

ai-admin

관리자 가이드

폐쇄망 배포·설정·권한·운영 절차

버전 v1.2.18

작성일 2026-09-10

문서 관리자 가이드

ai-admin 관리자 가이드

v1.2.18 기준입니다. 이 문서는 ai-admin을 설치하고 지키는 사람을 위한 것입니다. 화면을 쓰는 방법은 [사용자 가이드](#)에 있습니다.

화면 캡처는 합성 데이터로 채운 실제 ai-admin 화면을 1440×1024에서 찍은 것입니다. 캡처 도구가 가린 [민감정보 마스킹], [표 데이터 마스킹], [API 키 마스킹], [내부 URL 마스킹] 자리에는 실제 화면에서 해당 값이 그대로 표시됩니다.

깊이 들어가는 내용은 다음 문서에 있고 여기서는 링크만 겁니다.

- [운영 가이드](#) — 배포·백업·업그레이드·정기 점검
- [보안 가이드](#) — 인증·세션·키·저장 비밀값의 보안 모델
- [REST·AI API](#) · [MCP](#) — 연동 계약
- [아키텍처](#) · [레거시 관리 설계](#) · [데이터베이스 호환성](#)

1. 구성 요소

ai-admin은 Go 서버 하나가 React 정적 파일을 내장한 단일 컨테이너입니다. 서버 자체는 상태를 갖지 않고 모든 상태는 PostgreSQL에 있습니다.

구성 요소	필수	역할
ai-admin 컨테이너	예	HTTP :8080 하나로 UI, REST API, OpenAI 호환 AI 프록시, MCP를 제공
PostgreSQL	예	ai_admin 스키마(신규 관리 데이터)와 레거시 AI Portal 스키마를 모두 보관
Keycloak (OIDC)	아니요	SSO 로그인. 고면 로컬 계정만 사용
사내 AI 엔드포인트	아니요	관리자가 등록하는 OpenAI 호환 공급자. 없으면 AI 기능만 쓰지 못함
레거시 Java AI Portal	아니요	같은 DB를 공유하는 기존 서비스. 함께 운영할 때만 해당

주고받는 것

방향	대상	내용
브라우저 → ai-admin	:8080	세션 쿠키 + CSRF 쿠키로 인증한 REST 호출
자동화 → ai-admin	:8080	Authorization: Bearer aia_... API 키. /v1/chat/completions , /v1/models , /mcp
ai-admin → PostgreSQL	5432	최대 20 · 최소 2 연결 풀
ai-admin → Keycloak	443 등	discovery, 토큰 교환, JWKS
ai-admin → AI 공급자	공급자 Base URL	OpenAI 호환 요청 중계(스트리밍 포함)

Compose 파일은 PostgreSQL을 함께 띄우지 않습니다. POSTGRES_DSN 의 호스트는 컨테이너에서 실제로 닿는 주소여야 합니다.

2. 설치

릴리즈 자산으로 처음부터 끝까지 진행합니다. 인터넷이 연결된 빌드 환경에서 직접 빌드하는 방법은 [README](#)에 있습니다.

2.1 필요한 자원

항목	값
노출 포트	8080/tcp 하나
볼륨	없음. 컨테이너는 read_only 로 뜨고 /tmp 만 64MB tmpfs
컨테이너 권한	cap_drop: ALL , no-new-privileges:true
필요한 바깥 연결	PostgreSQL, (선택) Keycloak, (선택) AI 공급자 엔드포인트
DB 권한	ai_admin 스키마 생성·변경(DDL)과 레거시 스키마 읽기, 관리 대상 테이블 쓰기

2.2 이미지 반입

GitHub Release에서 ai-admin-v1.2.18.tar.gz 와 SHA256SUMS 를 받아 승인된 매체로 반입합니다. 반입 전후 모두 체크섬을 확인하세요. 공식 아카이브는 Linux amd64 입니다.

```
sha256sum -c SHA256SUMS
gzip -t ai-admin-v1.2.18.tar.gz
gzip -dc ai-admin-v1.2.18.tar.gz | docker load
docker image inspect ai-admin:v1.2.18 --format '{{.RepoTags}}'
```

2.3 환경 파일과 기동

`compose.offline.yml` 과 `.env` 를 같은 디렉터리에 둡니다. `.env` 에는 아래 네 개만 넣습니다.

```
openssl rand -base64 32 # ENCRYPTION_KEY 로 쓸 값을 만든다
```

```
POSTGRES_DSN=postgres://ai_admin:CHANGE_ME@postgres.example.com:5432/aiportal?sslmode=require
BOOTSTRAP_ADMIN=admin@example.com
BOOTSTRAP_ADMIN_PASSWORD=CHANGE_ME_AT_LEAST_12_CHARS
ENCRYPTION_KEY=REPLACE_WITH_BASE64_32_BYTES
```

```
docker compose --env-file .env -f compose.offline.yml up -d
docker compose -f compose.offline.yml ps
curl --fail http://localhost:8080/health/live
curl --fail http://localhost:8080/health/ready
curl --fail http://localhost:8080/api/v1/meta
```

