출입 통제 시스템: 역할 및 권한 정의서 (RBAC)

본 문서는 `Admin UI` 및 API에 대한 접근을 통제하는 **역할 기반 접근 제어(RBAC)** 모델을 상세히 정의합니다.

1. RBAC 아키텍처 개요

본 시스템의 권한 모델은 `sdac-database-schema.md` (DB 스키마)와 `sdac-api-contract-part2-iam.md` (API)에 정의된 **다대다(M:N) 매핑**을 기반으로 합니다.

1. **권한 (Permissions):** 시스템에서 수행할 수 있는 가장 작은 단위의 행동입니다. (예: `USER_CREATE` - 출입자 생성)
2. **역할 (Roles):** 여러 '권한'의 묶음(집합)입니다. (예: `USER_MANAGER` - 사용자 관리자 역할)
3. **관리자 (Admins):** 여러 '역할'을 할당받는 실제 계정입니다. (예: `admin_kim`)

M:N 관계:

- 한 명의 관리자(`admin_users`)는 여러 개의 역할(`roles`)을 가질 수 있습니다.
- 하나의 역할(`roles`)은 여러 개의 권한(`permissions`)을 가질 수 있습니다.

2. 권한 (Permissions) 상세 목록

`permissions` 테이블에 저장되며, `sdac-api-contract-detailed.md`의 각 API 엔드포인트와 1:1로 매핑되는 시스템의 모든 세부 권한입니다.

A. 관리자 계정 및 권한 관리 (IAM)

권한 (Permission)	API (예시)	설명 (무엇을 할 수 있는가)
`ADMIN_READ`	`GET /api/admin/iam/admins`	관리자 계정 목록 및 상세 정보 조회
`ADMIN_CREATE`	`POST /api/admin/iam/admins`	새 관리자 계정 생성
`ADMIN_UPDATE`	`PUT /api/admin/iam/admins/{id}`	관리자 정보(이름, 부서, 연락처) 수정
`ADMIN_STATUS_UPDATE`	`PUT /api/admin/iam/admins/{id}/status`	관리자 계정 활성화/잠금(비활성화)(셀프 수정

권한 (Permission)	API (예시)	설명 (무엇을 할 수 있는가)
		불가)
ADMIN_PASSWORD_RESET	POST /api/admin/iam/admins/{id}/reset-password	(중요) 타 관리자의 비밀번호를 강제 재설정
ADMIN_ROLE_UPDATE	PUT /api/admin/iam/admins/{id}/roles	(중요) 관리자에게 역할을 할당(매핑)
ROLE_READ	GET /api/admin/iam/roles	역할 목록 및 상세 정보 조회
ROLE_CREATE	POST /api/admin/iam/roles	새 역할 생성
ROLE_DELETE	PUT /api/admin/iam/roles/{id}/status	역할 비활성화(Soft Delete)
PERMISSION_READ	GET /api/admin/iam/permissions	권한 목록 및 상세 정보 조회
PERMISSION_CREATE	POST /api/admin/iam/permissions	새 권한 생성 (개발/운영용)
PERMISSION_DELETE	PUT /api/admin/iam/permissions/{id}/status	권한 비활성화(Soft Delete)
ROLE_PERMISSION_UPDATE	PUT /api/admin/iam/roles/{id}/permissions	(중요) 역할에 권한을 할당(매핑)
DEPARTMENT_READ	GET /api/admin/users/departments	부서 목록 및 상세 정보 조회
DEPARTMENT_CREATE	POST /api/admin/users/departments	새 부서 생성
DEPARTMENT_UPDATE	PUT /api/admin/users/departments/{id}	부서 정보 수정
DEPARTMENT_DELETE	PUT /api/admin/users/departments/{id}/status	부서 비활성화(Soft Delete)

B. 출입자 및 인증 매체 관리 (User)

권한 (Permission)	API (예시)	설명 (무엇을 할 수 있는가)
USER_READ	GET /api/admin/users	출입자 목록 및 상세 정보 조회
USER_CREATE	POST /api/admin/users	새 출입자 등록
USER_UPDATE	PUT /api/admin/users/{id}	출입자 정보(이름, 부서, 사번 등) 수정
USER_STATUS_UPDATE	PUT /api/admin/users/{id}/status	출입자 계정 활성화/정지(비활성화)

권한 (Permission)	API (예시)	설명 (무엇을 할 수 있는가)
USER_GROUP_READ	GET /api/admin/users/groups	출입자 그룹 목록 및 상세 정보 조회
USER_GROUP_CREATE	POST /api/admin/users/groups	새 출입자 그룹 생성
USER_GROUP_UPDATE	PUT /api/admin/users/groups/{id}	출입자 그룹 정보 수정
USER_GROUP_DELETE	PUT /api/admin/users/groups/{id}/status	출입자 그룹 비활성화(Soft Delete)
USER_GROUP_ASSIGN	PUT /api/admin/users/{id}/groups	출입자에게 그룹을 할당(매핑)
CREDENTIAL_READ	GET /api/admin/credentials	인증 매체(카드, 지문 등) 목록 및 상세 조회
CREDENTIAL_CREATE	POST /api/admin/credentials	출입자에게 새 인증 매체 등록(발급)
CREDENTIAL_UPDATE	PUT /api/admin/credentials/{id}/status	인증 매체 상태 변경 (예: '분실', '만료')
FILE_UPLOAD	POST /api/admin/uploads/prepare	출입자/관리자 사진 업로드 (MinIO 연동)

