시간: 장치에 표시할 시간을 직접 설정합니다.
 - 표준 시간대: 사용하려는 시간대를 선택합니다.
 - 현재 PC 시간으로 동기화: BioStar 클라이언트 프로그램이 설치되어 있는 로컬 PC의 날짜와 시간을 가져와 바로 아래 날짜와 시간 스피너 상자에 표시합니다. 시간 적용을 클릭하면, 장치의 날짜와 시간이 로컬 PC의 날짜와 시간으로 설정됩니다.
 - 시간 가져오기: 현재 장치에서 표시되고 있는 시간을 가져옵니다.
 - 시간 적용: 장치의 시간을 설정한 시간으로 변경합니다.
- **지문 동작 모드:**
 - 지문: 인증을 위해 장치가 지문만 요구하도록 설정합니다.
 - 지문 + 비밀번호: 인증을 위해 장치가 지문과 비밀번호를 요구하도록 설정합니다.
- **ID 동작모드:** 이 영역에서는 일정에 따라 각각 다른 인증 모드가 적용되도록 설정할 수 있습니다. 예를 들어, 근무 시간에는 일반적인 인증 모드를 적용하고 근무 시간 이외에는 좀더 엄격한 인증모드를 적용할 수 있습니다. 장치에 설정된 인증 모드를 적용할지 아니면 개별 사용자에게 설정된 인증 모드를 적용할지도 여기에서 설정할 수 있습니다(5.4.1 참조). 사용자의 인증 모드를 개별적으로 설정하지 않았다면, 장치에 설정된 인증 모드가 적용됩니다.
 - ID + 지문: 인증을 위해 장치가 ID와 지문을 요구하도록 설정합니다.
 - ID + 비밀번호: 인증을 위해 장치가 ID와 비밀번호를 요구하도록 설정합니다.
 - ID + 지문/비밀번호: 인증을 위해 장치가 ID와 지문 또는 ID와 비밀번호를 요구하도록 설정합니다.
 - ID + 지문 + 비밀번호: 인증을 위해 장치가 ID와 지문과 비밀번호를 요구하도록 설정합니다. (항상적용, 사용안함, 사용자가 설정한 출입시간)
- **카드 동작 모드:**
 - 카드: 인증을 위해 장치가 카드만 요구하도록 설정합니다.
 - 카드 + 지문: 인증을 위해 장치가 카드와 지문을 요구하도록 설정합니다.
 - 카드 + 비밀번호: 인증을 위해 장치가 카드와 비밀번호를 요구하도록 설정합니다.
 - 카드 + 지문/비밀번호: 인증을 위해 장치가 카드와 지문 또는 카드와 비밀번호를 요구하도록 설정합니다.

5. 사용자 설정

- **카드 + 지문 + 비밀번호:** 인증을 위해 장치가 카드와 지문과 비밀번호를 요구하도록 설정합니다. (**항상적용, 사용안함**, 사용자가 설정한 출입시간)
- **기타 옵션**
 - **서버 매칭:** 지문이 일치하는지를 장치에서 판별하지 않고 BioStar 서버에서 판별하도록 설정합니다. 이 옵션을 선택하면, 장치는 지문의 일치 여부를 판별하기 위해 사용자 ID 나 지문 템플릿이나 카드 ID 정보를 서버에 보냅니다. 사용자의 수가 너무 많아 개별 장치에 모든 정보를 저장할 수 없거나 또는 보안상의 이유로 개별 장치에 정보를 보관할 수 없을 때 이 옵션을 사용하면 편리합니다.
 - **인증 제한 시간:** 지문의 일치 여부를 판별할 때 장치가 작업을 그만두는 시간(**3 초, 7 초, 10 초, 15 초, 20 초, 30 초**)을 설정합니다.
 - **인증 대기 시간:** 크리덴셜을 두 개 이상 사용할 때 다음 크리덴셜을 인증하는 대기 시간(**3 초~20 초**)을 설정합니다.
- **스마트 카드 레이아웃 보기**
 - **MIFARE:** 장치에서 사용하고 있는 MIFARE 레이아웃을 확인합니다. MIFARE 레이아웃의 편집 방법은 3.6.4.7 을 참조하십시오.
 - **iCLASS:** 장치에서 사용하고 있는 iCLASS 레이아웃을 확인합니다. iCLASS 레이아웃의 편집 방법은 3.6.4.9 을 참조하십시오.
 - **DESFire:** 장치에서 사용하고 있는 DESFire 레이아웃을 확인합니다. DESFire 레이아웃의 편집 방법은 3.6.4.8 을 참조하십시오.
- **카드 ID 포맷**
 - **포맷:** 카드 ID 데이터를 어떤 방식으로 읽어 들일 것인가를 설정합니다. **일반**을 선택하면 카드 ID 데이터를 일반적인 형식으로 처리합니다. **Wiegand** 를 선택하면 위겐드 형식 설정에 따라 카드 ID 데이터를 처리합니다.
 - **Byte Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. **MSB** 를 선택하면 큰 단위의 바이트에서 작은 단위의 바이트 순으로 처리합니다. **LSB** 를 선택하면 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.
주의: 1.x 장치와 2.x 장치는 카드 데이터를 읽는 방식이 다르지만 BioStar 에서 카드 데이터를 보정하기 때문에 동일하게 사용할 수 있습니다. 이 때문에 1.x 장치와 2.x 장치에서 동일하게 MSB/LSB 를 설정해야 합니다. 장치가 표시하는 카드 ID 는 헥사(Hexa)값을 기준으로 표시하기 때문에 반대로 보일 수 있으나 카드 데이터는 올바르게 읽히므로 무시해도 됩니다.
 - 이중 인증 모드에서 Admin User 를 반드시 포함하는 설정 옵션을 지원합니다. 이중 인증 모드 운영 시에는 Normal User 인증 후 15 초 이내에 반드시 Admin User 가 인증해야 Door Relay 가 켜집니다. 이 옵션을 사용하지 않는 경우 기존과 동일하게 Normal User 나 Admin User 여부와 관계 없이 다른 두 사용자가 15 초 이내에 인증하면 Door Relay 가 켜지게 됩니다.
 - **Wiegand Card Bypass 사용:** BioStar 의 Wiegand 설정에 따라 인증 성공 여부와 상관 없이 CSN 을 내보내는 기능으로, BioStar 제품군 장치를 타사 ACU 와 Wiegand 로 연동하여 인증 여부를 판단하고 출입문 제어 기능이 없는 Dummy 장치로 사용하고자 할 때 필요한 기능입니다. 카드가 입력되면 장치에서는 별도의 인증 처리 없이 바로 Wiegand 로 카드 ID 를 출력하게 됩니다.

5. 사용자 설정

5.1.9.2 지문 탭

지문 탭에서 BioStation 2의 지문 인증 설정을 변경할 수 있습니다.

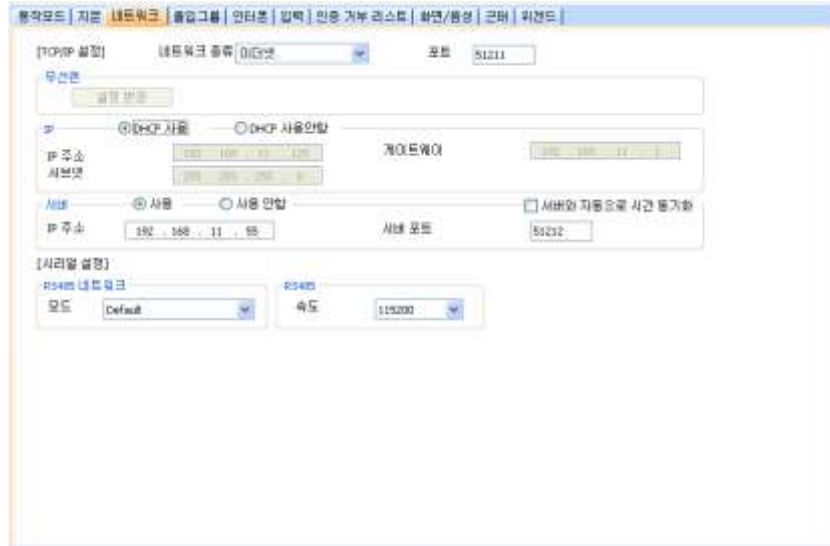


- 지문
 - 보안 등급: 지문을 인증할 때 사용할 보안 등급을 설정합니다(보통, 안전, 가장 안전). 보안 등급을 높일수록 본인 거부율(본인의 지문이 확실한데도 장치가 인식하지 못하는 확률)도 같이 증가합니다.
 - 영상 품질 기준: 지문의 품질 등급(낮음, 보통, 높음)을 설정합니다. 지문의 품질이 설정한 품질 등급보다 낮으면 시스템이 거부합니다.
 - 지문 입력 시간: 지문 입력을 끝마쳐야 하는 시간(1 초-20 초)을 설정합니다. 정해진 시간 안에 지문을 입력하지 않으면 인증이 실패하게 됩니다.
 - 등록 품질 검사: 높은 품질의 지문 정보를 저장하기 위해 스캔한 지문의 품질을 검사합니다. 사용으로 설정하면 지문 품질이 낮을 경우 사용자에게 알려주어 지문을 올바르게 스캔하도록 도와줍니다.
 - 1:N 인식 속도: 지문의 일치 여부를 판별하는 데 걸리는 시간을 줄이려면 인식 속도(자동, 보통, 빠름, 가장 빠름)를 조절합니다. 자동을 선택하면 장치에 등록된 총 지문 템플릿의 수에 따라 자동으로 판별 속도가 결정됩니다.
 - 센서 모드: 자동 켜짐으로 설정하면 지문 센서가 사용자의 손가락을 인식하여 켜집니다. 항상 켜짐으로 선택하면 센서가 항상 켜져 있습니다.
 - 등록 지문 영상: BioStation 2의 화면에 지문을 보일 것인지 말 것인지(보임, 보이지 않음)를 선택합니다.
- 지문 옵션 정보: 전체 지문 템플릿 설정을 표시합니다. 지문 템플릿에 관한 자세한 내용은 4.9를 참조하십시오.

5. 사용자 설정

5.1.9.3 네트워크 탭

네트워크 탭에서 BioStation 2의 네트워크 설정과 서버 설정을 변경할 수 있습니다.

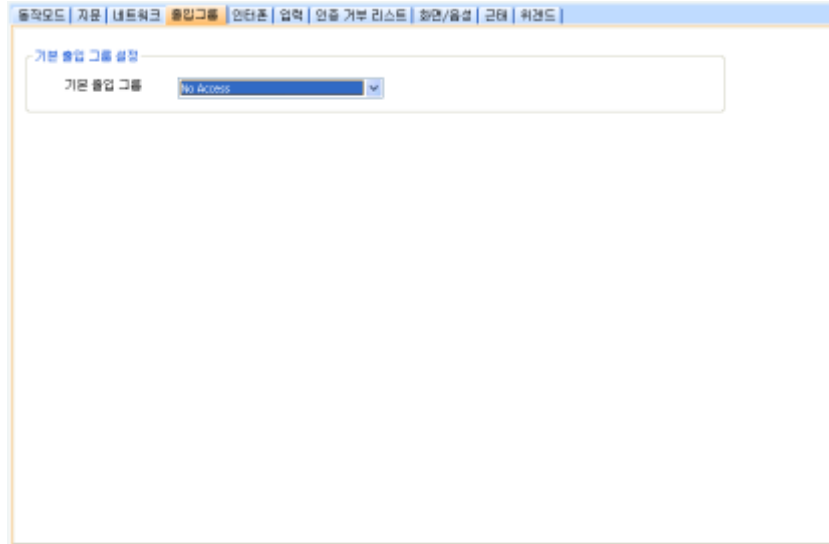


- **TCP/IP 설정**
 - **네트워크 종류:** 랜의 종류(이더넷, 무선 LAN 사용)를 선택합니다.
 - **포트:** 장치가 사용할 포트를 지정합니다.
- **무선랜**
 - **설정 변경:** 무선 랜을 설정하려면 클릭합니다. 네트워크 종류에서 무선 랜을 선택해야 이 옵션을 설정할 수 있습니다. 무선 랜을 설정하는 방법에 관한 자세한 내용은 3.2.4 를 참조하십시오.
- **IP**
 - **DHCP 사용:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용합니다.
 - **DHCP 사용 안함:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용하지 않습니다.
 - **IP 주소:** 장치의 IP 주소를 입력합니다.
 - **서브넷:** 장치의 서브넷 주소를 입력합니다.
 - **게이트웨이:** 네트워크의 게이트웨이를 입력합니다.
- **서버**
 - **사용:** 서버 모드(장치를 BioStar 서버에 연결)를 사용합니다.
 - **사용 안함:** 서버 모드를 사용하지 않습니다.
 - **IP 주소:** BioStar 서버의 IP 주소를 입력합니다.
 - **서버 포트:** BioStar 가 사용하는 포트를 입력합니다.
 - **서버와 자동으로 시간 동기화:** 장치의 시간을 서버의 시간과 동기화합니다. 장치에서 1 시간마다 서버 시간을 폴링하여, 서버의 시간과 5 초 이상 차이가 나면, 서버의 시간과 동기화합니다.
- **시리얼 설정**
 - **RS485 네트워크 모드:** RS485 로 연결된 장치의 모드(기본값, 호스트, 슬레이브)를 설정합니다. RS485 모드에 관한 자세한 내용은 3.2.1 과 3.2.2 를 참조하십시오.
 - **RS485 속도:** RS485 로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.

5. 사용자 설정

5.1.9.4 출입그룹 탭

출입그룹 탭에서 BioStation 2의 기본 출입그룹을 변경할 수 있습니다.



- **기본 출입 그룹 설정:** 다른 출입그룹에 포함되지 않은 새로운 사용자에게 적용할 기본 출입그룹을 선택합니다.

5.1.9.5 인터폰 탭

BioStation 2의 인터폰 기능을 사용하여 출입문 안쪽에 있는 상대방과 전화 통화할 수 있습니다.



아날로그 인터폰이 지원됩니다.

5.1.9.6 입력 탭

입력 탭에는 BioStation 2에 지정된 입력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 입력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Input 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 입력 설정의 구성 방법은 3.10.3.2를 참조하십시오.

5. 사용자 설정



- **작업 조건**
 - **장치:** 조건을 추가할 장치를 선택합니다.
 - **종류:** 입력 또는 이벤트를 선택할 수 있습니다.
- **입력:** 작업 조건의 종류를 입력으로 선택했을 때 설정합니다.
 - **포트:** 입력 0, 입력 1, 탬퍼를 선택할 수 있습니다.
 - **스위치:** 버튼을 클릭하여 입력 스위치의 보통 상태(N/O: 평상시 열림, N/C: 평상시 닫힘)를 설정합니다.
 - **동작시간:** 입력 신호를 감시할 일정(사용안함, 항상적용)을 설정합니다.
 - **입력시간(ms):** 지정한 동작을 발생시키기 위해 필요한 입력 신호의 지속 시간(1000분의 1 초)을 입력합니다.
- **이벤트:** 조건 이벤트를 선택합니다. 작업 조건의 종류를 이벤트로 선택했을 때 설정합니다.
- **동작**
 - **장치:** 동작을 수행할 장치를 선택합니다.
 - **종류:** Output 또는 기능을 선택할 수 있습니다.
- **출력:** 동작의 종류를 Output으로 선택했을 때 설정합니다.
 - **포트:** 신호를 출력할 장치의 릴레이를 선택합니다.
 - **신호 파형:** 메뉴 표시줄의 옵션 > 이벤트 > Output 포트 설정에서 이미 설정한 신호 파형 중 하나를 선택합니다.
- **기능:** 입력을 받았을 때 취할 동작을 선택합니다. 동작의 종류를 기능으로 선택했을 때 설정합니다.
 - **사용 안함:** 입력 포트를 감시하지 않습니다.
 - **모든 경보 해제:** 이 장치와 연결된 모든 경보를 해제합니다.
 - **장치 재 시작:** 장치를 재시동합니다.
 - **장치 잠금:** 장치가 잠깁니다. 잠긴 장치는 BioStar 서버와 통신할 수 없으며 또한 지문이나 카드 입력을 처리할 수 없습니다. 통신을 다시 연결하려면, 관리자가 BioStation 2 에서 직접 인증해야 합니다.

5.1.9.7 인증 거부 리스트 탭

인증 거부 리스트 탭에서 사용자 ID 나 카드 번호를 등록하여 사용자의 출입 시도 시 장치에서 인증되지 않도록 설정할 수 있습니다.

5. 사용자 설정



- **전체:** 인증 거부 목록에 등록된 사용자 ID 나 카드의 총 수를 표시합니다.
 - **추가가능:** 등록할 수 있는 사용자 ID 나 카드의 수를 표시합니다.
- 참고: 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있습니다.

5.1.9.8 화면/음성 탭

화면/음성 탭에서 BioStation 2 의 화면 설정과 소리 설정을 변경할 수 있습니다. 변경한 설정을 적용하려면 반드시 탭의 아래에 있는 **적용**을 클릭해야 합니다. **다른장치 적용**을 클릭하여 다른 장치에 같은 설정을 적용할 수 있습니다.



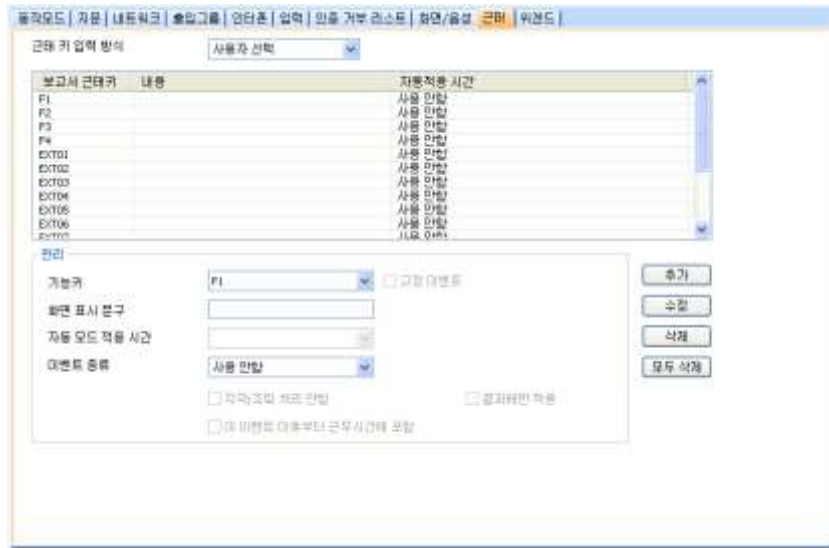
- **화면/음성 설정**
 - 언어: 화면에 표시할 언어(한글, 영문, 사용자 정의)를 선택합니다.
 - 하단정보: 부가적인 정보가 BioStation 2 의 화면 하단에 표시될 시간(무제한, 10 초, 20 초, 30 초)을 설정합니다.
 - 백라이트 타임아웃: 화면의 조명 시간을 설정합니다.
 - 테마: 화면 테마를 설정합니다.
 - 효과음 사용: 효과음 사용 여부를 설정합니다.
 - 구성 파일: BioStation 2 에서 사용할 언어 파일(변경 안함, 영어 구성 파일, 한국어 구성 파일, 사용자 정의)을 설정합니다. 영어나 한국어 이외의 언어 파일을 사용하려면, 사용자 정의를 선택한 후 줄임표(...)를 클릭한 다음, 언어 파일을 지정합니다.
 - 배경 화면: BioStation 2 에서 사용할 배경화면의 종류(로고, 공지사항, 슬라이드쇼)를 설정합니다. 지원되는 파일 종류는 JPG, GIF, BMP, PNG 이며 320×240 픽셀을 초과해서는 안됩니다. 로고나 공지사항에 사용되는 그림은 오직 한번에 하나의 그림만 사용할 수 있습니다.