Compose를 쓰지 않으면 같은 설정을 `docker run` 으로 줍니다.

```
docker run -d --name ai-admin --restart unless-stopped \
  --env-file .env -p 8080:8080 \
  --read-only --tmpfs /tmp:size=64m,noexec,nosuid \
  --cap-drop ALL --security-opt no-new-privileges \
  ai-admin:v1.2.18
```

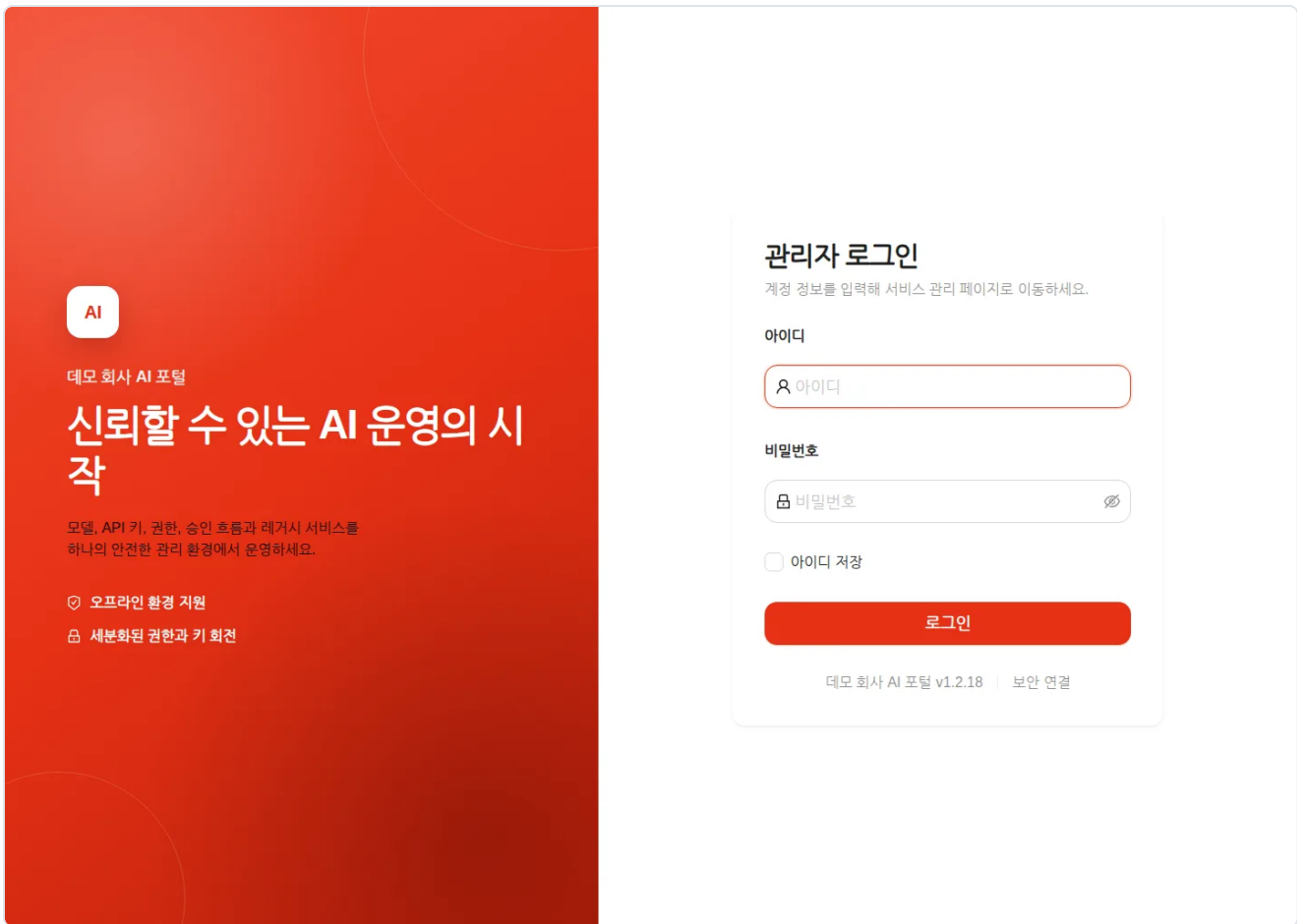
시작할 때 DB 연결 → migration → seed 순으로 진행하며, 하나라도 실패하면 프로세스는 종료됩니다.

2.4 최초 관리자 계정

`BOOTSTRAP_ADMIN` · `BOOTSTRAP_ADMIN_PASSWORD` 로 만든 계정이 최초 로컬 서비스 관리자입니다.