C. 정책 및 장치 관리 (Policy)

권한 (Permission)	API (예시)	설명 (무엇을 할 수 있는가)
POLICY_READ	GET /api/admin/policies/rules	접근 규칙, 구역(Zone), 시간표(Schedule) 조회
POLICY_CREATE	POST /api/admin/policies/rules	새 접근 규칙(매핑) 생성
POLICY_UPDATE	PUT /api/admin/policies/rules/{id}	접근 규칙 수정 (시간표 변경 등)
POLICY_DELETE	PUT /api/admin/policies/rules/{id}/status	접근 규칙 비활성화
DEVICE_READ	GET /api/admin/policies/devices	장치(리더기, ACU) 목록 및 상세 조회
DEVICE_CREATE	POST /api/admin/policies/devices	새 장치 등록
DEVICE_UPDATE	PUT /api/admin/policies/devices/{id}	장치 정보(이름, IP, 위치 등) 수정
DEVICE_TOKEN_RESET	POST /api/admin/policies/devices/{id}/rotate-token	(중요) 장치 토큰(비밀 키) 강제 재발급
DEVICE_ASSIGN	PUT /api/admin/policies/doors/{id}/devices	문(Door)에 장치(Device)를 할당(매핑)

D. 로그 및 명령 (Log & Command)

권한 (Permission)	API (예시)	설명 (무엇을 할 수 있는가)
`LOG_READ_ACCESS`	`GET /api/admin/logs/access`	**출입 기록** 조회 및 검색
`LOG_READ_AUDIT`	`GET /api/admin/logs/audit`	**관리자 활동 기록** 조회 및 검색
`COMMAND_DOOR_OPEN`	`POST /api/admin/commands/open-door`	(중요) 특정 문을 원격으로 개방
`COMMAND_LOCKDOWN`	`POST /api/admin/commands/lockdown`	(중요) 특정 구역(또는 전체)을 비상 봉쇄
`COMMAND_ALL_OPEN`	`POST /api/admin/commands/all-open`	(중요) 특정 구역(또는 전체)을 비상 개방

3. 기본 역할 (Roles) 정의 (예시)

시스템 운영을 위한 4가지 기본 역할 예시입니다. `POST /api/admin/iam/roles`로 생성하고 `PUT .../roles/{id}/permissions`로 권한을 할당합니다.

A. 최고 관리자 (Super Administrator)

- **설명:** 시스템의 모든 권한을 가진, 시스템 구축 시 생성되는 최초의 관리자입니다.
- **주요 권한 (예시):** `모든 권한 (All Permissions)`
  - `ADMIN_CREATE`, `ADMIN_PASSWORD_RESET`, `ROLE_PERMISSION_UPDATE` 등 모든 관리자/역할/권한 관리
  - 모든 출입자 및 정책 관리
  - 모든 로그 조회

B. 정책/인사 관리자 (HR & Policy Manager)

- **설명:** 출입자 정보를 등록/관리하고, 출입 정책을 설정하는 관리자입니다.
- **주요 권한 (예시):**
  - `USER_READ`, `USER_CREATE`, `USER_UPDATE`, `USER_STATUS_UPDATE`
  - `CREDENTIAL_READ`, `CREDENTIAL_CREATE`, `CREDENTIAL_UPDATE`
  - `POLICY_READ`, `POLICY_CREATE`, `POLICY_UPDATE`, `POLICY_DELETE`
  - `DEVICE_READ`, `DEVICE_CREATE`, `DEVICE_UPDATE`, `DEVICE_ASSIGN`
  - `DEPARTMENT_CREATE`, `DEPARTMENT_UPDATE`
  - `FILE_UPLOAD`

- **제외:** `ADMIN_*` (관리자 계정 관리 불가), `LOG_READ_AUDIT` (감사 로그 불가), `COMMAND_*` (비상 명령 불가)

C. 보안/감사 담당자 (Security Auditor)

- **설명:** 시스템의 모든 설정을 **'읽기 전용(Read-Only)'**으로 조회하고 감사 로그를 확인할 수 있는 역할입니다. (수정/생성/삭제 불가)
- **주요 권한 (예시):**
  - `LOG_READ_ACCESS` (필수)
  - `LOG_READ_AUDIT` (필수)
  - `ADMIN_READ`, `ROLE_READ`, `PERMISSION_READ`, `DEPARTMENT_READ`
  - `USER_READ`, `USER_GROUP_READ`, `CREDENTIAL_READ`
  - `POLICY_READ`, `DEVICE_READ`
- **제외:** `_CREATE`, `_UPDATE`, `_DELETE` 등 모든 변경 권한, `COMMAND_*` (비상 명령 불가)

D. 현장 보안 요원 (Security Operator)

- **설명:** `Admin UI`의 실시간 대시보드를 모니터링하고, 비상 상황(예: 방문객 원격 개방)에 대응하는 현장 요원입니다.
- **주요 권한 (예시):**
  - `COMMAND_DOOR_OPEN` (필수)
  - `LOG_READ_ACCESS` (방금 통과한 사람 확인용)
  - `USER_READ` (출입자 사진 대조용)
- **제외:** `POLICY_*`, `ADMIN_*` 등 모든 '설정' 관련 권한