5. 사용자 설정

- **공지사항:** BioStation 2 화면에 표시할 공지사항을 추가합니다. 공지사항을 추가했다면, 적용을 클릭하여 현재 선택된 장치에 적용하거나 또는 **다른장치 적용**을 클릭하여 다른 모든 장치에 적용할 수 있습니다.
- **음량:** BioStation 2의 음량(0% - 100%)을 설정합니다.
- **메시지 타임아웃:** 인증 실패 메시지나 인증 성공 메시지가 표시될 시간을 설정합니다.
- **시계 표시:** 시계 표시 여부를 설정합니다.
- **배경화면 변경:** 이 체크 상자를 선택하여 새로운 배경화면을 장치에 저장할 수 있습니다. **추가**를 클릭한 후 새로운 그림 파일을 지정해서 추가합니다.
- **효과음 변경:** 이 체크 상자를 선택하여 각 이벤트에 임의의 소리를 적용할 수 있습니다. 목록에 있는 이벤트를 클릭한 다음, **추가**를 클릭한 후 새로운 소리 파일을 지정해서 추가합니다.

5.1.9.9 근태 탭

근태 탭에서 BioStation 2 장치의 근태 키 입력 방식을 설정할 수 있습니다. 설정을 저장하려면 장치 창의 하단에 있는 **적용**을 클릭해야 합니다. **다른장치 적용**을 클릭하여 다른 장치에 현재 장치의 설정을 동일하게 적용할 수 있습니다.



- **근태 키 입력 방식:** 장치에 적용할 근태 키 입력 방식을 선택합니다.
 - **사용 안함:** 사용자가 장치에서 근태 이벤트를 기록할 수 없습니다.
 - **사용자 선택:** 사용자가 근태 이벤트를 기록하려고 할 때마다 목록에 맞는 근태 기능키를 눌러야 합니다.
 - **선택 후 유지:** 한 사용자가 특정 근태 기능키를 누를 경우 다른 근태 기능키를 누를 때까지 그 기능키가 유지됩니다.
 - **자동 설정:** 설정된 출입시간 일정에 맞게 BioStation 2 장치가 자동으로 근태 기능을 표시합니다.
 - **이벤트 고정:** BioStation T2은 사용자가 설정한 근태 기능만 표시합니다.
- **관리:** 근태 기능에 사용할 키를 선택하고 어떤 근태 이벤트를 할당할지 설정합니다.
 - **BioStation 2 기능키:** 아래 화살표를 클릭하여 목록에서 근태 기능에 사용할 키(F1~F4, EXT01~EXT12)를 선택합니다. **이벤트 고정** 방식을 선택하였다면, 오른쪽에 있는 **고정 이벤트체크** 상자를 선택합니다.
 - **화면 표시 문구:** BioStation 2 화면에 표시할 근태 기능에 맞는 문구를 입력합니다.

5. 사용자 설정

- **자동 모드 적용 시간:** 자동 설정 방식을 선택한 경우 아래 화살표를 클릭하여 목록에서 장치에 적용할 출입시간을 선택합니다. 선택한 시간에 맞추어 설정된 기능을 표시합니다. 출입시간을 추가하는 방법에 관해서는 3. 7.1 을 참조하십시오.
- **이벤트 종류:** 선택한 키에 할당할 이벤트의 종류(사용 안함, 출근, 퇴근, 들어옴, 나감)를 선택합니다. 출근 또는 퇴근을 선택한 경우 **지각/조퇴 처리 안함** 체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면 사용자의 실제 출퇴근 시간에 관계없이 항상 정시에 출퇴근한 것으로 기록합니다. 근태 보고서의 결과에만 정시에 출퇴근한 것으로 기록하고 실제 근무 시간은 올바르게 계산하려면 **결과에만 적용체크** 상자를 선택합니다. 나감을 선택한 경우에는 **이 이벤트 이후부터 근무시간에 포함체크** 상자를 선택할 수 있습니다. 이 옵션을 선택하면, 사용자가 근무상의 이유로 밖으로 나가는 것으로 간주하여 실제 근무 시간보다 빨리 나갔다고 하더라도 정상적으로 모든 시간을 근무한 것으로 기록합니다.

5.1.9.10 위캔드 탭

위캔드 탭에서 BioStation T2 에서 사용할 Wiegand 형식을 설정할 수 있습니다. BioStation 2 에서 위캔드 기능을 사용하려면 **Wiegand 입력**과 **Wiegand 출력**을 설정합니다. Wiegand 설정 마법사를 실행하려면 **포맷 변경**을 클릭합니다. 위캔드 형식에 관한 자세한 내용은 3.2.16 을 참조하십시오.



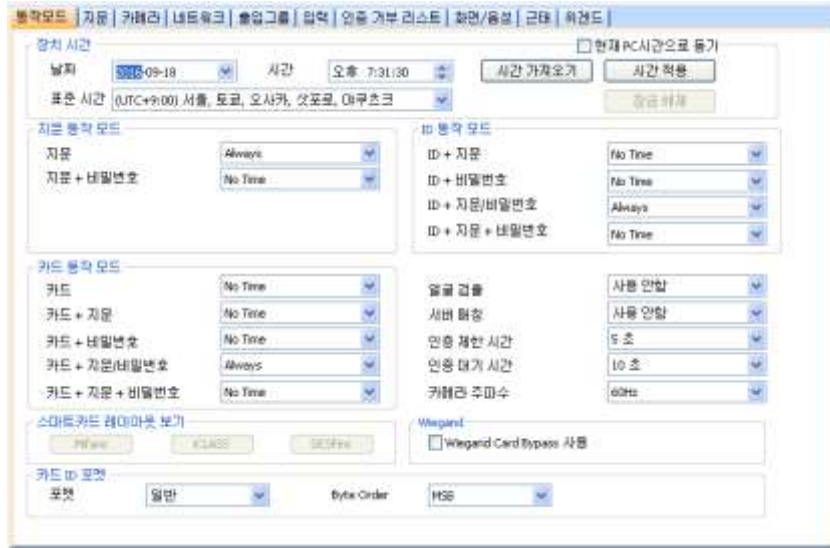
- **Wiegand 모드:** 카드 ID 데이터를 읽을 때 사용할 위캔드 모드(확장모드)를 선택합니다. 확장모드를 선택하면 연결된 RF 장치가 독립된 장치로 인식됩니다. 확장모드를 이용할 경우 RF 장치는 자신의 ID 로 로그를 남길 뿐 아니라 출입문을 구성할 수 있으며 구역에 포함될 수 있습니다.
- **Wiegand 입/출력:** 위캔드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 어떻게 처리할지 선택합니다.
 - **Wiegand (카드):** 위캔드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 카드 ID 로 처리합니다.

5.1.10 BioStation A2 설정 변경하기

5.1.10.1 동작모드 탭

동작모드 탭에서 BioStation A2 의 시간을 변경할 수 있으며 동작 모드와 관련한 다양한 설정을 변경할 수 있습니다.

5. 사용자 설정



- **장치 시간**
 - 날짜: 장치에 표시할 날짜를 직접 설정합니다.
 - 시간: 장치에 표시할 시간을 직접 설정합니다.
 - 표준 시간대: 사용하려는 시간대를 선택합니다.
 - 현재 PC 시간으로 동기화: BioStar 클라이언트 프로그램이 설치되어 있는 로컬 PC의 날짜와 시간을 가져와 바로 아래 날짜와 시간 스피너 상자에 표시합니다. 시간 적용을 클릭하면, 장치의 날짜와 시간이 로컬 PC의 날짜와 시간으로 설정됩니다.
 - 시간 가져오기: 현재 장치에서 표시되고 있는 시간을 가져옵니다.
 - 시간 적용: 장치의 시간을 설정한 시간으로 변경합니다.
- **지문 동작 모드:**
 - 지문: 인증을 위해 장치가 지문만 요구하도록 설정합니다.
 - 지문 + 비밀번호: 인증을 위해 장치가 지문과 비밀번호를 요구하도록 설정합니다.
- **ID 동작모드:** 이 영역에서는 일정에 따라 각각 다른 인증 모드가 적용되도록 설정할 수 있습니다. 예를 들어, 근무 시간에는 일반적인 인증 모드를 적용하고 근무 시간 이외에는 좀더 엄격한 인증모드를 적용할 수 있습니다. 장치에 설정된 인증 모드를 적용하지 아니면 개별 사용자에게 설정된 인증 모드를 적용할지도 여기에서 설정할 수 있습니다(5.4.1 참조). 사용자의 인증 모드를 개별적으로 설정하지 않았다면, 장치에 설정된 인증 모드가 적용됩니다.
 - ID + 지문: 인증을 위해 장치가 ID와 지문을 요구하도록 설정합니다.
 - ID + 비밀번호: 인증을 위해 장치가 ID와 비밀번호를 요구하도록 설정합니다.
 - ID + 지문/비밀번호: 인증을 위해 장치가 ID와 지문 또는 ID와 비밀번호를 요구하도록 설정합니다.
 - ID + 지문 + 비밀번호: 인증을 위해 장치가 ID와 지문과 비밀번호를 요구하도록 설정합니다. (항상적용, 사용안함, 사용자가 설정한 출입시간)
- **카드 동작 모드:**
 - 카드: 인증을 위해 장치가 카드만 요구하도록 설정합니다.
 - 카드 + 지문: 인증을 위해 장치가 카드와 지문을 요구하도록 설정합니다.
 - 카드 + 비밀번호: 인증을 위해 장치가 카드와 비밀번호를 요구하도록 설정합니다.

5. 사용자 설정

- **카드 + 지문/비밀번호:** 인증을 위해 장치가 카드와 지문 또는 카드와 비밀번호를 요구하도록 설정합니다.
- **카드 + 지문 + 비밀번호:** 인증을 위해 장치가 카드와 지문과 비밀번호를 요구하도록 설정합니다. (**항상적용, 사용안함**, 사용자가 설정한 출입시간)
- **기타 옵션**
 - **얼굴 검출:** 인증이 성공하였을 때 얼굴 이미지를 강제로 검출하여 출입하는 사용자의 얼굴 이미지를 확보합니다.
 - **서버 매칭:** 지문이 일치하는지를 장치에서 판별하지 않고 BioStar 서버에서 판별하도록 설정합니다. 이 옵션을 선택하면, 장치는 지문의 일치 여부를 판별하기 위해 사용자 ID 나 지문 템플릿이나 카드 ID 정보를 서버에 보냅니다. 사용자의 수가 너무 많아 개별 장치에 모든 정보를 저장할 수 없거나 또는 보안상의 이유로 개별 장치에 정보를 보관할 수 없을 때 이 옵션을 사용하면 편리합니다.
 - **인증 제한 시간:** 지문의 일치 여부를 판별할 때 장치가 작업을 그만두는 시간(**3 초, 7 초, 10 초, 15 초, 20 초, 30 초**)을 설정합니다.
 - **인증 대기 시간:** 크리덴셜을 두 개 이상 사용할 때 다음 크리덴셜을 인증하는 대기 시간(**3 초~20 초**)을 설정합니다.
 - **카메라 주파수:** 카메라 주파수를 설정합니다. 형광등을 사용하는 환경에서 주파수를 잘못 설정하면 이미지에 깜빡임이 발생할 수 있으므로, 해당 지역의 대리점에 문의하십시오. (**50 Hz, 60 Hz**)
- **스마트 카드 레이아웃 보기**
 - **MIFARE:** 장치에서 사용하고 있는 MIFARE 레이아웃을 확인합니다. MIFARE 레이아웃의 편집 방법은 3.6.4.7 을 참조하십시오.
 - **iCLASS:** 장치에서 사용하고 있는 iCLASS 레이아웃을 확인합니다. iCLASS 레이아웃의 편집 방법은 3.6.4.9 을 참조하십시오.
 - **DESFire:** 장치에서 사용하고 있는 DESFire 레이아웃을 확인합니다. DESFire 레이아웃의 편집 방법은 3.6.4.8 을 참조하십시오.
- **카드 ID 포맷**
 - **포맷:** 카드 ID 데이터를 어떤 방식으로 읽어 들일 것인가를 설정합니다. **일반**을 선택하면 카드 ID 데이터를 일반적인 형식으로 처리합니다. **Wiegand** 를 선택하면 위간드 형식 설정에 따라 카드 ID 데이터를 처리합니다.
 - **Byte Order:** 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. **MSB** 를 선택하면 큰 단위의 바이트에서 작은 단위의 바이트 순으로 처리합니다. **LSB** 를 선택하면 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.
주의: 1.x 장치와 2.x 장치는 카드 데이터를 읽는 방식이 다르지만 BioStar 에서 카드 데이터를 보정하기 때문에 동일하게 사용할 수 있습니다. 이 때문에 1.x 장치와 2.x 장치에서 동일하게 MSB/LSB 를 설정해야 합니다. 장치가 표시하는 카드 ID 는 헥사(Hexa)값을 기준으로 표시하기 때문에 반대로 보일 수 있으나 카드 데이터는 올바르게 읽히므로 무시해도 됩니다.
 - 이중 인증 모드에서 Admin User 를 반드시 포함하는 설정 옵션을 지원합니다. 이중 인증 모드 운영 시에는 Normal User 인증 후 15 초 이내에 반드시 Admin User 가 인증해야 Door Relay 가 켜집니다. 이 옵션을 사용하지 않는 경우 기존과 동일하게 Normal User 나 Admin User 여부와 관계 없이 다른 두 사용자가 15 초 이내에 인증하면 Door Relay 가 켜지게 됩니다.
 - **Wiegand Card Bypass 사용:** BioStar 의 Wiegand 설정에 따라 인증 성공 여부와 상관 없이 CSN 을 내보내는 기능으로, BioStar 제품군 장치를 타사 ACU 와 Wiegand 로 연동하여 인증 여부를 판단하고 출입문 제어 기능이 없는 Dummy

5. 사용자 설정

장치로 사용하고자 할 때 필요한 기능입니다. 카드가 입력되면 장치에서는 별도의 인증 처리 없이 바로 Wiegand 로 카드 ID 를 출력하게 됩니다.

5.1.10.2 지문 탭

지문 탭에서 BioStation A2 의 지문 인증 설정을 변경할 수 있습니다.



- **지문**
 - **보안 등급:** 지문을 인증할 때 사용할 보안 등급을 설정합니다(보통, 안전, 가장 안전). 보안 등급을 높일수록 본인 거부율(본인의 지문이 확실한데도 장치가 인식하지 못하는 확률)도 같이 증가합니다.
 - **영상 품질 기준:** 지문의 품질 등급(낮음, 보통, 높음)을 설정합니다. 지문의 품질이 설정한 품질 등급보다 낮으면 시스템이 거부합니다.
 - **지문 입력 시간:** 지문 입력을 끝마쳐야 하는 시간(1 초-20 초)을 설정합니다. 정해진 시간 안에 지문을 입력하지 않으면 인증이 실패하게 됩니다.
 - **등록 품질 검사:** 높은 품질의 지문 정보를 저장하기 위해 스캔한 지문의 품질을 검사합니다. **사용**으로 설정하면 지문 품질이 낮을 경우 사용자에게 알려주어 지문을 올바르게 스캔하도록 도와줍니다.
 - **1:N 인식 속도:** 지문의 일치 여부를 판별하는 데 걸리는 시간을 줄이려면 인식 속도(자동, 보통, 빠름, 가장 빠름)를 조절합니다. **자동**을 선택하면 장치에 등록된 총 지문 템플릿의 수에 따라 자동으로 판별 속도가 결정됩니다.
 - **센서 모드:** **자동 켜짐**으로 설정하면 지문 센서가 사용자의 손가락을 인식하여 켜집니다. **항상 켜짐**으로 선택하면 센서가 항상 켜져 있습니다.
 - **등록 지문 영상:** BioStation A2 의 화면에 지문을 보일 것인지 말 것인지(보임, 보이지 않음)를 선택합니다.
 - **위조 지문 검사:** 위조 지문 공격을 방지하기 위하여 위조 지문을 검사할지(**사용**) 검사하지 않을지(**사용 안함**) 설정합니다.
- **지문 옵션 정보:** 전체 지문 템플릿 설정을 표시합니다. 지문 템플릿에 관한 자세한 내용은 4.9 를 참조하십시오.

5. 사용자 설정

5.1.10.3 카메라 탭

카메라 탭에서 BioStation A2의 카메라 설정을 변경할 수 있습니다. 출입 시간대별 발생하는 이벤트에 따라 카메라의 작동을 설정할 수 있습니다. **추가**를 클릭하여 카메라를 작동할 이벤트를 추가한 후 **적용**을 클릭하여 변경 사항을 저장합니다.



주의: 보안을 위해 카메라 이벤트에 인증 이벤트를 추가할 것을 권장합니다. 장치와 서버간의 네트워크 부하를 줄이기 위해 최대 30개의 이벤트만 추가하십시오.

5.1.10.4 네트워크 탭

네트워크 탭에서 BioStation A2의 네트워크 설정과 서버 설정을 변경할 수 있습니다.



- **TCP/IP 설정**
 - **네트워크 종류:** 랜의 종류(이더넷, 무선 LAN 사용)를 선택합니다.
 - **포트:** 장치가 사용할 포트를 지정합니다.
- **무선랜**
 - **설정 변경:** 무선 랜을 설정하려면 클릭합니다. 네트워크 종류에서 **무선 랜**을 선택해야 이 옵션을 설정할 수 있습니다. 무선 랜을 설정하는 방법에 관한 자세한 내용은 3.2.4를 참조하십시오.
- **IP**
 - **DHCP 사용:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용합니다.
 - **DHCP 사용 안함:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용하지 않습니다.
 - **IP 주소:** 장치의 IP 주소를 입력합니다.
 - **서브넷:** 장치의 서브넷 주소를 입력합니다.
 - **게이트웨이:** 네트워크의 게이트웨이를 입력합니다.
- **서버**
 - **사용:** 서버 모드(장치를 BioStar 서버에 연결)를 사용합니다.