- 매 시작마다 `super_admin` 역할이 보장됩니다.
- 같은 아이디의 로컬 계정이 이미 있으면 역할만 보장하고 비밀번호는 덮어쓰지 않습니다.
- 같은 아이디가 OIDC 등 비로컬 계정이면 서비스가 시작을 거부합니다.
- 아이디 조화는 대소문자를 구분하지 않습니다.

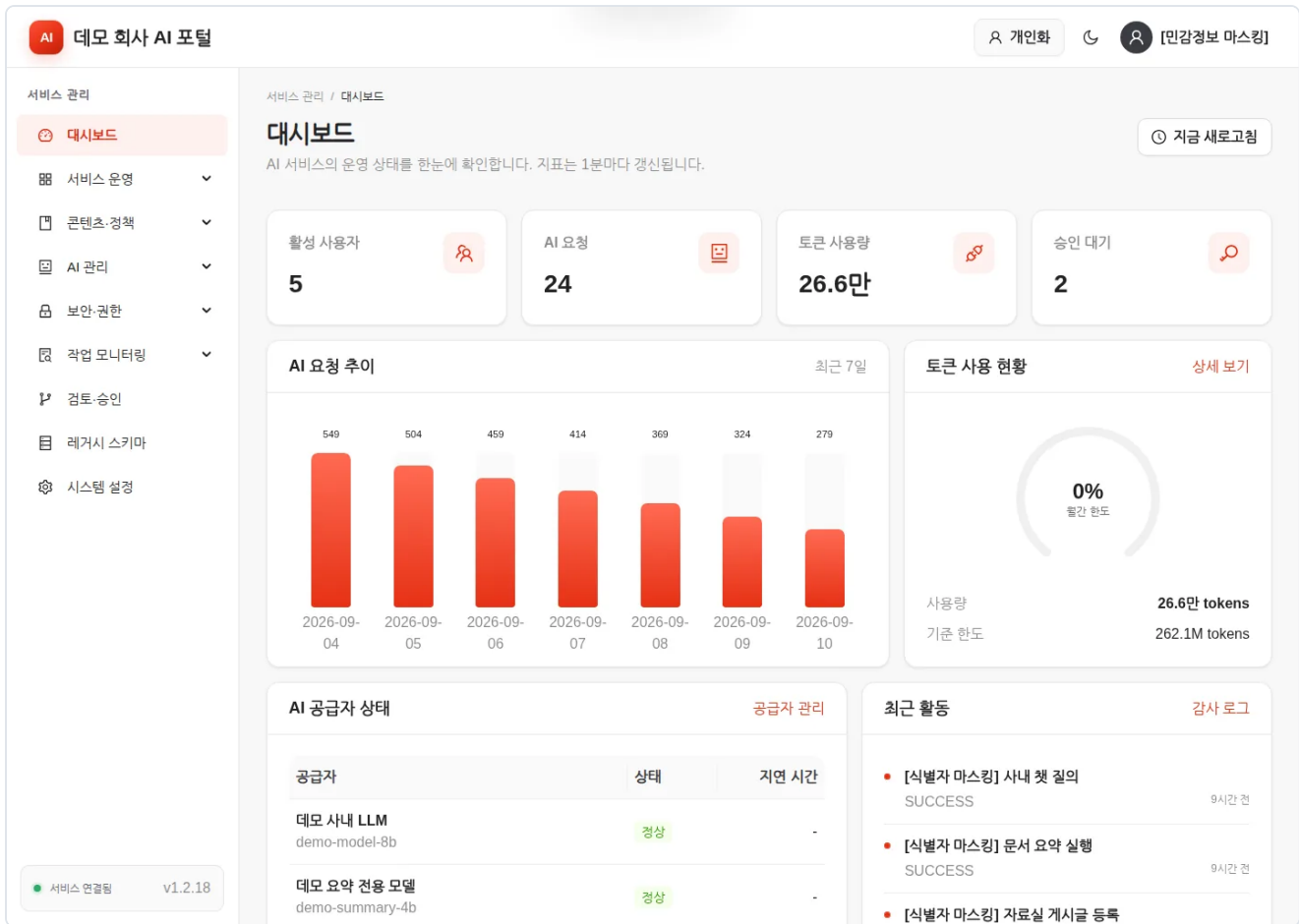
브라우저에서 `http://<호스트>:8080` 을 열고 이 계정으로 로그인합니다.



로그인 화면 — 아이디·비밀번호와 카드 아래 서비스 이름·버전

로그인 카드 아래의 버전이 배포한 이미지 태그와 같은지 확인하세요.

2.5 최초 로그인 후 점검



대시보드 — 활성 사용자·AI 요청·토큰 사용량·승인 대기와 AI 공급자 상태

1. 대시보드가 뜨고 지표가 오류 없이 계산되는지 확인합니다.
2. 프로필 메뉴에서 서비스 버전을 다시 확인합니다.
3. 시스템 설정 → 서비스 기본에서 서비스 표시 이름과 서비스 Public URL을 확인합니다.
4. 레거시 스키마에서 실제 스키마 이름과 테이블 목록이 보이는지 확인합니다.
5. 두 번째 서비스 관리자 또는 복구 절차를 확보한 뒤에 SSO를 컷니다.