5. 사용자 설정

- **사용 안함:** 서버 모드를 사용하지 않습니다.
- **IP 주소:** BioStar 서버의 IP 주소를 입력합니다.
- **서버 포트:** BioStar 가 사용하는 포트를 입력합니다.
- **서버와 자동으로 시간 동기화:** 장치의 시간을 서버의 시간과 동기화합니다. 장치에서 1 시간마다 서버 시간을 폴링하여, 서버의 시간과 5 초 이상 차이가 나면, 서버의 시간과 동기화합니다.
- **시리얼 설정**
 - **RS485 네트워크 모드:** RS485 로 연결된 장치의 모드(기본값, 호스트, 슬레이브)를 설정합니다. RS485 모드에 관한 자세한 내용은 3.2.1 과 3.2.2 를 참조하십시오.
 - **RS485 속도:** RS485 로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.

5.1.10.5 출입그룹 탭

출입그룹 탭에서 BioStation A2 의 기본 출입그룹을 변경할 수 있습니다.



- **기본 출입 그룹 설정:** 다른 출입그룹에 포함되지 않은 새로운 사용자에게 적용할 기본 출입그룹을 선택합니다.

5.1.10.6 입력 탭

입력 탭에는 BioStation A2 에 지정된 입력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 입력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Input 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 입력 설정의 구성 방법은 3.10.3.2 를 참조하십시오.



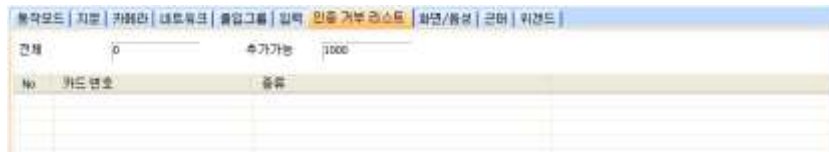
- **작업 조건**
 - **장치:** 조건을 추가할 장치를 선택합니다.
 - **종류:** 입력 또는 이벤트를 선택할 수 있습니다.
- **입력:** 작업 조건의 종류를 입력으로 선택했을 때 설정합니다.
 - **포트:** 입력 0, 입력 1, 탬퍼를 선택할 수 있습니다.

5. 사용자 설정

- 스위치: 버튼을 클릭하여 입력 스위치의 보통 상태(N/O: 평상시 열림, N/C: 평상시 닫힘)를 설정합니다.
- 동작시간: 입력 신호를 감시할 일정(사용안함, 항상적용)을 설정합니다.
- 입력시간(ms): 지정한 동작을 발생시키기 위해 필요한 입력 신호의 지속 시간(1000 분의 1 초)을 입력합니다.
- 이벤트: 조건 이벤트를 선택합니다. 작업 조건의 종류를 이벤트로 선택했을 때 설정합니다.
- 동작
 - 장치: 동작을 수행할 장치를 선택합니다.
 - 종류: Output 또는 기능을 선택할 수 있습니다.
- 출력: 동작의 종류를 Output 으로 선택했을 때 설정합니다.
 - 포트: 신호를 출력할 장치의 릴레이를 선택합니다.
 - 신호 파형: 메뉴 표시줄의 옵션 > 이벤트 > Output 포트 설정에서 이미 설정한 신호 파형 중 하나를 선택합니다.
- 기능: 입력을 받았을 때 취할 동작을 선택합니다. 동작의 종류를 기능으로 선택했을 때 설정합니다.
 - 사용 안함: 입력 포트를 감시하지 않습니다.
 - 모든 경보 해제: 이 장치와 연결된 모든 경보를 해제합니다.
 - 장치 재 시작: 장치를 재시동합니다.
 - 장치 잠금: 장치가 잠깁니다. 잠긴 장치는 BioStar 서버와 통신할 수 없으며 또한 지문이나 카드 입력을 처리할 수 없습니다. 통신을 다시 연결하려면, 관리자가 BioStation 2 에서 직접 인증해야 합니다.

5.1.10.7 인증 거부 리스트 탭

인증 거부 리스트 탭에서 사용자 ID 나 카드 번호를 등록하여 사용자의 출입 시도 시 장치에서 인증되지 않도록 설정할 수 있습니다.



- 전체: 인증 거부 목록에 등록된 사용자 ID 나 카드의 총 수를 표시합니다.
- 추가가능: 등록할 수 있는 사용자 ID 나 카드의 수를 표시합니다.

참고: 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있습니다.

5.1.10.8 화면/음성 탭

화면/음성 탭에서 BioStation A2 의 화면 설정과 소리 설정을 변경할 수 있습니다. 변경한 설정을 적용하려면 반드시 탭의 아래에 있는 적용을 클릭해야 합니다. 다른장치 적용을 클릭하여 다른 장치에 같은 설정을 적용할 수 있습니다.

5. 사용자 설정

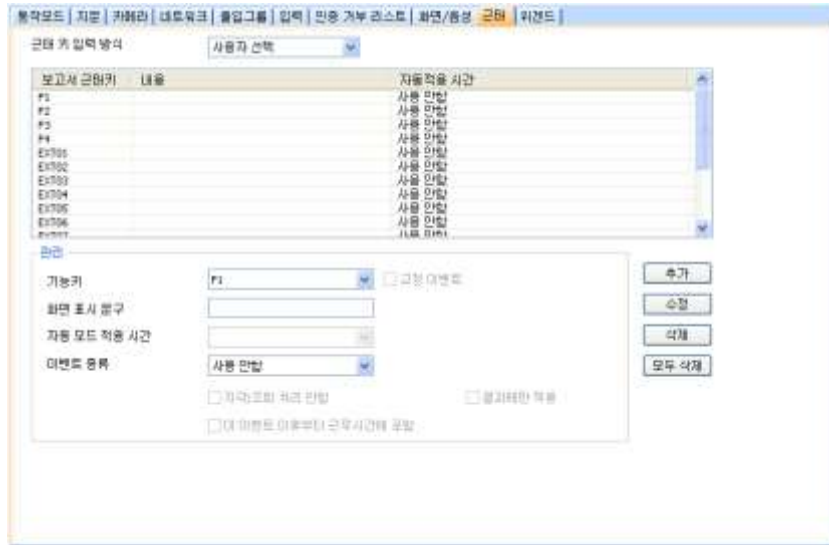


- **화면/음성 설정**
 - 언어: 화면에 표시할 언어(한글, 영문, 사용자 정의)를 선택합니다.
 - 하단정보: 추가적인 정보가 BioStation A2 의 화면 하단에 표시될 시간(무제한, 10 초, 20 초, 30 초)을 설정합니다.
 - 백라이트 타임아웃: 화면의 조명 시간을 설정합니다.
 - 효과음 사용: 효과음 사용 여부를 설정합니다.
 - 구성 파일: BioStation A2 에서 사용할 언어 파일(변경 안함, 영어 구성 파일, 한국어 구성 파일, 사용자 정의)을 설정합니다. 영어나 한국어 이외의 언어 파일을 사용하려면, 사용자 정의를 선택한 후 줄임표(...)를 클릭한 다음, 언어 파일을 지정합니다.
 - 배경 화면: BioStation A2 에서 사용할 배경화면의 종류(로고, 공지사항, 슬라이드쇼)를 설정합니다. 지원되는 파일 종류는 JPG, GIF, BMP, PNG 이며 480×854 픽셀을 초과해서는 안됩니다. 로고나 공지사항에 사용되는 그림은 오직 한번에 하나의 그림만 사용할 수 있습니다.
 - 공지사항: BioStation A2 화면에 표시할 공지사항을 추가합니다. 공지사항을 추가했다면, 적용을 클릭하여 현재 선택된 장치에 적용하거나 또는 다른장치 적용을 클릭하여 다른 모든 장치에 적용할 수 있습니다.
 - 음량: BioStation A2 의 음량(0% - 100%)을 설정합니다.
 - 메시지 타임아웃: 인증 실패 메시지나 인증 성공 메시지가 표시될 시간을 설정합니다.
 - 시계 표시: 시계 표시 여부를 설정합니다.
- **배경화면 변경:** 이 체크 상자를 선택하여 새로운 배경화면을 장치에 저장할 수 있습니다. 추가를 클릭한 후 새로운 그림 파일을 지정해서 추가합니다.
- **효과음 변경:** 이 체크 상자를 선택하여 각 이벤트에 임의의 소리를 적용할 수 있습니다. 목록에 있는 이벤트를 클릭한 다음, 추가를 클릭한 후 새로운 소리 파일을 지정해서 추가합니다.

5.1.10.9 근태 탭

근태 탭에서 BioStation A2 장치의 근태 키 입력 방식을 설정할 수 있습니다. 설정을 저장하려면 장치 창의 하단에 있는 적용을 클릭해야 합니다. 다른장치 적용을 클릭하여 다른 장치에 현재 장치의 설정을 동일하게 적용할 수 있습니다.

5. 사용자 설정



- 근태 키 입력 방식: 장치에 적용할 근태 키 입력 방식을 선택합니다.
 - 사용 안함: 사용자가 장치에서 근태 이벤트를 기록할 수 없습니다.
 - 사용자 선택: 사용자가 근태 이벤트를 기록하려고 할 때마다 목적에 맞는 근태 기능키를 눌러야 합니다.
 - 선택 후 유지: 한 사용자가 특정 근태 기능키를 누를 경우 다른 근태 기능키를 누를 때까지 그 기능키가 유지됩니다.
 - 자동 설정: 설정된 출입시간 일정에 맞게 BioStation A2 장치가 자동으로 근태 기능을 표시합니다.
 - 이벤트 고정: BioStation A2 은 사용자가 설정한 근태 기능만 표시합니다.
- 관리: 근태 기능에 사용할 키를 선택하고 어떤 근태 이벤트를 할당할지 설정합니다.
 - BioStation A2 기능키: 아래 화살표를 클릭하여 목록에서 근태 기능에 사용할 키(F1~F4, EXT01~EXT12)를 선택합니다. 이벤트 고정 방식을 선택하였다면, 오른쪽에 있는 고정 이벤트체크 상자를 선택합니다.
 - 화면 표시 문구: BioStation A2 화면에 표시할 근태 기능에 맞는 문구를 입력합니다.
 - 자동 모드 적용 시간: 자동 설정 방식을 선택한 경우 아래 화살표를 클릭하여 목록에서 장치에 적용할 출입시간을 선택합니다. 선택한 시간에 맞추어 설정된 기능을 표시합니다. 출입시간을 추가하는 방법에 관해서는 3. 7.1 을 참조하십시오.
 - 이벤트 종류: 선택한 키에 할당할 이벤트의 종류(사용 안함, 출근, 퇴근, 들어옴, 나감)를 선택합니다. 출근 또는 퇴근을 선택한 경우 지각/조퇴 처리 안함 체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면 사용자의 실제 출퇴근 시간에 관계없이 항상 정시에 출퇴근한 것으로 기록합니다. 근태 보고서의 결과에만 정시에 출퇴근한 것으로 기록하고 실제 근무 시간은 올바르게 계산하려면 결과에만 적용체크 상자를 선택합니다. 나감을 선택한 경우에는 이 이벤트 이후부터 근무시간에 포함체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면, 사용자가 근무상의 이유로 밖으로 나가는 것으로 간주하여 실제 근무 시간보다 빨리 나갔다고 하더라도 정상적으로 모든 시간을 근무한 것으로 기록합니다.

5.1.10.10 위깅드 탭

위깅드 탭에서 BioStation A2 에서 사용할 Wiegand 형식을 설정할 수 있습니다. BioStation A2 에서 위깅드 기능을 사용하려면 Wiegand 입력과 Wiegand 출력을 설정합니다. Wiegand

5. 사용자 설정

설정 마법사를 실행하려면 **포맷 변경**을 클릭합니다. 위갠드 형식에 관한 자세한 내용은 3.2.16을 참조하십시오.

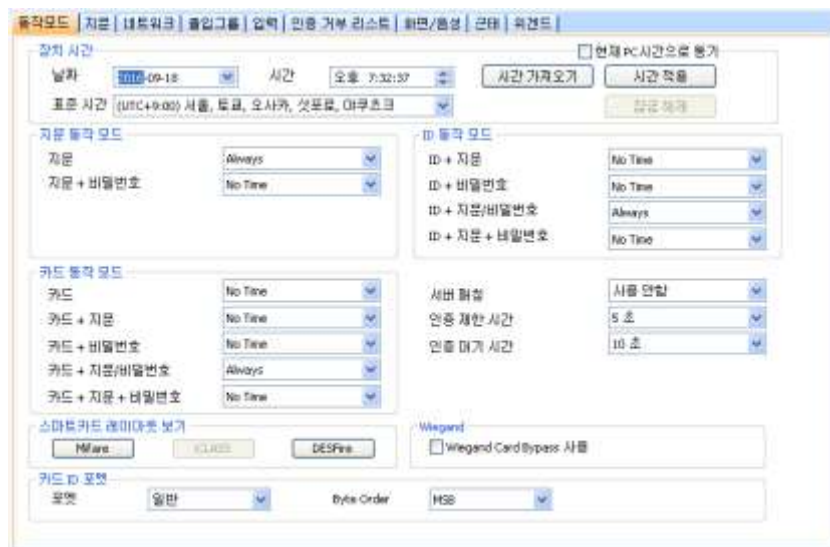


- **Wiegand 모드:** 카드 ID 데이터를 읽을 때 사용할 위갠드 모드(**확장모드**)를 선택합니다. 확장모드를 선택하면 연결된 RF 장치가 독립된 장치로 인식됩니다. 확장모드를 이용할 경우 RF 장치는 자신의 ID 로 로그를 남길 뿐 아니라 출입문을 구성할 수 있으며 구역에 포함될 수 있습니다.
- **Wiegand 입/출력:** 위갠드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 어떻게 처리할지 선택합니다.
 - **Wiegand (카드):** 위갠드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 카드 ID 로 처리합니다.

5.1.11 BioStation L2 설정 변경하기

5.1.11.1 동작모드 탭

동작모드 탭에서 BioStation L2 의 시간을 변경할 수 있으며 동작 모드와 관련한 다양한 설정을 변경할 수 있습니다.



- **장치 시간**
 - 날짜: 장치에 표시할 날짜를 직접 설정합니다.
 - 시간: 장치에 표시할 시간을 직접 설정합니다.

5. 사용자 설정

- **표준 시간대:** 사용하려는 시간대를 선택합니다.
- **현재 PC 시간으로 동기화:** BioStar 클라이언트 프로그램이 설치되어 있는 로컬 PC의 날짜와 시간을 가져와 바로 아래 날짜와 시간 스피너 상자에 표시합니다. 시간 적용을 클릭하면, 장치의 날짜와 시간이 로컬 PC의 날짜와 시간으로 설정됩니다.
- **시간 가져오기:** 현재 장치에서 표시되고 있는 시간을 가져옵니다.
- **시간 적용:** 장치의 시간을 설정한 시간으로 변경합니다.
- **지문 동작 모드:**
 - **지문:** 인증을 위해 장치가 지문만 요구하도록 설정합니다.
 - **지문 + 비밀번호:** 인증을 위해 장치가 지문과 비밀번호를 요구하도록 설정합니다.
- **ID 동작모드:** 이 영역에서는 일정에 따라 각각 다른 인증 모드가 적용되도록 설정할 수 있습니다. 예를 들어, 근무 시간에는 일반적인 인증 모드를 적용하고 근무 시간 이외에는 좀더 엄격한 인증모드를 적용할 수 있습니다. 장치에 설정된 인증 모드를 적용할지 아니면 개별 사용자에게 설정된 인증 모드를 적용할지도 여기에서 설정할 수 있습니다(5.4.1 참조). 사용자의 인증 모드를 개별적으로 설정하지 않았다면, 장치에 설정된 인증 모드가 적용됩니다.
 - **ID + 지문:** 인증을 위해 장치가 ID와 지문을 요구하도록 설정합니다.
 - **ID + 비밀번호:** 인증을 위해 장치가 ID와 비밀번호를 요구하도록 설정합니다.
 - **ID + 지문/비밀번호:** 인증을 위해 장치가 ID와 지문 또는 ID와 비밀번호를 요구하도록 설정합니다.
 - **ID + 지문 + 비밀번호:** 인증을 위해 장치가 ID와 지문과 비밀번호를 요구하도록 설정합니다. (**항상적용, 사용안함**, 사용자가 설정한 출입시간)
- **카드 동작 모드:**
 - **카드:** 인증을 위해 장치가 카드만 요구하도록 설정합니다.
 - **카드 + 지문:** 인증을 위해 장치가 카드와 지문을 요구하도록 설정합니다.
 - **카드 + 비밀번호:** 인증을 위해 장치가 카드와 비밀번호를 요구하도록 설정합니다.
 - **카드 + 지문/비밀번호:** 인증을 위해 장치가 카드와 지문 또는 카드와 비밀번호를 요구하도록 설정합니다.
 - **카드 + 지문 + 비밀번호:** 인증을 위해 장치가 카드와 지문과 비밀번호를 요구하도록 설정합니다. (**항상적용, 사용안함**, 사용자가 설정한 출입시간)
- **기타 옵션**
 - **서버 매칭:** 지문이 일치하는지를 장치에서 판별하지 않고 BioStar 서버에서 판별하도록 설정합니다. 이 옵션을 선택하면, 장치는 지문의 일치 여부를 판별하기 위해 사용자 ID나 지문 템플릿이나 카드 ID 정보를 서버에 보냅니다. 사용자의 수가 너무 많아 개별 장치에 모든 정보를 저장할 수 없거나 또는 보안상의 이유로 개별 장치에 정보를 보관할 수 없을 때 이 옵션을 사용하면 편리합니다.
 - **인증 제한 시간:** 지문의 일치 여부를 판별할 때 장치가 작업을 그만두는 시간(3초, 7초, 10초, 15초, 20초, 30초)을 설정합니다.
 - **인증 대기 시간:** 크리덴셜을 두 개 이상 사용할 때 다음 크리덴셜을 인증하는 대기 시간(3초~20초)을 설정합니다.
- **스마트 카드 레이아웃 보기**
 - **MIFARE:** 장치에서 사용하고 있는 MIFARE 레이아웃을 확인합니다. MIFARE 레이아웃의 편집 방법은 3.6.4.7을 참조하십시오.
 - **iCLASS:** 장치에서 사용하고 있는 iCLASS 레이아웃을 확인합니다. iCLASS 레이아웃의 편집 방법은 3.6.4.9을 참조하십시오.

5. 사용자 설정

- **DESFire**: 장치에서 사용하고 있는 DESFire 레이아웃을 확인합니다. DESFire 레이아웃의 편집 방법은 3.6.4.8을 참조하십시오.
- **카드 ID 포맷**
 - **포맷**: 카드 ID 데이터를 어떤 방식으로 읽어 들일 것인가를 설정합니다. **일반**을 선택하면 카드 ID 데이터를 일반적인 형식으로 처리합니다. **Wiegand**를 선택하면 위갠드 형식 설정에 따라 카드 ID 데이터를 처리합니다.
 - **Byte Order**: 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. **MSB**를 선택하면 큰 단위의 바이트에서 작은 단위의 바이트 순으로 처리합니다. **LSB**를 선택하면 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.
주의: 1.x 장치와 2.x 장치는 카드 데이터를 읽는 방식이 다르지만 BioStar에서 카드 데이터를 보정하기 때문에 동일하게 사용할 수 있습니다. 이 때문에 1.x 장치와 2.x 장치에서 동일하게 MSB/LSB를 설정해야 합니다. 장치가 표시하는 카드 ID는 헥사(Hexa)값을 기준으로 표시하기 때문에 반대로 보일 수 있으나 카드 데이터는 올바르게 읽히므로 무시해도 됩니다.
 - 이중 인증 모드에서 Admin User를 반드시 포함하는 설정 옵션을 지원합니다. 이중 인증 모드 운영 시에는 Normal User 인증 후 15초 이내에 반드시 Admin User가 인증해야 Door Relay가 켜집니다. 이 옵션을 사용하지 않는 경우 기존과 동일하게 Normal User나 Admin User 여부와 관계 없이 다른 두 사용자가 15초 이내에 인증하면 Door Relay가 켜지게 됩니다.
 - **Wiegand Card Bypass 사용**: BioStar의 Wiegand 설정에 따라 인증 성공 여부와 상관 없이 CSN을 내보내는 기능으로, BioStar 제품군 장치를 타사 ACU와 Wiegand로 연동하여 인증 여부를 판단하고 출입문 제어 기능이 없는 Dummy 장치로 사용하고자 할 때 필요한 기능입니다. 카드가 입력되면 장치에서는 별도의 인증 처리 없이 바로 Wiegand로 카드 ID를 출력하게 됩니다.

5.1.11.2 지문 탭

지문 탭에서 BioStation L2의 지문 인증 설정을 변경할 수 있습니다.

- **지문**
 - **보안 등급**: 지문을 인증할 때 사용할 보안 등급을 설정합니다(보통, 안전, 가장 안전). 보안 등급을 높일수록 본인 거부율(본인의 지문이 확실한데도 장치가 인식하지 못하는 확률)도 같이 증가합니다.

5. 사용자 설정

- **영상 품질 기준:** 지문의 품질 등급(낮음, 보통, 높음)을 설정합니다. 지문의 품질이 설정한 품질 등급보다 낮으면 시스템이 거부합니다.
- **지문 입력 시간:** 지문 입력을 끝마쳐야 하는 시간(1 초-20 초)을 설정합니다. 정해진 시간 안에 지문을 입력하지 않으면 인증이 실패하게 됩니다.
- **등록 품질 검사:** 높은 품질의 지문 정보를 저장하기 위해 스캔한 지문의 품질을 검사합니다. **사용**으로 설정하면 지문 품질이 낮을 경우 사용자에게 알려주어 지문을 올바르게 스캔하도록 도와줍니다.
- **1:N 인식 속도:** 지문의 일치 여부를 판별하는 데 걸리는 시간을 줄이려면 인식 속도(자동, 보통, 빠름, 가장 빠름)를 조절합니다. **자동**을 선택하면 장치에 등록된 총 지문 템플릿의 수에 따라 자동으로 판별 속도가 결정됩니다.
- **센서 모드:** **자동 켜짐**으로 설정하면 지문 센서가 사용자의 손가락을 인식하여 켜집니다. **항상 켜짐**으로 선택하면 센서가 항상 켜져 있습니다.
- **등록 지문 영상:** BioStation L2 의 화면에 지문을 보일 것인지 말 것인지(**보임**, **보이지 않음**)을 선택합니다.
- **위조 지문 검사:** 위조 지문 공격을 방지하기 위하여 위조 지문을 검사할지(**사용**) 검사하지 않을지(**사용 안함**) 설정합니다.
- **지문 옵션 정보:** 전체 지문 템플릿 설정을 표시합니다. 지문 템플릿에 관한 자세한 내용은 4.9 를 참조하십시오.

5.1.11.3 네트워크 탭

네트워크 탭에서 BioStation L2 의 네트워크 설정과 서버 설정을 변경할 수 있습니다.



- **TCP/IP 설정**
 - **네트워크 종류:** 랜의 종류(이더넷)를 선택합니다.
 - **포트:** 장치가 사용할 포트를 지정합니다.
- **무선랜**
 - BioStation L2 는 무선 랜을 설정할 수 없습니다.
- **IP**
 - **DHCP 사용:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용합니다.
 - **DHCP 사용 안함:** 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용하지 않습니다.
 - **IP 주소:** 장치의 IP 주소를 입력합니다.
 - **서브넷:** 장치의 서브넷 주소를 입력합니다.
 - **게이트웨이:** 네트워크의 게이트웨이를 입력합니다.
- **서버**
 - **사용:** 서버 모드(장치를 BioStar 서버에 연결)를 사용합니다.
 - **사용 안함:** 서버 모드를 사용하지 않습니다.

5. 사용자 설정

- IP 주소: BioStar 서버의 IP 주소를 입력합니다.
- 서버 포트: BioStar 가 사용하는 포트를 입력합니다.
- 서버와 자동으로 시간 동기화: 장치의 시간을 서버의 시간과 동기화합니다. 장치에서 1 시간마다 서버 시간을 폴링하여, 서버의 시간과 5 초 이상 차이가 나면, 서버의 시간과 동기화합니다.
- 시리얼 설정
 - RS485 네트워크 모드: RS485 로 연결된 장치의 모드(기본값, 호스트, 슬레이브)를 설정합니다. RS485 모드에 관한 자세한 내용은 3.2.1 과 3.2.2 를 참조하십시오.
 - RS485 속도: RS485 로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.

5.1.11.4 출입그룹 탭

출입그룹 탭에서 BioStation L2 의 기본 출입그룹을 변경할 수 있습니다.



- 기본 출입 그룹 설정: 다른 출입그룹에 포함되지 않은 새로운 사용자에게 적용할 기본 출입그룹을 선택합니다.

5.1.11.5 입력 탭

입력 탭에는 BioStation L2 에 지정된 입력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 입력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Input 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 입력 설정의 구성 방법은 3.10.3.2 를 참조하십시오.



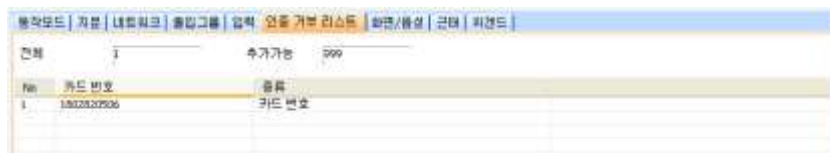
- 작업 조건
 - 장치: 조건을 추가할 장치를 선택합니다.
 - 종류: 입력 또는 이벤트를 선택할 수 있습니다.
- 입력: 작업 조건의 종류를 입력으로 선택했을 때 설정합니다.
 - 포트: 입력 0, 입력 1, 탬퍼를 선택할 수 있습니다.

5. 사용자 설정

- 스위치: 버튼을 클릭하여 입력 스위치의 보통 상태(N/O: 평상시 열림, N/C: 평상시 닫힘)를 설정합니다.
- 동작시간: 입력 신호를 감시할 일정(사용안함, 항상적용)을 설정합니다.
- 입력시간(ms): 지정한 동작을 발생시키기 위해 필요한 입력 신호의 지속 시간(1000 분의 1 초)을 입력합니다.
- 이벤트: 조건 이벤트를 선택합니다. 작업 조건의 종류를 이벤트로 선택했을 때 설정합니다.
- 동작
 - 장치: 동작을 수행할 장치를 선택합니다.
 - 종류: Output 또는 기능을 선택할 수 있습니다.
- 출력: 동작의 종류를 Output 으로 선택했을 때 설정합니다.
 - 포트: 신호를 출력할 장치의 릴레이를 선택합니다.
 - 신호 파형: 메뉴 표시줄의 옵션 > 이벤트 > Output 포트 설정에서 이미 설정한 신호 파형 중 하나를 선택합니다.
- 기능: 입력을 받았을 때 취할 동작을 선택합니다. 동작의 종류를 기능으로 선택했을 때 설정합니다.
 - 사용 안함: 입력 포트를 감시하지 않습니다.
 - 모든 경보 해제: 이 장치와 연결된 모든 경보를 해제합니다.
 - 장치 재 시작: 장치를 재시동합니다.
 - 장치 잠금: 장치가 잠깁니다. 잠긴 장치는 BioStar 서버와 통신할 수 없으며 또한 지문이나 카드 입력을 처리할 수 없습니다. 통신을 다시 연결하려면, 관리자가 BioStation L2 에서 직접 인증해야 합니다.

5.1.11.6 인증 거부 리스트 탭

인증 거부 리스트 탭에서 사용자 ID 나 카드 번호를 등록하여 사용자의 출입 시도 시 장치에서 인증되지 않도록 설정할 수 있습니다.



- 전체: 인증 거부 목록에 등록된 사용자 ID 나 카드의 총 수를 표시합니다.
- 추가가능: 등록할 수 있는 사용자 ID 나 카드의 수를 표시합니다.

참고: 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있습니다.

5.1.11.7 화면/음성 탭

화면/음성 탭에서 BioStation L2 의 화면 설정과 소리 설정을 변경할 수 있습니다. 변경한 설정을 적용하려면 반드시 탭의 아래에 있는 적용을 클릭해야 합니다. 다른장치 적용을 클릭하여 다른 장치에 같은 설정을 적용할 수 있습니다.

5. 사용자 설정



- **화면/음성 설정**
 - 언어: 화면에 표시할 언어(한글, 영문, 사용자 정의)를 선택합니다.
 - 하단정보: 부가적인 정보가 BioStation L2 의 화면 하단에 표시될 시간(무제한, 10 초, 20 초, 30 초)을 설정합니다.
 - 백라이트 타임아웃: 화면의 조명 시간을 설정합니다.
 - 테마: 화면 테마를 설정합니다.
 - 효과음 사용: 효과음 사용 여부를 설정합니다.
 - 구성 파일: BioStation L2 에서 사용할 언어 파일(변경 안함, 영어 구성 파일, 한국어 구성 파일, 사용자 정의)을 설정합니다. 영어나 한국어 이외의 언어 파일을 사용하려면, 사용자 정의를 선택한 후 줄임표(...)를 클릭한 다음, 언어 파일을 지정합니다.
 - 배경 화면: BioStation L2 에서 사용할 배경화면의 종류(로고)를 설정합니다. 지원되는 파일 종류는 JPG, GIF, BMP, PNG 이며 220×176 픽셀을 초과해서는 안됩니다. 로고에 사용되는 그림은 오직 한번에 하나의 그림만 사용할 수 있습니다.
 - 음량: BioStation L2 의 음량(0% - 100%)을 설정합니다.
 - 메시지 타임아웃: 인증 실패 메시지나 인증 성공 메시지가 표시될 시간을 설정합니다.
 - 시계 표시: 시계 표시 여부를 설정합니다.
- **배경화면 변경:** 이 체크 상자를 선택하여 새로운 배경화면을 장치에 저장할 수 있습니다. 추가를 클릭한 후 새로운 그림 파일을 지정해서 추가합니다.
- **효과음 변경:** 이 체크 상자를 선택하여 각 이벤트에 임의의 소리를 적용할 수 있습니다. 목록에 있는 이벤트를 클릭한 다음, 추가를 클릭한 후 새로운 소리 파일을 지정해서 추가합니다.

5.1.11.8 근태 탭

근태 탭에서 BioStation L2 장치의 근태 키 입력 방식을 설정할 수 있습니다. 설정을 저장하려면 장치 창의 하단에 있는 적용을 클릭해야 합니다. 다른장치 적용을 클릭하여 다른 장치에 현재 장치의 설정을 동일하게 적용할 수 있습니다.

5. 사용자 설정



- **근태 키 입력 방식:** 장치에 적용할 근태 키 입력 방식을 선택합니다.
 - **사용 안함:** 사용자가 장치에서 근태 이벤트를 기록할 수 없습니다.
 - **사용자 선택:** 사용자가 근태 이벤트를 기록하려고 할 때마다 목적에 맞는 근태 기능키를 눌러야 합니다.
 - **선택 후 유지:** 한 사용자가 특정 근태 기능키를 누를 경우 다른 근태 기능키를 누를 때까지 그 기능키가 유지됩니다.
 - **자동 설정:** 설정된 출입시간 일정에 맞게 BioStation L2 장치가 자동으로 근태 기능을 표시합니다.
 - **이벤트 고정:** BioStation L2 은 사용자가 설정한 근태 기능만 표시합니다.
- **관리:** 근태 기능에 사용할 키를 선택하고 어떤 근태 이벤트를 할당할지 설정합니다.
 - **BioStation L2 기능키:** 아래 화살표를 클릭하여 목록에서 근태 기능에 사용할 키(F1~F4, EXT01~EXT12)를 선택합니다. **이벤트 고정** 방식을 선택하였다면, 오른쪽에 있는 **고정 이벤트** 체크 상자를 선택합니다.
 - **화면 표시 문구:** BioStation L2 화면에 표시할 근태 기능에 맞는 문구를 입력합니다.
 - **자동 모드 적용 시간:** **자동 설정** 방식을 선택한 경우 아래 화살표를 클릭하여 목록에서 장치에 적용할 출입시간을 선택합니다. 선택한 시간에 맞추어 설정된 기능을 표시합니다. 출입시간을 추가하는 방법에 관해서는 3.7.1 을 참조하십시오.
 - **이벤트 종류:** 선택한 키에 할당할 이벤트의 종류(**사용 안함**, **출근**, **퇴근**, **들어옴**, **나감**)을 선택합니다. **출근** 또는 **퇴근**을 선택한 경우 **지각/조퇴 처리 안함** 체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면 사용자의 실제 출퇴근 시간에 관계없이 항상 정시에 출퇴근한 것으로 기록합니다. 근태 보고서의 결과에만 정시에 출퇴근한 것으로 기록하고 실제 근무 시간은 올바르게 계산하려면 **결과에만 적용** 체크 상자를 선택합니다. **나감**을 선택한 경우에는 **이 이벤트 이후부터 근무시간에 포함** 체크 상자를 선택할 수 있습니다. 이 옵션을 선택하면, 사용자가 근무상의 이유로 밖으로 나가는 것으로 간주하여 실제 근무 시간보다 빨리 나갔다고 하더라도 정상적으로 모든 시간을 근무한 것으로 기록합니다.

5.1.11.9 위깅드 탭

위깅드 탭에서 BioStation L2 에서 사용할 Wiegand 형식을 설정할 수 있습니다. BioStation L2 에서 위깅드 기능을 사용하려면 **Wiegand 입력**과 **Wiegand 출력**을 설정합니다. Wiegand

5. 사용자 설정

설정 마법사를 실행하려면 **포맷 변경**을 클릭합니다. 위갠드 형식에 관한 자세한 내용은 3.2.16을 참조하십시오.



- **Wiegand 모드:** 카드 ID 데이터를 읽을 때 사용할 위갠드 모드(확장모드)를 선택합니다. 확장모드를 선택하면 연결된 RF 장치가 독립된 장치로 인식됩니다. 확장모드를 이용할 경우 RF 장치는 자신의 ID 로 로그를 남길 뿐 아니라 출입문을 구성할 수 있으며 구역에 포함될 수 있습니다.
- **Wiegand 입/출력:** 위갠드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 어떻게 처리할지 선택합니다.
 - **Wiegand (카드):** 위갠드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 카드 ID 로 처리합니다.

5.1.12 BioEntry W2 설정 변경하기

5.1.12.1 동작모드 탭

동작모드 탭에서 BioEntry W2의 시간을 변경할 수 있으며 동작 모드와 관련한 다양한 설정을 변경할 수 있습니다.



- **장치 시간**
 - **날짜:** 장치에 표시할 날짜를 직접 설정합니다.

5. 사용자 설정

- 시간: 장치에 표시할 시간을 직접 설정합니다.
- 표준 시간대: 사용하려는 시간대를 선택합니다.
- 현재 PC 시간으로 동기화: BioStar 클라이언트 프로그램이 설치되어 있는 로컬 PC의 날짜와 시간을 가져와 바로 아래 날짜와 시간 스피너 상자에 표시합니다. 시간 적용을 클릭하면, 장치의 날짜와 시간이 로컬 PC의 날짜와 시간으로 설정됩니다.
- 시간 가져오기: 현재 장치에서 표시되고 있는 시간을 가져옵니다.
- 시간 적용: 장치의 시간을 설정한 시간으로 변경합니다.
- 지문 동작 모드:
 - 지문: 인증을 위해 장치가 지문만 요구하도록 설정합니다.
- 카드 동작 모드:
 - 카드: 인증을 위해 장치가 카드만 요구하도록 설정합니다.
 - 카드 + 지문: 인증을 위해 장치가 카드와 지문을 요구하도록 설정합니다.
- 기타 옵션
 - 서버 매칭: 지문이 일치하는지를 장치에서 판별하지 않고 BioStar 서버에서 판별하도록 설정합니다. 이 옵션을 선택하면, 장치는 지문의 일치 여부를 판별하기 위해 사용자 ID 나 지문 템플릿이나 카드 ID 정보를 서버에 보냅니다. 사용자의 수가 너무 많아 개별 장치에 모든 정보를 저장할 수 없거나 또는 보안상의 이유로 개별 장치에 정보를 보관할 수 없을 때 이 옵션을 사용하면 편리합니다.
 - 인증 제한 시간: 지문의 일치 여부를 판별할 때 장치가 작업을 그만두는 시간(3 초, 7 초, 10 초, 15 초, 20 초, 30 초)을 설정합니다.
 - 인증 대기 시간: 크리덴셜을 두 개 이상 사용할 때 다음 크리덴셜을 인증하는 대기 시간(3 초~20 초)을 설정합니다.
- 스마트 카드 레이아웃 보기
 - MIFARE: 장치에서 사용하고 있는 MIFARE 레이아웃을 확인합니다. MIFARE 레이아웃의 편집 방법은 3.6.4.7을 참조하십시오.
 - iCLASS: 장치에서 사용하고 있는 iCLASS 레이아웃을 확인합니다. iCLASS 레이아웃의 편집 방법은 3.6.4.9을 참조하십시오.
 - DESFire: 장치에서 사용하고 있는 DESFire 레이아웃을 확인합니다. DESFire 레이아웃의 편집 방법은 3.6.4.8을 참조하십시오.
- 카드 ID 포맷
 - 포맷: 카드 ID 데이터를 어떤 방식으로 읽어 들일 것인가를 설정합니다. 일반을 선택하면 카드 ID 데이터를 일반적인 형식으로 처리합니다. Wiegand를 선택하면 위갠드 형식 설정에 따라 카드 ID 데이터를 처리합니다.
 - Byte Order: 카드 ID 데이터를 처리할 때 어떤 순서로 바이트를 처리할지 선택합니다. MSB를 선택하면 큰 단위의 바이트에서 작은 단위의 바이트 순으로 처리합니다. LSB를 선택하면 작은 단위의 바이트에서 큰 단위의 바이트 순으로 처리합니다.