3. 설정

3.1 환경 변수 (전수)

ai-admin이 읽는 환경 변수는 다음 네 개가 전부입니다. 나머지 운영 설정은 모두 관리자 화면에 있습니다. 예시 값은 모두가짜입니다.

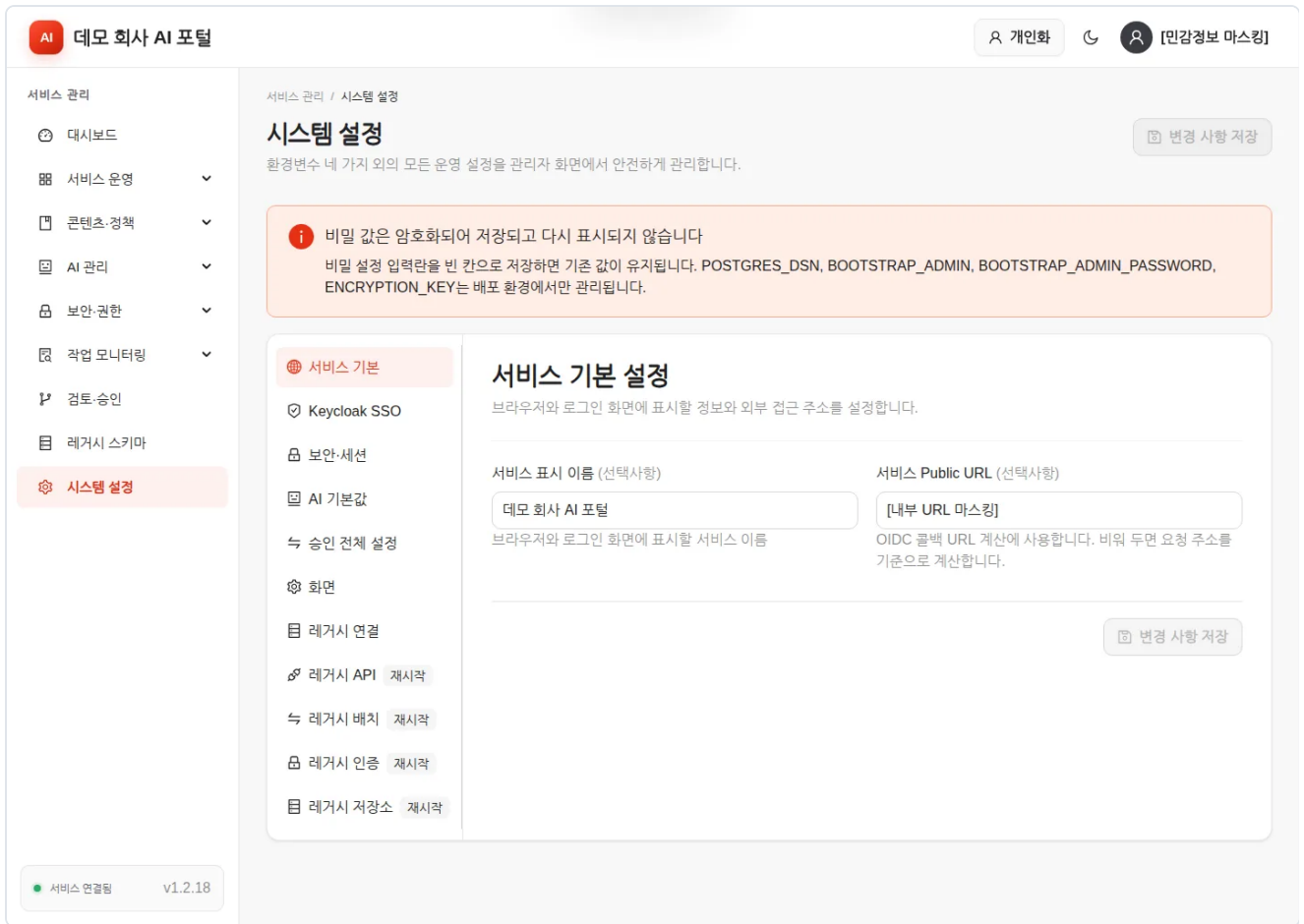
이름	기본값	필수	설명
POSTGRES_DSN	없음	예	레거시 스키마와 ai_admin 스키마가 있는 PostgreSQL DSN. 컨테이너에서 접속 가능해야 함. 예: postgres://ai_admin:CHANGE_ME@postgres.example.com:5432/aiportal?sslmode=require
BOOTSTRAP_ADMIN	없음	예	최초 로컬 서비스 관리자 아이디. 예: admin@example.com
BOOTSTRAP_ADMIN_PASSWORD	없음	예	위 계정의 비밀번호. 12자 이상이어야 하며 미만이면 시작을 거부
ENCRYPTION_KEY	없음	예	저장 비밀값용 AES-256 키. 정확히 32바이트를 표준(또는 패딩 없는) Base64로 인코딩. openssl rand -base64 32

수신 주소는 코드에 :8080 으로 고정되어 있어 환경 변수로 바꿀 수 없습니다. 다른 포트로 노출하려면 컨테이너 포트 매핑 (-p 9090:8080)을 바꾸세요.

네 값 중 하나라도 비어 있으면 로그에 configuration rejected 와 함께 빠진 이름이 나오고 프로세스가 종료됩니다.

3.2 화면에서 관리하는 설정

시스템 설정에서 나머지를 전부 다룹니다. 비밀 설정은 암호화 저장되며 다시 표시되지 않습니다. 비밀 입력란을 빈 칸으로 두고 저장하면 기존 값이 유지됩니다.



시스템 설정 — 서비스 기본 탭과 왼쪽 설정 그룹 목록

그룹	다루는 것
서비스 기본	서비스 표시 이름, 서비스 Public URL(OIDC 콜백 계산 기준)
Keycloak SSO	issuer, client id/secret, scope, 관리자 역할 매핑, HTTP issuer 허용, 저장된 설정 진단
보안·세션	세션 유효 시간(분), HTTPS 전용 쿠키
AI 기본값	기본 공급자, 기본 스트리밍 여부
승인 전체 설정	검토·승인 전역 스위치
화면	기본 테마, 컴팩트 모드
레거시 연결	레거시 스키마 이름
레거시 API / 배치 / 인증 / 저장소	기존 Java YAML 운영 값. 재시작 배지가 붙습니다

레거시 API·배치·인증·저장소 네 그룹은 저장한다고 실행 중인 Java 프로세스에 반영되지 않습니다. 왼쪽 탭에 재시작 배지가 붙고, 화면 제목 옆에 레거시 Java 재시작 필요 표시와 함께 배포 절차 안내가 나옵니다.

시스템 설정 → 서비스 기본에서 서비스 Public URL을 먼저 확인한 뒤, Keycloak SSO에 issuer URL, Client ID, Client Secret, Scopes(최소 openid profile email), 관리자 역할 매핑을 넣습니다. issuer는 discovery 문서를 제공하고 컨테이너에서 달아야 합니다. localhost 가 아닌 HTTP issuer는 HTTP Issuer 허용을 컨 격리 개발망에서만 씁니다.

저장한 뒤 **OIDC 연결 사전 진단** → 저장된 설정 진단을 실행하면 discovery, Authorization·Token·JWKS 엔드포인트, PKCE S256, Client ID·Secret, 콜백 URL, 관리자 역할 매핑을 한 번에 확인합니다. 진단은 의도적으로 무효한 인증 코드를 쓰므로 계정이나 세션을 만들지 않습니다.