주의: 1.x 장치와 2.x 장치는 카드 데이터를 읽는 방식이 다르지만 BioStar에서 카드 데이터를 보정하기 때문에 동일하게 사용할 수 있습니다. 이 때문에 1.x 장치와 2.x 장치에서 동일하게 MSB/LSB를 설정해야 합니다. 장치가 표시하는 카드 ID는 헥사(Hexa)값을 기준으로 표시하기 때문에 반대로 보일 수 있으나 카드 데이터는 올바르게 읽히므로 무시해도 됩니다.
 - 이중 인증 모드에서 Admin User를 반드시 포함하는 설정 옵션을 지원합니다. 이중 인증 모드 운영 시에는 Normal User 인증 후 15초 이내에 반드시 Admin User가 인증해야 Door Relay가 켜집니다. 이 옵션을 사용하지 않는 경우 기존과 동일하게

5. 사용자 설정

Normal User 나 Admin User 여부와 관계 없이 다른 두 사용자가 15 초 이내에 인증하면 Door Relay 가 켜지게 됩니다.

- **Wiegand Card Bypass 사용:** BioStar 의 Wiegand 설정에 따라 인증 성공 여부와 상관 없이 CSN 을 내보내는 기능으로, BioStar 제품군 장치를 타사 ACU 와 Wiegand 로 연동하여 인증 여부를 판단하고 출입문 제어 기능이 없는 Dummy 장치로 사용하고자 할 때 필요한 기능입니다. 카드가 입력되면 장치에서는 별도의 인증 처리 없이 바로 Wiegand 로 카드 ID 를 출력하게 됩니다.

5.1.12.2 지문 탭

지문 탭에서 BioEntry W2 의 지문 인증 설정을 변경할 수 있습니다.



- **지문**
 - **보안 등급:** 지문을 인증할 때 사용할 보안 등급을 설정합니다(보통, 안전, 가장 안전). 보안 등급을 높일수록 본인 거부율(본인의 지문이 확실한데도 장치가 인식하지 못하는 확률)도 같이 증가합니다.
 - **영상 품질 기준:** 지문의 품질 등급(낮음, 보통, 높음)을 설정합니다. 지문의 품질이 설정한 품질 등급보다 낮으면 시스템이 거부합니다.
 - **지문 입력 시간:** 지문 입력을 끝마쳐야 하는 시간(1 초-20 초)을 설정합니다. 정해진 시간 안에 지문을 입력하지 않으면 인증이 실패하게 됩니다.
 - **등록 품질 검사:** 높은 품질의 지문 정보를 저장하기 위해 스캔한 지문의 품질을 검사합니다. **사용**으로 설정하면 지문 품질이 낮을 경우 사용자에게 알려주어 지문을 올바르게 스캔하도록 도와줍니다.
 - **1:N 인식 속도:** 지문의 일치 여부를 판별하는 데 걸리는 시간을 줄이려면 인식 속도(자동, 보통, 빠름, 가장 빠름)를 조절합니다. **자동**을 선택하면 장치에 등록된 총 지문 템플릿의 수에 따라 자동으로 판별 속도가 결정됩니다.
 - **센서 모드:** **자동 켜짐**으로 설정하면 지문 센서가 사용자의 손가락을 인식하여 켜집니다. **항상 켜짐**으로 선택하면 센서가 항상 켜져 있습니다.
 - **위조 지문 검사:** 위조 지문 공격을 방지하기 위하여 위조 지문을 검사할지(**사용**) 검사하지 않을지(**사용 안함**) 설정합니다.
- **지문 옵션 정보:** 전체 지문 템플릿 설정을 표시합니다. 지문 템플릿에 관한 자세한 내용은 4.9 를 참조하십시오.

5. 사용자 설정

5.1.12.3 네트워크 탭

네트워크 탭에서 BioEntry W2의 네트워크 설정과 서버 설정을 변경할 수 있습니다.



- TCP/IP 설정
 - 네트워크 종류: 랜의 종류(이더넷)를 선택합니다.
 - 포트: 장치가 사용할 포트를 지정합니다.
- IP
 - DHCP 사용: 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용합니다.
 - DHCP 사용 안함: 장치에서 동적 호스트 구성 프로토콜(DHCP)을 사용하지 않습니다.
 - IP 주소: 장치의 IP 주소를 입력합니다.
 - 서브넷: 장치의 서브넷 주소를 입력합니다.
 - 게이트웨이: 네트워크의 게이트웨이를 입력합니다.
- 서버
 - 사용: 서버 모드(장치를 BioStar 서버에 연결)를 사용합니다.
 - 사용 안함: 서버 모드를 사용하지 않습니다.
 - IP 주소: BioStar 서버의 IP 주소를 입력합니다.
 - 서버 포트: BioStar가 사용하는 포트를 입력합니다.
 - 서버와 자동으로 시간 동기화: 장치의 시간을 서버의 시간과 동기화합니다. 장치에서 1 시간마다 서버 시간을 폴링하여, 서버의 시간과 5 초 이상 차이가 나면, 서버의 시간과 동기화합니다.
- 시리얼 설정
 - RS485 네트워크 모드: RS485로 연결된 장치의 모드(기본값, 호스트, 슬레이브)를 설정합니다. RS485 모드에 관한 자세한 내용은 3.2.1과 3.2.2를 참조하십시오.
 - RS485 속도: RS485로 연결된 장치의 전송 속도(9600-115200)를 설정합니다.

5.1.12.4 출입그룹 탭

출입그룹 탭에서 BioEntry W2의 기본 출입그룹을 변경할 수 있습니다.



- 기본 출입 그룹 설정: 다른 출입그룹에 포함되지 않은 새로운 사용자에게 적용할 기본 출입그룹을 선택합니다.

5. 사용자 설정

5.1.12.5 입력 탭

입력 탭에는 BioEntry W2 에 지정된 입력 설정이 표시됩니다. 메인 창의 아래에 있는 버튼을 이용하여 입력 설정을 추가하거나, 수정하거나, 삭제할 수 있습니다. 추가하거나 수정하려면, 반드시 Input 설정 대화 상자에서 관련 옵션을 지정해야 합니다. 입력 설정의 구성 방법은 3.10.3.2 를 참조하십시오.



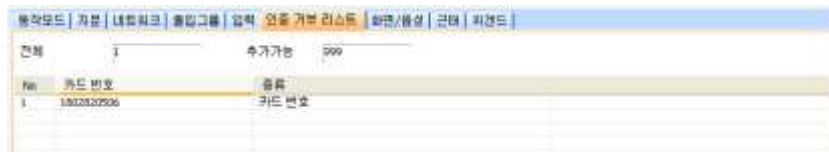
- **작업 조건**
 - **장치:** 조건을 추가할 장치를 선택합니다.
 - **종류:** 입력 또는 이벤트를 선택할 수 있습니다.
- **입력:** 작업 조건의 종류를 입력으로 선택했을 때 설정합니다.
 - **포트:** 입력 0, 입력 1, 탭퍼를 선택할 수 있습니다.
 - **스위치:** 버튼을 클릭하여 입력 스위치의 보통 상태(N/O: 평상시 열림, N/C: 평상시 닫힘)를 설정합니다.
 - **동작시간:** 입력 신호를 감시할 일정(사용안함, 항상적용)을 설정합니다.
 - **입력시간(ms):** 지정한 동작을 발생시키기 위해 필요한 입력 신호의 지속 시간(1000 분의 1 초)을 입력합니다.
- **이벤트:** 조건 이벤트를 선택합니다. 작업 조건의 종류를 이벤트로 선택했을 때 설정합니다.
- **동작**
 - **장치:** 동작을 수행할 장치를 선택합니다.
 - **종류:** Output 또는 기능을 선택할 수 있습니다.
- **출력:** 동작의 종류를 Output 으로 선택했을 때 설정합니다.
 - **포트:** 신호를 출력할 장치의 릴레이를 선택합니다.
 - **신호 파형:** 메뉴 표시줄의 옵션 > 이벤트 > Output 포트 설정에서 이미 설정한 신호 파형 중 하나를 선택합니다.
- **기능:** 입력을 받았을 때 취할 동작을 선택합니다. 동작의 종류를 기능으로 선택했을 때 설정합니다.
 - **사용 안함:** 입력 포트를 감시하지 않습니다.
 - **모든 경보 해제:** 이 장치와 연결된 모든 경보를 해제합니다.
 - **장치 재 시작:** 장치를 재시동합니다.

5. 사용자 설정

- **장치 잠금:** 장치가 잠깁니다. 잠긴 장치는 BioStar 서버와 통신할 수 없으며 또한 지문이나 카드 입력을 처리할 수 없습니다. 통신을 다시 연결하려면, 관리자가 BioEntry W2 에서 직접 인증해야 합니다.

5.1.12.6 인증 거부 리스트 탭

인증 거부 리스트 탭에서 사용자 ID 나 카드 번호를 등록하여 사용자의 출입 시도 시 장치에서 인증되지 않도록 설정할 수 있습니다.



- **전체:** 인증 거부 목록에 등록된 사용자 ID 나 카드의 총 수를 표시합니다.
- **추가가능:** 등록할 수 있는 사용자 ID 나 카드의 수를 표시합니다.

참고: 장치의 카드 모드가 '템플릿 온 카드'로 설정되어 있을 때에만, 인증 거부 기능을 사용할 수 있습니다.

5.1.12.7 화면/음성 탭

화면/음성 탭에서 BioEntry W2 에서 발생하는 이벤트나 상태에 따라 LED 와 Buzzer 를 설정하여 작동상태를 표시할 수 있습니다. 설정한 후 이벤트 별로 저장 버튼을 클릭해야 저장이 됩니다.



- **이벤트:** 설정을 적용할 이벤트를 선택합니다.
- **LED:** 선택한 이벤트 발생 시 LED 의 행동 패턴을 설정합니다.
 - **횟수:** 선택한 이벤트 발생 시 LED 의 반복 사이클을 설정합니다. 0 을 입력하면 무한 반복되며 -1 을 입력하면 LED 가 작동하지 않습니다.
 - **색상:** 최대 3 개의 LED 색상을 선택합니다. 위에서 아래 순서대로 LED 의 색상이 바뀌면서 반복됩니다. 숫자 필드에는 각 색상이 지속되는 시간을 밀리초 단위로 입력합니다.

5. 사용자 설정

- **Buzzer:** 선택한 이벤트 발생 시 경고음의 패턴을 설정합니다.
 - **횟수:** 경고음의 반복 횟수를 설정합니다. 0 을 입력하면 계속 경고음이 발생하며 -1 을 입력하면 경고음이 발생하지 않습니다.
 - **음량:** 경고음의 크기(Low /Middle /High)를 설정합니다. 위에서 아래의 순서로 선택한 음량 크기대로 경고음이 반복됩니다. 숫자 필드에는 각 경고음이 지속되는 시간을 밀리초 단위로 입력합니다.
 - **페이드아웃:** 경고음의 소리가 점차 작아집니다.

5.1.12.8 근태 탭

근태 탭에서 BioEntry W2 장치의 근태 입력 방식을 설정할 수 있습니다. 설정을 저장하려면 장치 창의 하단에 있는 **적용**을 클릭해야 합니다. **다른장치 적용**을 클릭하여 다른 장치에 현재 장치의 설정을 동일하게 적용할 수 있습니다.



- **근태 모드 선택:** 장치에 적용할 근태 입력 방식을 선택합니다.
 - **사용 안함:** 사용자가 장치에서 근태 이벤트를 기록할 수 없습니다.
 - **출근 고정:** 근태 이벤트로 출근만 기록합니다.
 - **퇴근 고정:** 근태 이벤트로 퇴근만 기록합니다.
 - **자동 설정:** 설정된 출입시간 일정에 맞게 BioEntry W2 장치가 자동으로 근태 모드를 변경합니다.
- **출근 고정 시간:** 자동 설정 방식을 선택한 경우 목록에서 장치에 적용할 출근 시간을 선택합니다. 출입시간을 추가하는 방법에 관해서는 3.7.1 을 참조하십시오.
- **퇴근 고정 시간:** 자동 설정을 선택한 경우 목록에서 장치에 적용할 퇴근 시간을 선택합니다. 출입시간을 추가하는 방법에 관해서는 3.7.1 을 참조하십시오.
- **출근 이벤트 표시 문구:** 출근 이벤트로 기록할 문구를 입력합니다.
- **퇴근 이벤트 표시 문구:** 퇴근 이벤트로 기록할 문구를 입력합니다.

5.1.12.9 위깅드 탭

위깅드 탭에서 BioEntry W2 에서 사용할 Wiegand 형식을 설정할 수 있습니다. BioEntry W2 에서 위깅드 기능을 사용하려면 **Wiegand 입력**과 **Wiegand 출력**을 설정합니다.

5. 사용자 설정

Wiegand 설정 마법사를 실행하려면 **포맷 변경**을 클릭합니다. 위갠드 형식에 관한 자세한 내용은 3.2.16을 참조하십시오.



- **Wiegand 모드:** 카드 ID 데이터를 읽을 때 사용할 위갠드 모드(**확장모드**)를 선택합니다. 확장모드를 선택하면 연결된 RF 장치가 독립된 장치로 인식됩니다. 확장모드를 이용할 경우 RF 장치는 자신의 ID 로 로그를 남길 뿐 아니라 출입문을 구성할 수 있으며 구역에 포함될 수 있습니다.
- **Wiegand 입/출력:** 위갠드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 어떻게 처리할지 선택합니다.
 - **Wiegand (카드):** 위갠드 입/출력을 통해 내보내는 신호와 들어오는 ID 데이터를 카드 ID 로 처리합니다.

5.2 출입문 설정 변경하기

이 절에서는 BioStar 시스템에 추가된 출입문을 설정하는 방법에 관해서 설명합니다. 이러한 설정을 변경하여 현재 처해있는 상황이나 운영상의 필요에 맞게 출입문의 기능을 변경할 수 있습니다. 아래에서 설명하는 탭을 화면에 띄우려면 단축 메뉴 창의 **출입문**을 클릭한 후 출입문의 이름을 클릭해야 합니다.

주의: 2.x 장치(BioStation A2, BioStation 2, BioStation L2, BioEntry W2)는 1.x 장치(BioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, Xpass S2, X-Station, BioStation T2, FaceStation)와 함께 출입문을 구성할 수 없습니다.

5.2.1 추가정보 탭

추가정보 탭에서 출입문의 내부와 내부에 어떤 장치가 설치되어 있는지, 장치가 출입문을 어떻게 제어할 것인지, anti-passback 기능을 어떻게 적용할 것인지 설정할 수 있습니다. 하나의 출입문에 2 개의 장치를 연결할 때에는 반드시 RS485 를 이용하여 두 장치를 연결해야 합니다. 이러한 경우에는 오직 한 장치의 I/O 포트만 사용할 수 있습니다. IO 장치 목록 상자에서 어떤 장치의 I/O 포트를 사용할지 설정하십시오.

5. 사용자 설정

- **안쪽 장치:** 출입문의 안쪽에 설치된 장치를 선택합니다.
- **바깥쪽 장치:** 출입문의 바깥쪽에 설치된 장치를 선택합니다.
- **개방 시간:** 출입문이 일반적인 상태에서 열린 채로 유지되는 시간을 선택합니다. 이 시간 동안에는 출입문의 릴레이가 활성화됩니다.
- **폐쇄 시간:** 출입문이 일반적인 상태에서 닫힌 채로 유지되는 시간을 선택합니다. 이 시간 동안에는 출입문의 릴레이가 비활성화됩니다.
- **IO 장치:** 하나의 출입문에 2 개의 장치를 사용할 때 어느 장치의 IO 포트를 사용할지 지정합니다.
- **문열림 릴레이:** 출입문 릴레이를 선택합니다.
- **문열림 버튼:** 문열림 버튼에 사용할 입력(**사용 안함**, **입력 0**, **입력 1**)을 선택합니다.
- **(스위치 종류):** 버튼을 클릭하여 문열림 버튼에 사용되는 입력의 보통 상태(**N/O**: 평상시 열림, **N/C**: 평상시 닫힘)를 설정합니다.
- **문열림 상태:** 출입문의 현재 상태를 감지하는 센서에 사용할 입력을 선택합니다.
- **(스위치 종류):** 출입문의 상태를 감지하는 센서에 사용되는 입력의 보통 상태(**N/O**: 평상시 열림, **N/C**: 평상시 닫힘)를 설정합니다.
- **문 열림 시간(초):** 문이 열렸을 때 릴레이가 활성화되는 시간(초 단위)을 입력합니다. 이 시간이 지나면, 릴레이는 더 이상 출입문에 신호를 보내지 않습니다. 기본값은 3 초입니다.
- **장시간 문 열림(초):** 알람이 울리기 전까지 출입문이 열린 채로 남아있어도 되는 시간을 입력합니다.
- **문열림 이벤트:** 어떤 이벤트에 의해 출입문을 열지 선택합니다.
 - **모든 이벤트 (기본값):** 이벤트 종류에 관계 없이 이벤트가 발생하면 문을 엽니다.
 - **근태+인증 이벤트:** 일반 인증이나 근태 이벤트 발생 시 문을 엽니다. 이 옵션을 사용하려면 근태 탭에서 **문열림** 체크 상자를 선택해야 합니다. 이 옵션은 BioStation, BioLite Net, X-Station, BioStation T2, FaceStation, BioStation 2, BioStation A2, BioStation L2 장치에서만 사용할 수 있습니다. 근태 설정을 변경하는 방법에 관한 자세한 내용은 5.1.1.9 와 5.1.3.9 와 5.1.6.10 과 5.1.7.11 와 5.1.8.10 과 5.1.9.9 와 5.1.10.9 와 5.1.11.8 을 참조하십시오.
 - **인증 이벤트:** 일반 인증 이벤트 발생 시 문을 엽니다.
 - **근태 이벤트:** 근태 이벤트 발생 시 문을 엽니다. 이 옵션을 사용하려면 근태 탭에서 문열림 체크 상자를 선택해야 합니다. 이 옵션은 BioStation, BioLite Net, X-Station, BioStation T2, FaceStation, BioStation 2, BioStation A2, BioStation L2 장치에서만 사용할 수 있습니다. 근태 설정을 변경하는 방법에 관한 자세한 내용은 5.1.1.9 와 5.1.3.9 와 5.1.6.10 과 5.1.7.11 와 5.1.8.10 과 5.1.9.9 와 5.1.10.9 와 5.1.11.8 을 참조하십시오.
 - **사용 안함:** 이벤트 발생과 관계없이 문을 열지 않습니다.
- **문 잠금 조건:** 문을 닫는 조건을 선택합니다.
 - **Open period:** **문 열림 시간(초)**에서 입력된 시간이 지나면 문을 닫습니다.
 - **Open period+Status:** 문이 열린 것을 감지하면(문에 센서가 연결되어 있으며 BioStar 시스템이 이를 감지하면) 문을 닫습니다. 문에 센서가 연결되어 있지 않거나 BioStar 시스템이 문이 열린 것을 감지하지 못하더라도, **문 열림 시간(초)**에서 입력된 시간이 지나면 문을 닫습니다. 회전문과 같은 경우, 인증을 거치지 않고 뒷사람이 따라 들어오는 것을 방지하려 할 때 이 기능을 유용하게 사용할 수 있습니다.
- **Anti-passback:** anti-passback 기능을 활성화하려면 체크 상자를 선택합니다(출입문의 안쪽과 바깥쪽 모두에 장치가 설치되어 있는 경우에만 사용할 수 있습니다).
 - **장치 이름:** 장치 이름은 자동적으로 입력됩니다.

5. 사용자 설정

- 장치 IP: 장치 IP는 자동적으로 입력됩니다.
- AP 종류: 사용할 anti-passback 기능의 종류(Soft 또는 Hard)를 선택합니다.
- 초기화 시간(분): anti-passback 기능이 초기화되기까지 걸리는 시간(분 단위)을 입력합니다. 초기화 시간을 0으로 설정하면 anti-passback 기능이 초기화되지 않습니다.
- 개방 트리거 옵션
 - 개방 트리거 옵션: 출입문의 상세 탭에서 개방 시간 옵션을 지원합니다. 개방시간이 설정된 경우에 해당 시간이 되어도 출입문 개폐장치가 열리지 않고 옵션에 따라 관리자나 일반사용자가 인증해야만 개폐장치를 열 수 있는 기능입니다. 스케줄에 의해 출입문이 열릴 때 트리거 옵션이 켜져 있으면 해당 등급 사용자의 인증이 있어야 출입문이 열립니다. 설정 옵션은 정규 펌웨어 지원 제품에 대해서만 사용 안함, 일반, 관리자 항목으로 지원됩니다.

주의: 지원 펌웨어 버전: BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다. 2.x 장치(BioStation 2, BioStation A2, BioStation L2, BioEntry W2)는 지원되지 않습니다.

주의: 개방 시간옵션은 출입문을 슬레이브 단말기 또는 RF 3rd Party 단말기와 함께 2개의 리더로 구성된 경우에는 동작하지 않으며, 1개의 슈프리마 단말기로 출입문을 구성한 경우에만 지원됩니다. 그 외의 경우에는 지원되지 않으며, RF 3rd Party 단말기만으로 출입문을 구성한 경우에도 지원되지 않습니다.
 - 입력 지연 설정
 - 입력 지연 설정: 출입문의 상세 탭에서 입력 지연 설정을 지원합니다. 이 옵션을 켜면 단말기에 입력되는 신호에 대해 펌웨어에 지정한 일정 시간 동안 유지되는 경우에 한해서 정상적인 입력으로 처리하는 기능입니다. 설정 옵션은 정규 펌웨어 지원 제품에 대해서 사용, 사용 안함 항목으로 지원됩니다.

주의: 지원 펌웨어 버전: BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3 이상 지원됩니다.

5.2.2 알람 탭

알람 탭에서는 강제로 열리거나 열린 채로 남아 있는 출입문에 대해 어떠한 경보 동작을 취할지 설정할 수 있습니다. 강제 열림 경보는 장치를 통해 인증을 거치지 않고 강제로 출입문이 열리면 발동합니다. 열림 방지 경보는 출입문이 시스템 설정에서 지정된 시간보다 더 오랫동안 열려있으면 작동합니다.

그림 5.20

5. 사용자 설정

- 동작
 - **PC 사운드:** 체크 상자를 선택하고 BioStar 프로그램이 내보낼 소리를 선택합니다. 재생 횟수를 입력하면, 그 횟수만큼 소리를 내보내게 됩니다. 0 을 입력하면, 관리자가 실시간 이벤트 감시화면에서 Sound 아이콘을 클릭하여 멈출 때까지 재생됩니다. 임의의 소리를 추가하는 방법에 관해서는 3.10.1.2 를 참조하십시오.
 - **장치 사운드:** 출입문에 설치된 장치가 내보낼 소리를 선택합니다.
 - **Email 전송:** 시스템이 발송할 메일을 설정합니다. 메일 통지에 관한 자세한 내용은 3.10.2 를 참조하십시오.
 - **Output 장치:** 경보 신호를 내보낼 장치를 선택합니다.
 - **Output 포트:** 경보 신호를 내보낼 때 사용할 포트를 선택합니다.
 - **Output 신호파형:** 신호파형을 선택합니다.

5.3 구역 설정 변경하기

필요에 따라 구역 기능을 변경할 수 있습니다. 구역 설정을 변경하려면, 메뉴 창에서 **출입문**을 클릭한 후 구역의 이름을 클릭합니다.

주의: 2.x 장치(BioStation A2, BioStation 2, BioStation L2, BioEntry W2)는 1.x 장치(BioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, Xpass S2, X-Station, BioStation T2, FaceStation)와 함께 구역을 구성할 수 없습니다. 또한, BioStation A2, BioStation 2, BioStation L2, BioEntry W2 는 이중출입 장치 구역, 화재 경보 구역으로만 구성할 수 있습니다.

5.3.1 이중출입 방지 구역 설정하기

이 절에서는 이중출입 방지 구역에서 사용할 수 있는 설정에 대해서 설명합니다. 필요에 따라 이중출입 방지 구역의 기능을 변경할 수 있습니다.

5.3.1.1 추가정보 탭

상세정보 탭에서 anti-passback 기능의 종류를 선택할 수 있으며 anti-passback 기능이 초기화되는 시간을 설정할 수 있습니다.

5. 사용자 설정

No	장치	속성
1	40051[61.83.152.174]	입실용 마스터 장치

그림 5.21

- **AP 종류:** 사용할 anti-passback 기능의 종류(**Soft, Hard**)을 선택합니다.
- **초기화 시간(분):** anti-passback 기능이 초기화되기까지 걸리는 시간(분 단위)을 입력합니다. 초기화 시간을 "0"으로 설정하면 anti-passback 기능이 초기화되지 않습니다.
- **통신 장애시 문열림 옵션:** 마스터 장치와 통신이 끊어진 상황에서 사용자가 인증을 성공한 경우 출입 허용 여부를 설정합니다.

5.3.1.2 알람 탭

알람 탭에서 이중출입 방지 구역에 적용할 알람 동작과 출력 장치를 선택할 수 있습니다.

그림 5.22

- **동작**
 - **PC 사운드:** 체크 상자를 선택하고 BioStar 프로그램이 내보낼 소리를 선택합니다. 재생 횟수를 입력하면, 그 횟수만큼 소리를 내보내게 됩니다. 0은 관리자가 실시간 이벤트 감시화면에서 Sound 아이콘을 클릭하여 멈출 때까지 재생됩니다.) 소리 파일의 추가 방법은 3.10.1.2 를 참조하십시오.
 - **장치 사운드:** 출입문에 설치된 장치가 내보낼 소리를 선택합니다.
 - **Email 전송:** 시스템이 발송할 메일을 설정합니다. 메일 통지에 관한 자세한 내용은 3.10.2 를 참조하십시오.
 - **Output 장치:** 경보 신호를 내보낼 장치를 선택합니다.
 - **Output 포트:** 경보 신호를 내보낼 때 사용할 포트를 선택합니다.

5. 사용자 설정

- Output 신호파형: 신호파형을 선택합니다.

5.3.1.3 출입통제그룹 탭

출입통제그룹에서 이 구역에 설정된 일반적인 출입 제한을 무시할 수 있는 출입그룹을 선택할 수 있습니다. 이러한 우회 권한을 출입그룹에 부여하려면, 그룹을 선택한 후 구역 창의 아래에 있는 적용을 클릭합니다.

C	Access Group
<input type="checkbox"/>	전체제한
<input type="checkbox"/>	전체출입
<input type="checkbox"/>	사원
<input type="checkbox"/>	이사

그림 5.23

5.3.2 인증 제한 구역 설정하기

이 절에서는 인증 제한 구역에서 사용할 수 있는 설정에 대해서 설명합니다. 필요에 따라 인증 제한 구역의 기능을 변경할 수 있습니다.

5.3.2.1 추가정보 탭

추가정보 탭에서 인증 제한 시간과 인증 허용 횟수를 설정할 수 있습니다.

No	장치	속성
1	40051[61.83.152.174]	마스터 장치

그림 5.24

- **인증제한 구역 옵션:** 인증 제한 설정을 적용하려면 체크 상자를 선택한 후 이 설정을 적용할 시간을 입력합니다.
- **최대 인증 허용 횟수:** 지정된 인증 제한 시간 안에 허용할 최대 입장 수를 설정합니다.
- **분 이내 다시 인증하는 경우 거부 (0 일 때 사용 안함):** 인증 제한 구역에 다시 입장하기 위해 필요한 시간을 입력합니다.

5. 사용자 설정

- **통신 장애시 문열림 옵션:** 마스터 장치와 통신이 끊어진 상황에서 사용자가 인증을 성공한 경우 출입 허용 여부를 설정합니다.

5.3.2.2 알람 탭

알람 탭에서 인증 제한 구역에 적용할 알람 동작과 출력 장치를 선택할 수 있습니다.

그림 5.25

- **동작**
 - **PC 사운드:** BioStar 프로그램이 사용할 소리를 선택합니다. 재생 횟수를 입력하면, 그 횟수만큼 소리를 내보내게 됩니다. 0 은 관리자가 실시간 이벤트 감시화면에서 Sound 아이콘을 클릭하여 멈출 때까지 재생됩니다.)소리 파일의 추가 방법은 3.10.1.2 를 참조하십시오.
 - **장치 사운드:** 출입문에 설치된 장치가 내보낼 소리를 선택합니다.
 - **Email 전송:** 메일 통지에 사용할 메일을 지정합니다. 메일 통지에 관한 자세한 내용은 3.10.2 를 참조하십시오.
 - **Output 장치:** 경보 신호를 내보낼 장치를 선택합니다.
 - **Output 포트:** 경보 신호를 내보낼 때 사용할 포트를 선택합니다.
 - **Output 신호파형:** 신호파형을 선택합니다.

5.3.2.3 출입통제그룹 탭

출입통제그룹에서 이 구역에 설정된 일반적인 출입 제한을 무시할 수 있는 출입그룹을 선택할 수 있습니다. 이러한 우회 권한을 출입그룹에 부여하려면, 그룹을 선택한 후 구역 창의 아래에 있는 **적용**을 클릭합니다.

C	Access Group
<input type="checkbox"/>	전체제한
<input type="checkbox"/>	전체출입
<input type="checkbox"/>	사원
<input type="checkbox"/>	이사

그림 5.26

5.3.3 경보 구역 설정하기

이 절에서는 경보 구역에서 사용할 수 있는 설정에 대해서 설명합니다.

주의: BioStation A2, BioStation 2, BioStation L2, BioEntry W2 로 구성된 출입문/구역은 경비 개시와 경비 해제를 설정할 수 없습니다.

5. 사용자 설정

5.3.3.1 추가정보 탭

알람 탭에서 경비 개시와 경비 해제를 설정할 수 있습니다.

The screenshot shows the '추가정보' (Additional Information) tab. At the top, there are tabs for '추가정보', '알람', '출입통제그림', and '이벤트'. Below the tabs, there are input fields for '지연시간(초)' (Delay Time) with a dropdown for '경비' (Guard) and '해제' (Release). There are buttons for '설정' (Set) for '경비 개시/해제 종류' (Guard Start/Release Type) and '외부 I/O 연동' (External I/O Interlocking). Below these are two tables: '장치 목록' (Device List) and 'Input 목록' (Input List).

No	장치	속성	경비 개시/해제 방식
1	40051[61.83.152.174]	마스터 장치	

No	이름	장치	입력	스위치	입력시간(ms)

그림 5.27

- **지연시간(초)**
 - **경비 개시:** 경비를 개시하기 전의 지연 시간(초 단위)을 입력합니다.
 - **경비 해제:** 경비를 해제하기 전의 지연 시간(초 단위)을 입력합니다.
- **경비 개시/해제 종류:** 경비를 개시하거나 해제하기 위한 설정을 지정합니다. 경비 개시 및 경비 해제를 설정하는 방법에 관한 자세한 내용은 3.5.2.5, 경보를 설정하는 방법에 관한 자세한 내용은 3.10 을 참조하십시오.
- **외부 I/O 연동:** BioStar 시스템이 자동으로 경비 구역 및 경비 해제 구역을 설정할 수 있도록 지정하려면 선택합니다. 외부 입력/출력을 설정하는 방법에 관한 자세한 내용은 3.5.2.6 을 참조하십시오. 경보를 설정하는 방법에 관한 자세한 내용은 3.10 을 참조하십시오.

5.3.3.2 알람 탭

알람 탭에서 경보 구역에 적용할 알람 동작과 출력 장치를 선택할 수 있습니다.

The screenshot shows the '알람' (Alarm) tab. It features a '동작' (Action) section with checkboxes for 'PC 사운드' (checked), '장치 사운드' (checked), and 'Email 전송' (checked). There are dropdown menus for 'chimes.wav', '40051[61.83.152.174]', and '-'. A '재생 횟수' (Repeat Count) field is set to '0 (0 : 반복)'. The 'Output 장치' (Output Device) section has a checked checkbox and a dropdown for '40051[61.83.152.174]'. The 'Output 포트' (Output Port) dropdown is set to '[40051]릴레이 0'. The 'Output 신호파형' (Output Signal Waveform) dropdown is set to 'Signal1'.

그림 5.28

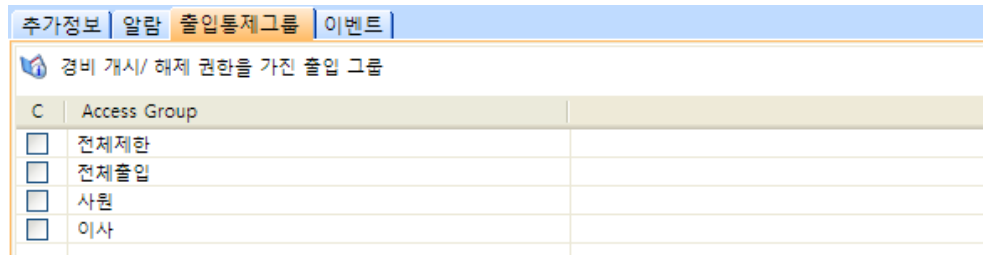
- **동작**

5. 사용자 설정

- **PC 사운드:** BioStar 프로그램이 사용할 소리를 선택합니다. 재생 횟수를 입력하면, 그 횟수만큼 소리를 내보내게 됩니다. 0 은 관리자가 실시간 이벤트 감시화면에서 Sound 아이콘을 클릭하여 멈출 때까지 재생됩니다. 소리 파일의 추가 방법은 3.10.1.2 를 참조하십시오.
- **장치 사운드:** 출입문에 설치된 장치가 내보낼 소리를 선택합니다.
- **Email 전송:** 메일 통지에 사용할 메일을 지정합니다. 메일 통지에 관한 자세한 내용은 3.10.2 를 참조하십시오.
- **Output 장치:** 체크 상자를 선택하고 경보 신호를 내보낼 장치를 선택합니다.
- **Output 포트:** 경보 신호를 내보낼 때 사용할 포트를 선택합니다.
- **Output 신호파형:** 신호파형을 선택합니다.

5.3.3.3 출입통제그룹

경보 구역의 출입통제그룹 탭에서는 경비를 개시하거나 멈출 수 있는 출입그룹을 설정할 수 있습니다. 이러한 권한을 출입그룹에 부여하려면, 그룹을 선택한 후 구역 창의 아래에 있는 **적용**을 클릭합니다.



C	Access Group
<input type="checkbox"/>	전체제한
<input type="checkbox"/>	전체출입
<input type="checkbox"/>	사원
<input type="checkbox"/>	이사

그림 5.29

5.3.4 화재 경보 구역 설정하기

이 절에서는 화재 경보 구역에서 사용할 수 있는 설정에 대해서 설명합니다. 필요에 따라 화재 경보 구역의 기능을 변경할 수 있습니다.

5.3.4.1 추가정보 탭

추가정보 탭에서 장치 목록에 장치를 추가하거나 삭제할 수 있으며, 입력 목록에 입력을 추가하거나 삭제할 수 있습니다. 장치를 추가하거나 삭제하려면 3.5.2.2 를 참조하십시오.

5. 사용자 설정

The screenshot shows two tables in a software interface. The top table, titled '장치 목록' (Device List), has columns for 'No', '장치' (Device), and '속성' (Property). It contains one entry with 'No' 1, '장치' 40051[61.83.152.174], and '속성' 마스터 장치 (Master Device). The bottom table, titled 'Input 목록' (Input List), has columns for 'No', '이름' (Name), '장치' (Device), '입력' (Input), '스위치' (Switch), and '입력시간(ms)' (Input Time (ms)). It is currently empty.

그림 5.30

5.3.4.2 알람 탭

알람 탭에서 화재 경보 구역에 적용할 알람 동작과 출력 장치를 선택할 수 있습니다. 화재 경보의 설정 방법은 3.10.1 을 참조하십시오.

The screenshot shows the '동작' (Action) configuration section. It includes several settings:

- PC 사운드: chimes.wav (재생 횟수: 0 (0 : 반복))
- 장치 사운드: 40051[61.83.152.174]
- Email 전송: ...
- Output 장치: 40051[61.83.152.174]
- Output 포트: [40051]터레이 0
- Output 신호파형: Signal1

그림 5.31

- **동작**
 - **PC 사운드:** BioStar 프로그램이 사용할 소리를 선택합니다. 재생 횟수를 입력하면, 그 횟수만큼 소리를 내보내게 됩니다. 0 을 선택하면 관리자가 실시간 이벤트 감시화면에서 Sound 아이콘을 클릭하여 멈출 때까지 재생됩니다. 소리 파일의 추가 방법은 3.10.1.2 를 참조하십시오.
 - **장치 사운드:** 출입문에 설치된 장치가 내보낼 소리를 선택합니다.
 - **Email 전송:** 메일 통지에 사용할 메일을 지정합니다. 메일 통지에 관한 자세한 내용은 3.10.2 를 참조하십시오.
 - **Output 장치:** 경보 신호를 내보낼 장치를 선택합니다.
 - **Output 포트:** 경보 신호를 내보낼 때 사용할 포트를 선택합니다.
 - **Output 신호파형:** 신호파형을 선택합니다.