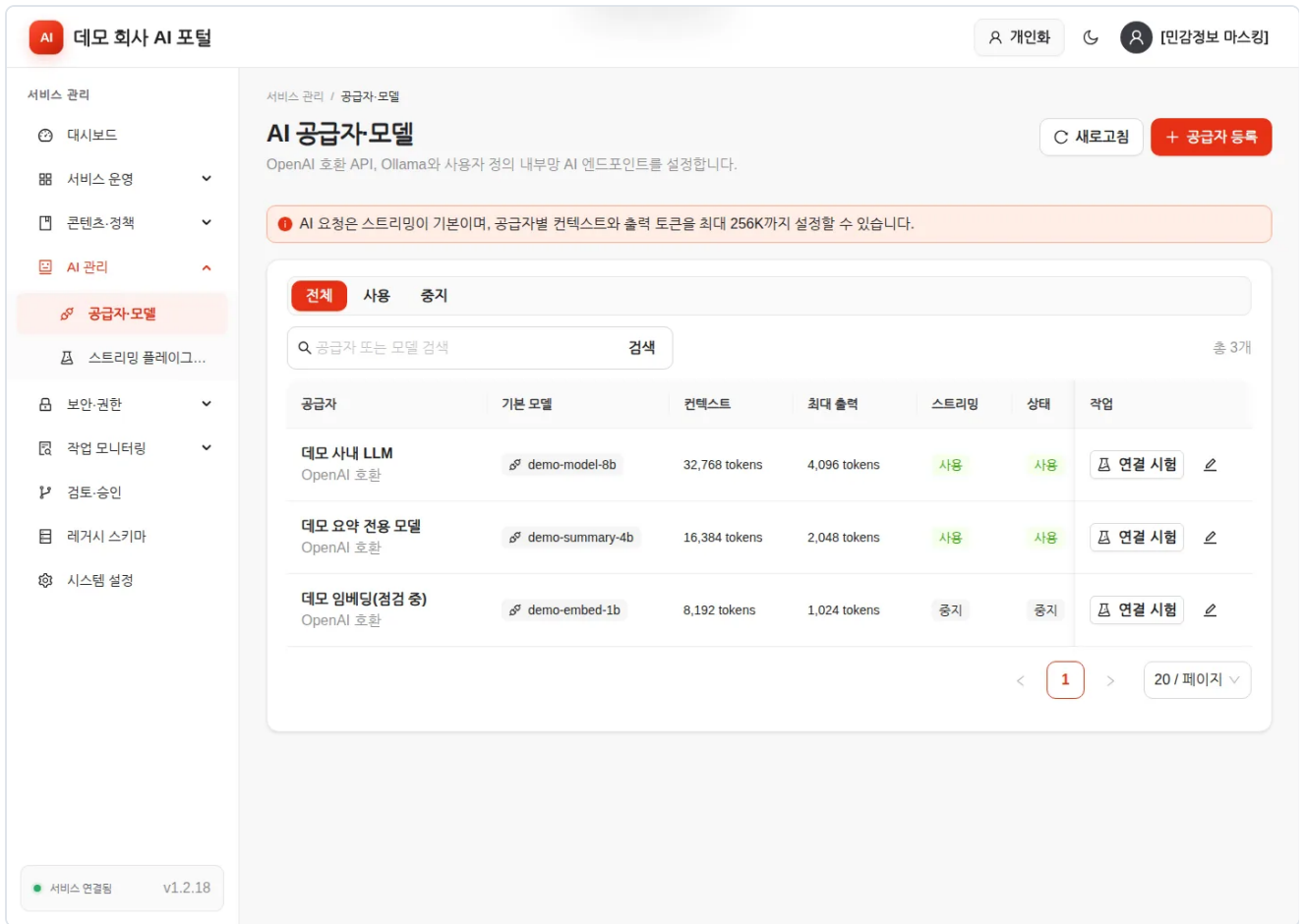
권장 순서

1. 로컬 Bootstrap 세션을 한 브라우저에 열어 둔 채로 진행합니다.
2. 진단이 정상 인지 확인하고, Keycloak의 Valid redirect URI와 화면의 콜백을 비교합니다.
3. 별도 시크릿 창에서 SSO 로그인을 시험합니다.
4. 새 OIDC 사용자의 생성·기본 역할·관리자 역할 매핑을 확인합니다.
5. 실패하면 로그인 화면의 처리 단계와 추적 ID를 감사 로그에서 검색합니다.
6. 필요하면 열어 둔 로컬 세션에서 SSO를 끄고 값을 고칩니다.

HTTPS로 서비스한다면 **보안·세션** → HTTPS 전용 쿠키도 함께 켜세요.

3.4 AI 공급자와 모델

AI 관리 → 공급자·모델에서 등록합니다.



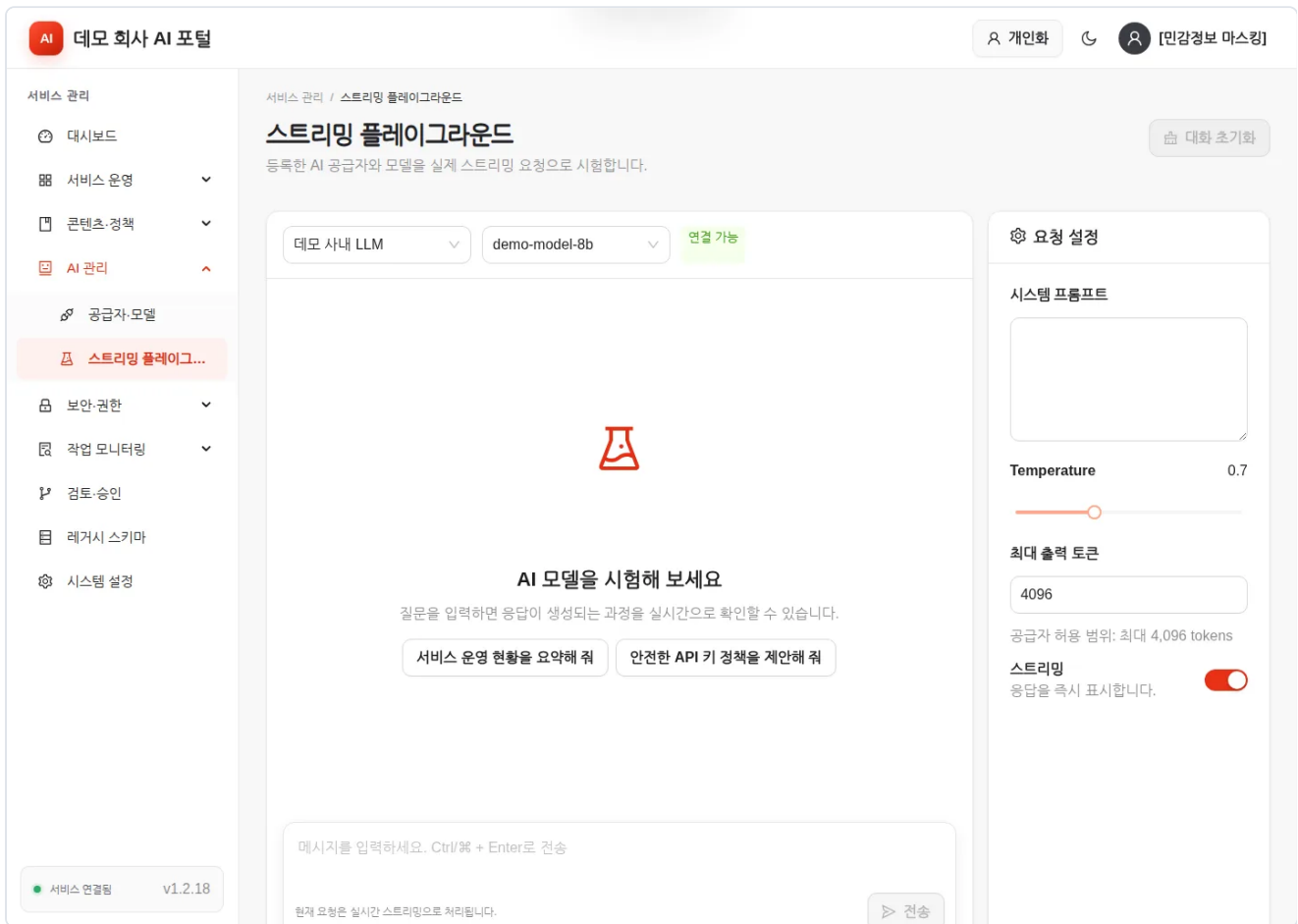
AI 공급자·모델 — 등록된 공급자 목록과 연결 시험 버튼

항목	값
공급자 유형	openai-compatible · ollama · custom
Base URL	내부망 엔드포인트
API 키	선택. 저장 시 암호화되며 목록·상세 응답에 원문이 나오지 않음
기본 모델 / 표시할 모델 목록	허용할 모델 이름
컨텍스트 · 최대 출력 토큰	각각 1 ~ 262,144
기본 스트리밍	요청에 지정이 없을 때의 기본값
요청 제한 시간	1 ~ 3,600초
사용 여부	끄면 요청에 쓰이지 않음

- **연결 시험**은 {Base URL}/v1/models (Base URL이 이미 /v1 로 끝나면 {Base URL}/models)을 호출합니다.
- 수정·삭제는 화면이 마지막으로 읽은 updatedAt 으로 충돌을 확인합니다. 다른 관리자가 먼저 바꿨으면 저장하지 않으니 새로고침한 뒤 최신 값을 검토하세요.
- 기본 공급자는 다른 기본 공급자를 먼저 지정하기 전에는 비활성화·삭제할 수 없습니다.

- 현재 upstream 어댑터는 유형과 무관하게 OpenAI 호환 URL과 Bearer 인증을 씁니다. Azure 전용 `api-version` · `deployment URL` · 별도 헤더가 필요하면 OpenAI 호환 게이트웨이를 앞에 두고 검증하세요.