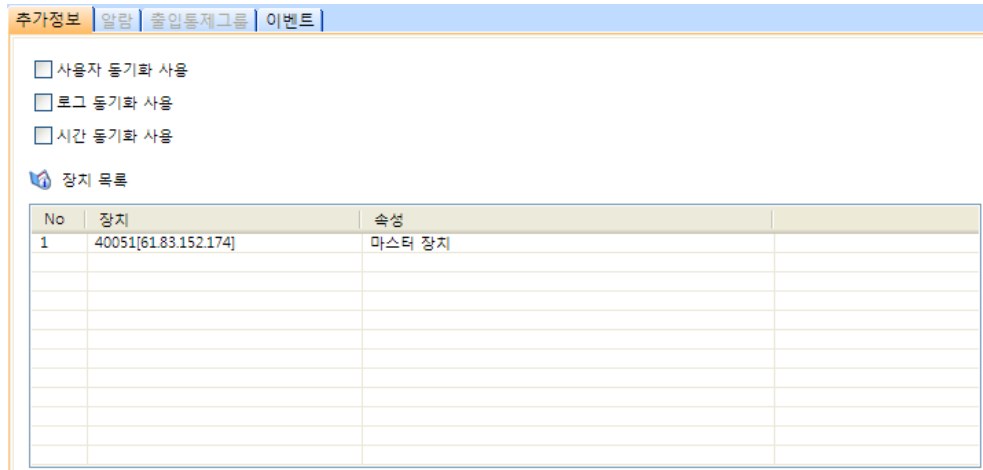
5. 사용자 설정

5.3.5 출입 구역 설정하기

이 절에서는 출입 구역에서 사용할 수 있는 설정에 대해서 설명합니다. 이 구역은 사용자 데이터를 동기화하기 위해 사용됩니다. 그렇기 때문에 알람 탭과 출입통제그룹 탭은 사용할 수 없습니다. 필요에 따라 출입 구역의 기능을 변경할 수 있습니다.

5.3.5.1 추가정보 탭

추가정보 탭에서 장치 목록에 장치를 추가할 수 있습니다.



No	장치	속성
1	40051[61.83.152.174]	마스터 장치

- **사용자 동기화 사용:** 사용자 정보를 자동으로 다른 장치에 전송합니다.
- **로그 동기화 사용:** (구역 안에 있는 다른 장치를 대신하여) 마스터 장치에 모든 로그를 자동으로 저장합니다.
- **시간 동기화 사용:** 구역 안에 있는 장치의 시간을 동기화합니다.

5.3.6 소집 구역 설정하기

이 절에서는 소집 구역에서 사용할 수 있는 설정에 대해서 설명합니다. 필요에 따라 소집 구역의 기능을 변경할 수 있습니다.

5. 사용자 설정

5.3.6.1 추가정보 탭

추가정보 탭에서 장치 목록에 장치를 추가할 수 있습니다.

추가정보 | 알람 | 출입통제그룹 | 이벤트

소집 구역 종류: 수동

추적 시간 (시): 2

장치 목록

No	장치	속성

그림 5.32

- **소집 구역 종류:** 모니터링의 종류를 나타냅니다. 기본값은 '수동'으로 설정되어 있으며, 소집 구역에 모인 사용자들의 출석 상황을 수동으로 확인할 수 있습니다. 소집 구역의 출석 상황표를 확인하는 방법은 4.1.1 을 참조하십시오.
- **추적 시간(시):** 몇 시간 전부터 사용자의 위치를 추적할지 설정합니다. 예를 들어, 8 시간으로 설정한다면 소집 구역의 출석 상황표를 확인하는 시점을 기준으로 8시간이전까지의 출입 기록을 볼 수 있습니다.

5.3.6.2 출입통제그룹 탭

출입통제그룹 탭에서 소집 구역에 해당하는 출입 그룹을 지정합니다.

추가정보 | 알람 | 출입통제그룹 | 이벤트

소집 구역에 소속 될 출입그룹

c	출입그룹
<input type="checkbox"/>	사원
<input type="checkbox"/>	전체제한
<input checked="" type="checkbox"/>	전체출입

그림 5.33

5. 사용자 설정

5.3.7 Interlock 구역 설정하기

이 절에서는 Interlock 구역에서 사용할 수 있는 설정에 대해서 설명합니다. 필요에 따라 Interlock 구역의 기능을 변경할 수 있습니다.

Interlock 구역은 아래 표기된 펌웨어가 설치된 장치들로 구성되어 있을 때만 동작합니다.

- FaceStation V1.3 이상, BioStation T2 V1.3 이상, BioStation V1.9 이상, BioEntry Plus V1.5 이상, BioEntry W V1.0 이상, BioLite Net V1.3 이상, Xpass V1.2 이상, X-Station V1.3 이상.
- D-Station, BioStation 2, BioStation A2, BioStation L2, BioEntry W2 에서는 지원되지 않습니다.

5.3.7.1 추가정보 탭

추가정보 탭에서 Interlock 구역의 양쪽 출입구에 사용할 출입문을 지정할 수 있습니다. 출입문 1, 출입문 2 를 지정하면 아래 장치 목록에 각 출입문에 연결되어 있는 장치목록이 순차적으로 나타납니다.

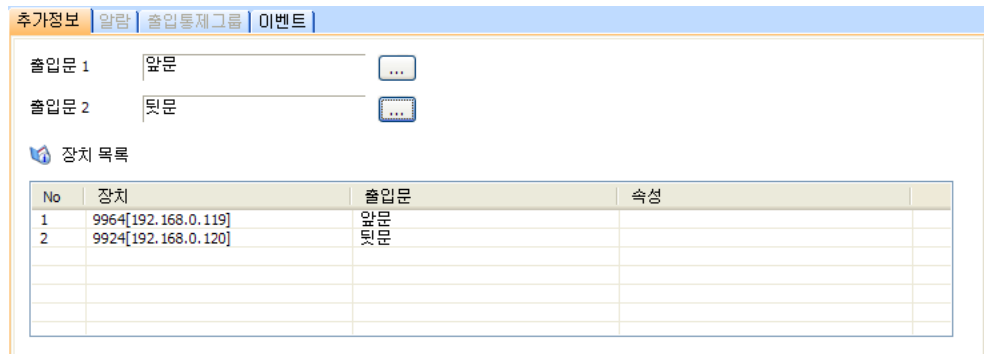


그림 5.34

- **출입문 1:** Interlock 구역의 첫 번째 출입문을 선택하려면 출입표(...) 버튼을 클릭합니다. 장치가 연결되지 않은 출입문은 Interlock 구역에 추가할 수 없습니다.
- **출입문 2:** Interlock 구역의 두 번째 출입문을 선택하려면 출입표(...) 버튼을 클릭합니다. 장치가 연결되지 않은 출입문은 Interlock 구역에 추가할 수 없습니다.

5.4 사용자 설정 변경하기

개인 추가 정보, 지문 정보, 출입 카드 정보를 포함하여 사용자와 관련된 설정을 변경할 수 있습니다. 아래에서 설명하는 탭을 화면에 띄우려면 단축 메뉴 창의 **사용자**를 클릭한 후 사용자의 이름을 클릭해야 합니다.

5. 사용자 설정

5.4.1 추가정보 탭

추가정보 탭에서는 사용자에게 관한 개인 정보를 수정하거나 사용자 계정의 유효 날짜를 변경할 수 있습니다. 이 영역을 편집하려면 4.5.3 을 참조하십시오.

추가정보	
ID	<input type="text" value="1"/>
시작일	2000-01-01
만료일시	2030-12-31 23 시
개인별 인증 모드	장치설정을 따름
직급	부장
핸드폰번호	010-1111-1111
성별	남자
생일	1980-09-14

그림 5.35

- ID: 사용자에게 부여할 식별 번호를 입력합니다.
- 시작일: BioStar 시스템으로부터 인증을 받을 수 있는 시작 날짜를 선택합니다.
- 만료일시: 사용자 계정이 만료되는 날짜를 선택합니다(계정이 만료되는 시간까지 입력할 수 있습니다).
- 개인별 인증 모드: 사용자를 인증하는 방법을 선택합니다(장치설정을 따름, 지문, 지문 + 비밀번호, 카드, 카드 + 지문, 카드 + 비밀번호, 카드 + 지문/비밀번호, 카드 + 지문 + 비밀번호, 아이디 + 지문, 아이디 + 비밀번호, 아이디 + 지문/비밀번호, 아이디 + 지문 + 비밀번호).
- 직급: 사용자의 직급을 선택합니다.
- 핸드폰번호: 사용자의 휴대전화 번호를 입력합니다.
- 성별: 사용자의 성별을 입력합니다.
- 생일:달력에서 사용자의 생일을 선택합니다.

5. 사용자 설정

5.4.2 지문 탭

지문 탭에서 지문을 등록하기 위해 사용할 스캐너(또는 장치)의 종류와 지문을 인증할 때 적용할 보안 등급을 설정할 수 있습니다. 또한 이 탭에서 지문이 일치하는지 테스트할 수 있으며, 협박 지문을 등록할 수 있습니다. 지문 등록 방법은 3.6.2 를 참조하십시오.

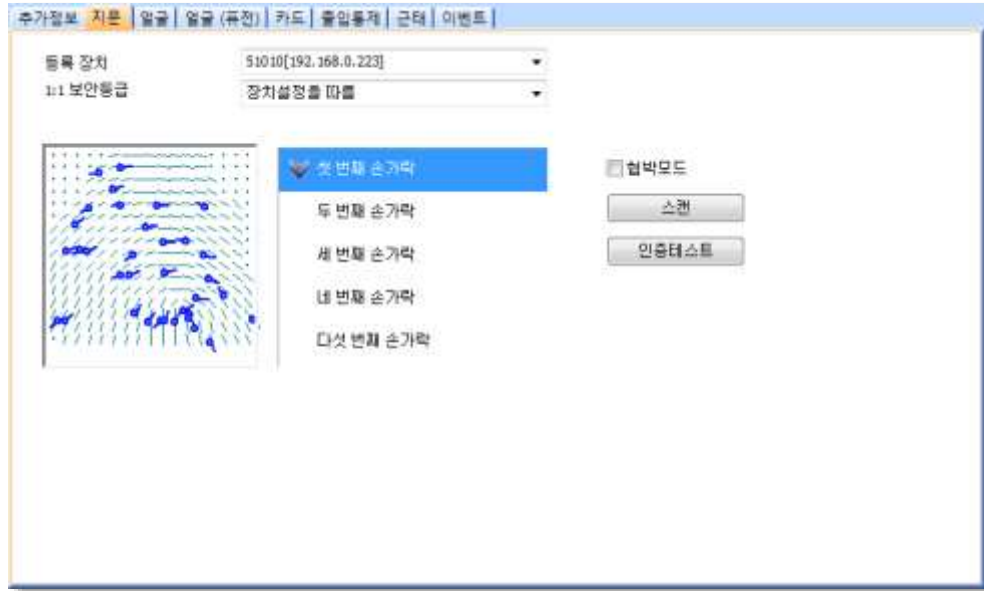


그림 5.36

- **등록 장치:** 사용자를 등록하기 위해 사용할 장치를 선택합니다.
- **1:1 보안등급:** 지문을 인증할 때 사용할 보안 등급(**장치설정을 따름, 아주 낮음 [1/1,000] - 아주 높음 [1/10,000,000]**)을 선택합니다. 보안 등급을 높일수록 본인 거부율(본인의 지문이 확실한데도 장치가 인식하지 못하는 확률)도 같이 증가합니다.
- **협박모드:** 협박 지문으로 사용할 지문을 설정합니다(협박 지문을 이용하여 인증을 하면 경보가 작동하게 됩니다).

5. 사용자 설정

5.4.3 얼굴 탭

얼굴 탭에서 FaceStation 을 이용하여 사용자의 얼굴 템플릿을 캡처할 수 있습니다. FaceStation 에서 등록(사용자당 5 개까지 가능)이 완료되면 25 개의 얼굴 템플릿이 BioStar 로 전송됩니다. 또한 인증 시, 입력된 사용자 얼굴 템플릿이 등록된 얼굴 템플릿보다 높은 점수를 얻은 경우 자동으로 업데이트됩니다. 이미지 캡처에 관한 자세한 내용은 3.6.3 을 참조하십시오.

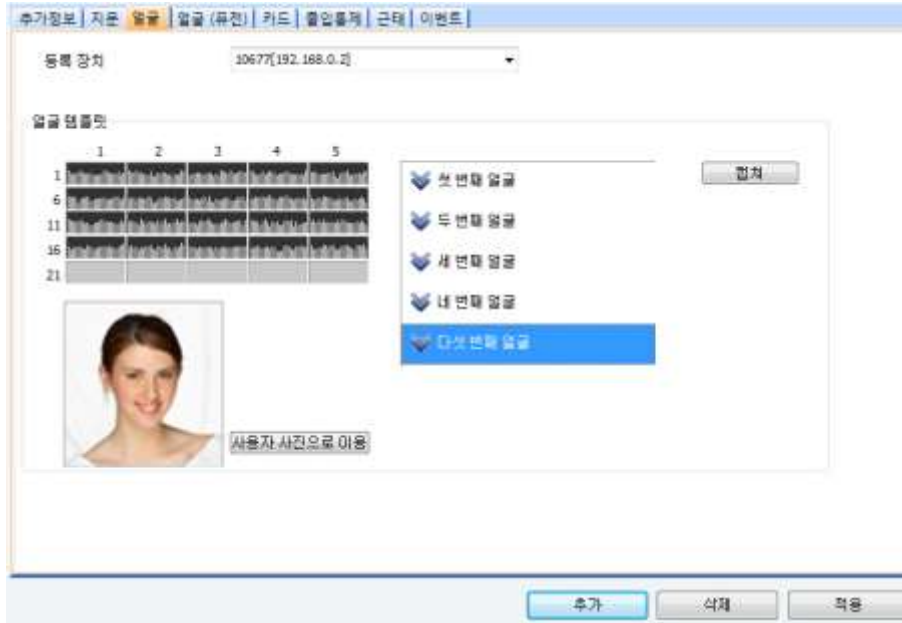


그림 5.37

등록장치: 얼굴 이미지를 캡처할 때 사용할 장치를 선택합니다.

5.4.4 카드 탭

카드 탭에서 카드의 종류와 ID 를 지정할 수 있으며 사용자에게 카드를 발급할 수 있습니다. 카드를 발급하는 방법에 관한 자세한 내용은 3.6.4 를 참조하십시오.

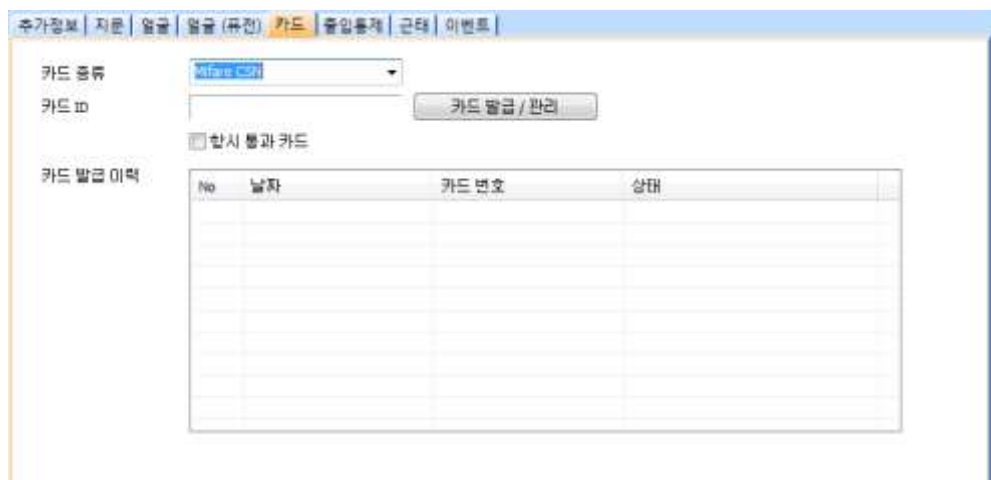


그림 5.38

5. 사용자 설정

- 카드 종류: 발급할 출입 카드의 종류(Mifare CSN, Mifare Template, EM 4100, HID Prox, iCLASS CSN 또는 iCLASS Template)를 선택합니다.
- 카드 ID: 출입 카드의 식별 번호를 입력합니다.
- Custom ID: 출입 카드의 사용자 ID 를 입력합니다.

5.4.5 근태 탭

근태 탭에서 근무 규칙, 휴일 규칙, 개인 휴가 기간을 사용자에게 설정할 수 있습니다. 각 항목을 추가하려면 탭 하단의 **추가**를 클릭합니다. 근태 설정에 변경 사항을 저장하려면 탭 하단의 **적용**을 클릭합니다. 입력한 내용을 선택한 후 **삭제**를 클릭하면 해당 내용을 삭제할 수 있습니다. 근태 설정에 관해 자세한 내용을 보려면 3.9 를 참조하십시오.



그림 5.39

- 근무규칙 설정: 사용자에게 적용할 근무규칙을 설정합니다.
- 휴일규칙 설정: 사용자에게 적용할 휴일규칙을 설정합니다.
- 개인휴가 설정: 개인의 휴가를 입력합니다.

06

기술 지원

BioStar 제품에 대한 의문 사항이나 기술 지원은, (주)슈프리마 기술지원팀(support@supremainc.com)으로 문의하시기 바랍니다.

원활한 기술 지원을 위해 다음 정보를 전달해 주시기 바랍니다.

- 회사명, 이름과 직급, 연락처 및 연락 가능한 시간
- 사용하고 있는 BioStar의 버전과 장치 모델(예: BioStar 1.92, BioStation 2 단말기)
- 에러 메시지의 내용
- 현상 및 문제 설명

오픈 라이선스 공지

AES

FIPS-197 compliant AES implementation Copyright (C) 2006-2007 Christophe Devine

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License, version 2.1 as published by the Free Software Foundation.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

The AES block cipher was designed by Vincent Rijmen and Joan Daemen.

<http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf>
<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

MD5

MD5C.C - RSA Data Security, Inc., MD5 message-digest algorithm
 Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

OpenSSL

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

=====

Copyright (c) 1998-2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

SHA-256

FIPS-180-2 compliant SHA-256 implementation

Copyright (C) 2006-2007 Christophe Devine

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License, version 2.1 as published by the Free Software Foundation.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

The SHA-256 Secure Hash Standard was published by NIST in 2002.

<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>

용어집

경보 구역: 특정 구역을 보호하기 위하여 사용되는 장치들의 묶음. BioStar 는 경보 구역의 입력 지점을 감시하여 침입을 감지하면 경보를 발동합니다.

근태 (T&A, time and attendance): 근로자의 출입(출퇴근) 시간을 기록하여 전체 근무 상황을 파악하고 근무 시간을 계산하고 이를 토대로 급료 등을 계산하는 기능을 가리킵니다. BioStar 를 이용하면 근무규칙(시간구분, 일일규칙, 개인휴가, 휴일규칙)을 설정하여 각 근로자의 근무 시간을 상세하게 파악할 수 있으며 근무 결과를 한 눈에 살펴볼 수 있습니다.

출입 카드: 특정 구역에 출입하기 위해 필요한 카드로 BioStar 는 MIFARE, EM4100, HID 근접식 카드, iCLASS, Felica 카드 등을 지원합니다.

참조: 근접식 카드

출입 통제 시스템: 물리 장치로 이루어지는 시스템으로, 특정 구역에 출입하는 것을 허가하거나 거부하는 등 출입 전반을 일괄 통제 BioStar 는 네트워크에 기반한 바이오인식 출입 통제 시스템입니다.

anti-passback: 출입 카드를 소유한 사람이 제 3 자에게 빌려주어 출입 권한이 없는 사람이 출입하는 것을 방지하기 위한 보안 통신 규약. 참조: timed anti-passback

바이오인식: 본인임을 식별하기 위하여 신체의 일부를 이용하는 기술. BioStar 는 슈프리마의 독보적인 지문인식 기술을 활용하여 지문을 통해서 각 개인의 신원을 확인한 후 출입을 허가합니다.

항시 통과 그룹: 구역에 설정되어 있는 일반적인 제한사항을 모두 무시하고 항상 통과할 수 있는 그룹.

클라이언트: BioStar 클라이언트를 이용하면, 운영자(또는 관리자)는 멀리 떨어진 곳에서도 BioStar 서버에 접속하여 서버에 연결된 장치들을 제어할 수 있습니다. BioStar 클라이언트를 이용하여 시스템에 접속하려면 운영자의 ID 와 비밀번호가 필요합니다.

부서: 직원을 직무의 종류에 따라 분류해 놓은 조직의 단위. 반드시 부서를 사용할 필요는 없지만, 조직의 규모가 큰 경우에는 사용자를 부서별로 분류해 놓은 것이 편리합니다.

장치: 이 설명서에서 "장치"는 BioStar 시스템이 지원하는 모든 종류의 슈프리마 제품을 가리킵니다. BioStar 는 BioStation, BioStationMiFARE, BioStation HID, BioStation T2, BioEntry Plus/BioEntry W, BioEntry PlusMiFARE/BioEntry W MiFARE, BioEntry PlusiCLASS, BioLite Net, Xpass, X-Station, BioMiniUS 단말기, Secure I/O 등의 장치를 지원합니다.

분산 지능: BioStar 시스템에서 인증 데이터베이스는 각 출입 장치에 저장되어 있습니다. 그렇기 때문에 인증 속도가 빠르며 네트워크 연결이 끊겨진 상태에서도 인증 작업을 수행할 수 있습니다.

출입문: 출입문은 빌딩이나 공간에 들어가기 위해서 통과해야 하는 물리적인 장벽을 가리킵니다. 출입을 통제하려면 최소한 하나의 장치가 출입문에 연결되어 있어야 합니다. 그러나 anti-passback 기능이나 기타 다른 기능(출입문 릴레이, 경보 릴레이, 문열림 스위치, 센서 등)을 사용하려면 2 개의 장치가 출입문에 연결되어 있어야 합니다.

협박 지문: 협박에 의해 출입문을 열어야 할 때 사용하기 위해 등록된 지문을 가리킵니다. 이 지문으로 인증을 하면 경보를 발동합니다. 예를 들어, 침입하려는 사람이 시스템에 등록된 사람을 협박하여 특정 장소에 들어가려 합니다. 이럴 때에 "협박 지문"을 이용하여 인증을 하면, 시스템이 출입 권한을 부여함과 동시에 설정된 경보 동작을 실행합니다.

등록: 사용자 계정을 만들고, 지문을 입력하고, 출입 카드를 발급하는 과정.

출입 제한(또는 인증 제한): 특정 구역에 출입할 수 있는 허가를 획득할 수 있는 최대 횟수. 출입 제한 기능은 출입시간 기능과 연동하여 활용할 수 있습니다. 예를 들어, 근무 시간 동안에는 특정 구역에 몇 회 이상 출입하지 못하도록 설정할 수 있습니다.

RF 장치: 무선 주파수를 이용하여 카드를 읽어 들여 출입 권한을 확인하는 장치. BioStar 시스템에서는 기존에 사용하던 제 3 사의 RF 장치도 슈프리마의 단말기에 연결하여 출입통제 시스템을 구성하는 일부분으로 계속 사용할 수 있습니다.

ESSID: Extended Service Set ID. ESSID 는 무선 네트워크의 무선 공유기(AP 장비)을 나타내기 위한 이름입니다. 이것을 사용함으로써 하나의 무선 네트워크를 다른 무선 네트워크와 구별할 수 있습니다. ESSID 는 SSID 의 한 종류이며, 다른 종류로 SSID 가 있습니다.

지문 인증: 2 개의 지문, 즉 이전에 입력한 지문과 현재 제시하는 지문을 비교하여 출입을 허가하는 과정. BioStar 는 여러 차례 수상한 경력이 있는 슈프리마의 독보적인 지문 인식 알고리즘을 사용합니다.

지문 센서: 지문을 디지털 이미지로 입력하기 위한 전자 장치. 지문 센서를 이용하여 지문을 입력하면 가공되지 않은 데이터로 저장됩니다. 이 가공되지 않은 데이터를 처리하여 지문 템플릿(개별 지문의 두드러진 특징을 모은 것)을 만들고, 이것을 이용하여 사용자를 인증합니다.

화재 경보 구역: 화재가 발생했을 경우 자동적으로 제어해야 할 필요가 있는 출입문들을 모아 놓은 집합.

호스트: RS485 네트워크에서 마스터로 동작하는 장치. 호스트 장치는 슬레이브 장치와 RS485 네트워크의 슬레이브 장치 사이에 이루어지는 데이터 교환을 중개합니다.

얼굴 인증: 얼굴 정보를 이용하여 사용자의 신원 확인을 하는 과정. 일반적으로 촬영된 얼굴 영상과 영상으로부터 추출된 얼굴의 윤곽, 눈, 코, 입 등의 외형 정보와 얼굴 내부의 조명에 불변한 질감 등의 특징 정보 등을 복합적으로 이용하여 기존에 시스템에 저장된 사용자의 얼굴 정보와 비교하여 신원 확인을 하는 과정

입력 신호: 문열림 버튼과 같은 슬레이브 장치에서 전달되는 신호.

운영자: BioStar 클라이언트를 사용할 수 있는 권한을 가진 직원. BioStar 에는 미리 정의된 3 가지 등급의 운영자(관리자, 운영자, 감독자)가 있습니다. 최대 16 개의 운영자 등급을 사용자가 직접 만들어 적용할 수 있습니다.

근접식 카드: 근접식 카드는 접촉하지 않고, 즉 장치에 긁지 않고서 사용할 수 있는 IC 카드를 가리킵니다. BioStation, BioEntry Plus, BioLite Net 및 Xpass 는 EM4100 카드를 지원하며, BioStationMiFARE, BioEntry PlusMiFARE, BioEntry W MiFARE, BioLite Net, Xpass, BioStation T2 및 X-Station 은 MiFARE 를 지원하며, BioStation HID 및 Xpass 는 HID 근접식 카드를 지원합니다.

보안 등급: 이 용어는 두 가지 개념, 즉 타인수락률과 본인거부율과 관계되어 있습니다.

- **타인수락률:** 타인수락률(FAR)은 실제 지문의 소유자와 다른 사용자에게 출입을 허가하는 확률을 가리킵니다. 타인수락률은 전체 인증을 대비 타인을 수락한 비율을 나타냅니다.
- **본인거부율:** 본인거부율(FRR)은 실제 지문의 소유자임에도 불구하고 시스템이 출입을 거부하는 확률을 가리킵니다. 본인거부율은 전체 인증을 대비 본인을 거부한 비율을 나타냅니다.

Timed anti-passback: anti-passback 기능과 기본적인 목적은 동일하며, 지정된 시간 안에 같은 ID 나 지문을 이용하여 특정 구역에 다시 출입할 수 없도록 하는 기능. 참조: anti-passback

출입시간: 지정된 시간에 출입을 허가하거나 금지하기 위하여 사용하는 일정. 출입시간과 출입문을 조합하여 출입그룹을 만들 수 있습니다.

사용자: 출입 권한을 가지고 있는 사람. 사용자의 출입 권한은 개별 사용자에게 적용된 권한(사용자 등급), 사용자가 속한 출입그룹에 적용된 권한, 특정 시간에 적용된 제한사항에 따라 결정됩니다.

위캔드 인터페이스: 카드 입력 장치와 그외 출입 시스템을 연결하기 위한 배선 표준. 위캔드 인터페이스는 3 개의 선을 이용합니다. 하나는 접지선이고 다른 두 선은 데이터를 전송하는 선입니다. 데이터 선은 DATA0과 DATA1로 불리며, 때로 Data High 와 Data Low 로 불립니다.

구역: 구역은 2 개 이상의 장치를 묶어서 만든 가상의 공간을 가리킵니다. BioStar 는 미리 설정된 7 개의 구역을 지원합니다.

2

2 중 인증 방식, 137, 189, 200

B

BioEntry Plus
설정하기, 35

BioEntry W
설정하기, 35

BioEntry W2
설정하기, 45

BioLite Net
설정하기, 36

BioStar 서버
설치하기, 13

BioStar 클라이언트
설치하기, 18

BioStation, 2
무선랜으로 연결하기, 35
설정하기, 34

BioStation 2 설정하기, 41

BioStation A2 설정하기, 42

BioStation L2
설정하기, 44

BioStation T2
설정하기, 39

BioStation T2, 2

F

FaceStation
설정하기, 40

I

Interlock 구역
추가정보 탭, 254

T

TCP/IP 설정, 139, 180, 192, 202, 213,
222, 230, 238

U

USB 동글, 1

W

Wiegand 탭
BioEntry Plus, 156
BioEntry W, 156
BioEntry W2, 241
BioStation, 146
BioStation 2, 218
BioStation A2, 226
BioStation L2, 234
BioStation T2, 199
FaceStation, 209
Xpass, 172
Xpass S2, 178
X-Station, 187

Wiegand 형식
26 비트 표준, 47
변경하기, 46
사용자 설정, 48
패스 스루, 47

X

Xpass
설정하기, 37

Xpass S2
설정하기, 37

X-Station
설정하기, 38

찾아보기

ㄱ

경보

- 경보 동작 설정하기, 96
- 경보와 경보음 설정하기, 96
- 해제하기, 118

경보 구역

- 경보 동작과 출력 설정하기, 58
- 경비 개시와 경비 해제 설정하기, 58
- 알람 탭, 249
- 외부 I/O 연동 설정하기, 60
- 추가정보 탭, 249
- 출입통제그룹 탭, 250

경보음

- 임의의 경보음 추가하기, 96

관리자 계정, 19

- 권한이나 비밀번호 변경하기, 26
- 임의의 관리자 계정 추가하기, 27
- 추가하기, 25

구역

- 경보 동작과 출력 설정하기, 58
- 구역 종류, 54
- 이벤트 보기, 61
- 입력 설정하기, 57
- 장치 추가하기, 55
- 제한 무시하기, 61
- 추가하기, 55

구역 설정하기, 245

- Interlock 구역, 254
- 경보 구역, 248
- 소집 구역, 252
- 이중출입 방지 구역, 245
- 인증 제한 구역, 247
- 출입 구역, 252
- 화재 경보 구역, 250

근태 보고서

- 생성하기, 127
- 수정하기, 129
- 인쇄하기 및 내보내기, 130

근태 설정하기

- 개인휴가 추가하기, 93

- 근무규칙 사용자에게 적용하기, 90

- 근무규칙 추가하기, 88
- 시간구분 추가하기, 86
- 일일규칙 추가하기, 87
- 휴일규칙 추가하기, 92

근태 탭

- BioEntry W2, 241
- BioLite Net, 164
- BioStation, 145
- BioStation 2, 217
- BioStation A2, 225
- BioStation L2, 233
- BioStation T2, 198
- FaceStation, 208
- X-Station, 186

ㄴ

네트워크 탭

- BioEntry Plus, 150
- BioEntry W, 150
- BioLite Net, 159
- BioStation, 139
- BioStation 2, 213
- BioStation A2, 222
- BioStation L2, 230
- BioStation T2, 191, 238
- FaceStation, 202
- Xpass, 167
- Xpass S2, 173
- X-Station, 180

ㄷ

데이터

- 사용자 데이터 가져오기, 125

데이터베이스

- BioAdmin 에서 BioStar 로 옮기기, 23

데이터베이스 만들기, 15

도구 표시줄, 21

동작 모드

- 1 대 1, 136, 173, 178

찾아보기

1 대 N, 137

동작모드 탭

BioEntry Plus, 146
BioEntry W, 146
BioEntry W2, 235
BioLite Net, 157
BioStation, 136
BioStation 2, 209
BioStation A2, 218
BioStation L2, 227
BioStation T2, 188
FaceStation, 199
Xpass, 166
Xpass S2, 172
X-Station, 178

ㄹ

리프트

사용자 추가하기, 52
설정하기, 51, 52
장치에 설정 전송하기, 53
추가하기, 51
출입 장치 연결하기, 51

□

무선랜

연결하기, 32

ㅂ

보안 등급, 138, 191, 201, 212, 221, 229, 237

비주얼 맵

추가하기, 114
출입문 감시하기, 116

ㅅ

사용자

계정 만들기, 61
근태 탭, 258
다른 부서로 이동하기, 122

데이터 가져오기, 125

데이터 내보내기, 124

모든 정보를 동기화하기, 76

삭제하기, 121

새로운 정보 항목 추가하기, 123

얼굴 탭, 257

장치에서 정보 가져오기, 76, 77

정의 항목 설정하기, 123

정의 항목 편집하기, 123

지문 등록하기, 63

지문 탭, 256

추가정보 탭, 255

카드 탭, 257

커맨드 카드로 개별 사용자 삭제하기, 121

커맨드 카드로 등록하기, 65

커맨드 카드로 모든 사용자 삭제하기, 122

서버 매칭

BioEntry Plus, 149
BioEntry W2, 236
BioLite Net, 159
BioStation, 138
BioStation 2, 211
BioStation A2, 220
BioStation L2, 228
BioStation T2, 189
Xpass, 166

서버 설정, 139, 181, 192, 203, 213, 222, 230, 238

설정 변경하기

BioEntry Plus, 146
BioEntry W, 146
BioLite Net, 157
BioStation, 135
BioStation T2, 188
FaceStation, 199
Xpass, 166
Xpass S2, 172
X-Station, 178

센서 감도, 138

소집 구역

추가정보 탭, 253
출입통제그룹 탭, 253

찾아보기

슬레이브 장치

- 내보내는 출력 설정하기, 99
- 받아들이는 입력 신호 설정하기, 100
- 추가하기, 30

시스템 요구사항, 11

실시간 감시, 107

실시간으로 소집구역 감시하기, 109

○

알람

- 동작 개시 이벤트, 142, 184, 195, 206
- 멈춤 이벤트, 143, 184, 195, 206
- 우선순위, 143, 184, 195, 206

얼굴 이미지 캡처하기, 66

얼굴 탭

- FaceStation, 201

이메일 통지, 97

이벤트

- 기록 보기, 110
- 기록을 바이오스타에 전송하기, 111
- 메인 창에서 기록 보기, 111
- 실시간으로 감시하기, 107

이벤트 기록

- 모니터링 창에서 보기, 112
- 엑세스 로그 보기, 113

이중출입 방지 구역

- 알람 탭, 246
- 추가정보 탭, 245
- 출입통제그룹 탭, 247

인증 거부 리스트 탭

- BioEntry Plus, 154
- BioEntry W, 154
- BioLite Net, 163
- BioStation, 143
- BioStation 2, 215
- BioStation A2, 224
- BioStation L2, 232
- BioStation T2, 196, 240
- X-Station, 185

인증 제한 구역

- 알람 탭, 248
- 추가정보 탭, 247
- 출입통제그룹 탭, 248

인증 제한 설정, 140, 181, 193, 203

인터폰 탭

- BioStation 2, 214
- BioStation T2, 193
- FaceStation, 204

입력 탭

- BioEntry Plus, 151
- BioEntry W, 151
- BioLite Net, 161
- BioStation, 140
- BioStation 2, 214
- BioStation A2, 223
- BioStation L2, 231
- BioStation T2, 194, 239
- FaceStation, 204
- Xpass S2, 174
- X-Station, 183

ㄴ

장치

- 검색 방법, 29
- 설정 변경하기, 135
- 자동 잠금 설정하기, 119
- 잠그거나 잠금 해제하기, 119
- 잠금 초기화하기, 120
- 제거하기, 132
- 추가하기, 28
- 펌웨어 업그레이드하기, 132

장치 창, 35, 36, 37

지문

- 등록하기, 64
- 센서에 올바르게 놓기, 63
- 암호화 사용하기, 133
- 영상 품질 기준, 138, 191, 212, 221, 230, 237

지문 탭

- BioEntry Plus, 148

찾아보기

BioEntry W, 148
BioLite Net, 158
BioStation, 138
BioStation 2, 212
BioStation A2, 221
BioStation L2, 229
BioStation T2, 190, 237

츠

출력 탭

BioEntry Plus, 152
BioEntry W, 152
BioLite Net, 162
Xpass, 169, 170
Xpass S2, 175

출입 구역

추가정보 탭, 252

출입 카드

DESFire 레이아웃 편집하기, 73
EM4100, 67
HID 근접식, 68
iClass CSN, 69
iCLASS 레이아웃 편집하기, 74
iCLASS 템플릿 카드, 70
MIFARE 레이아웃 편집하기, 72
MIFARE, DESFire 템플릿 카드, 70
Mifare/DESFire CSN, 69
발급하기, 67
사이트 키변경하기, 71

출입그룹

사용자 추가하기, 82
사용자에게 할당하기, 83
장치에 전송하기, 84
추가하기, 82

출입그룹 탭

BioEntry Plus, 151
BioEntry W, 151
BioLite Net, 160
BioStation 2, 214
BioStation A2, 223
BioStation L2, 231
BioStation T2, 193, 238

FaceStation, 203
Xpass S2, 174
X-Station, 181
바이 BioStation, 140

출입문

설정 변경하기, 242
설정하기, 50
알람 탭, 244
열거나 닫기, 118
장치 연결하기, 49
추가정보 탭, 242
추가하기, 49
출입문 그룹 만들기, 51

출입시간

만들기, 80
메인 창, 80

출입통제 그룹

선택하기, 61

출력 탭

BioStation, 141
BioStation T2, 195
FaceStation, 205
X-Station, 184

ㅋ

카메라 탭

BioStation A2, 222
BioStation T2, 191
FaceStation, 202
X-Station, 180

커맨드 카드

개별 사용자 삭제하기, 121
모든 사용자 삭제하기, 122
발급하기, 36, 38
사용자 등록하기, 65

커맨드카드 탭

BioEntry Plus, 155
BioEntry W, 155
Xpass, 170
Xpass S2, 176

찾아보기

ㅎ

호스트 장치

추가하기, 30

화면/음성 탭

BioEntry Plus, 155

BioEntry W, 155

BioLite Net, 163

BioStation, 143

BioStation 2, 216

BioStation A2, 224

BioStation L2, 232

BioStation T2, 196, 240

FaceStation, 207

Xpass, 171

Xpass S2, 177

X-Station, 185

화재 경보 구역

알람 탭, 251

추가정보 탭, 250

휴일군, 81

suprema BioStar



(주)슈프리마

463-863 경기도 성남시 분당구 정자동 파크뷰 오피스타워 16층

전화: 031-783-4510

팩스: 031-783-4517

이메일: sales@supremainc.com 홈페이지: www.supremainc.com