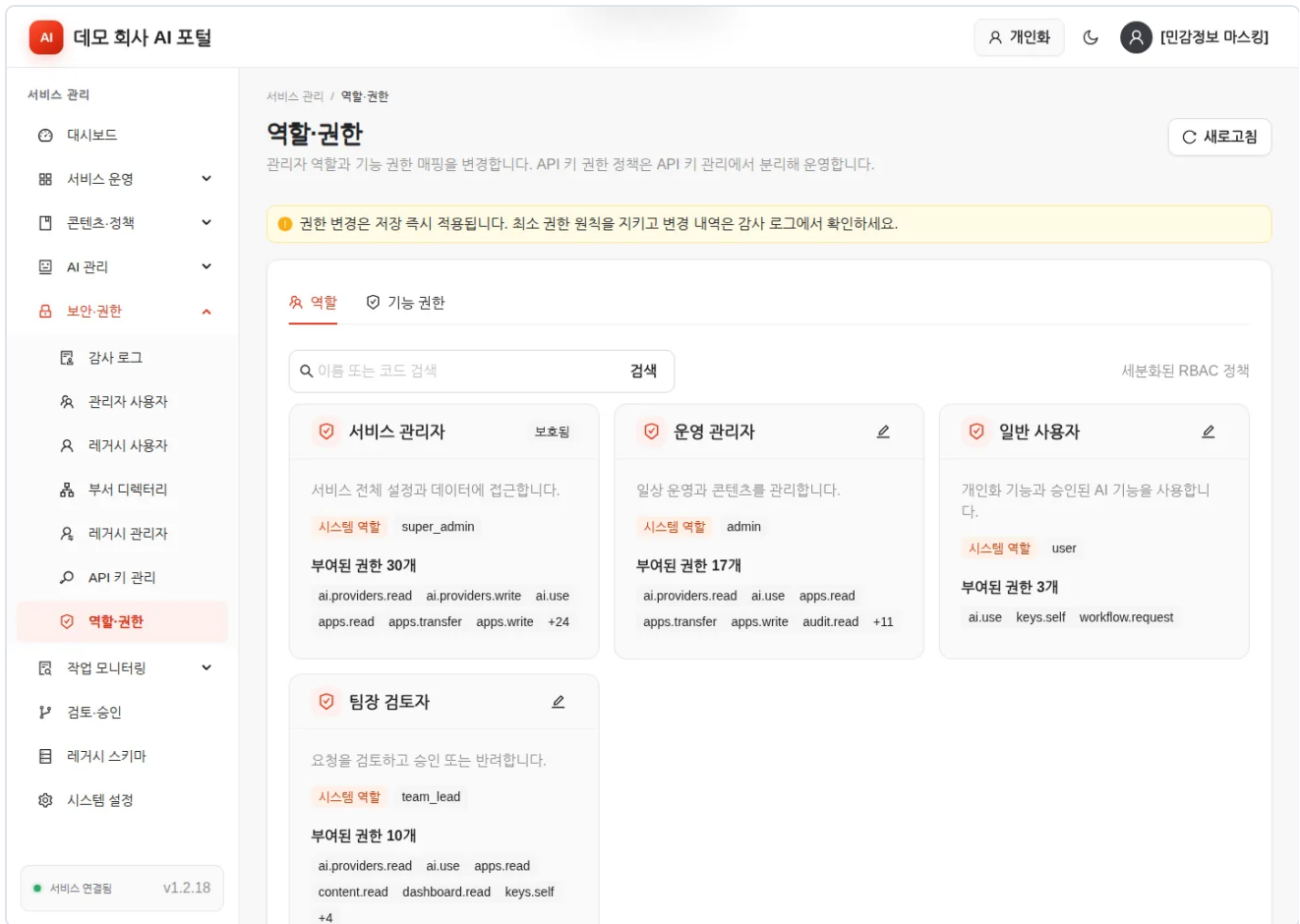
등록한 공급자는 AI 관리 → 스트리밍 플레이그라운드에서 바로 확인할 수 있습니다.



스트리밍 플레이그라운드 — 공급자·모델 선택과 요청 설정

4. 계정과 권한

4.1 기본 역할



역할·권한 — 네 기본 역할과 각 역할에 부여된 권한 수

역할 코드	화면 이름	할 수 있는 일
super_admin	서비스 관리자	서비스 전체 설정과 데이터. 전체 권한을 유지하도록 보호됨(축소 불가)
admin	운영 관리자	일상 운영, 콘텐츠, 통계, 사용자 조회 중심
team_lead	팀장 검토자	요청 검토와 승인·반려
user	일반 사용자	개인화 기능과 승인된 AI 기능

역할·권한 화면의 역할 탭에서 역할별 권한을 조정하고, 기능 권한 탭에서 권한 코드의 의미를 확인합니다. 변경은 저장 즉시 이후 요청의 서버 권한 검사에 반영됩니다.

권한을 나눌 때 지킬 것

- 업무에 필요한 최소 권한만 부여합니다.
- settings.write, roles.manage, keys.manage, schema.read, ai.providers.write 는 서로 분리합니다.
- settings.secrets.manage, settings.export, legacy.sensitive.read 는 목적별 별도 역할에만 둡니다.
- 팀장 검토자에게 workflow.review 를 줍니다.
- 전역 승인 스위치는 settings.write 와 workflow.manage 가 둘 다 있어야 바꿀 수 있습니다. 일반 설정 관리자에게 승인 후회 권한이 따라가지 않게 역할을 분리하세요.
- 바꾼 뒤에는 낮은 권한의 시험 계정으로 메뉴와 API를 확인합니다.

4.2 계정 관리

AI

데모 회사 AI 포털

개인화

로그아웃

민감정보 마스크

서비스 관리

대시보드

서비스 운영

콘텐츠 정책

AI 관리

보안·권한

감사 로그

관리자 사용자

레거시 사용자

부서 디렉터리

레거시 관리자

API 키 관리

역할·권한

작업 모니터링

검토 승인

레거시 스키마

시스템 설정

서비스 관리 / 관리자 사용자

관리자 사용자

신규 ai-admin 사용자 계정과 상태를 관리하고 역할은 역할·권한 화면에서 변경합니다.

새로고침

이름, 아이디 또는 이메일 검색

검색

총 5건

이름	아이디	이메일	인증	레거시 사용자	작업
[표 데이터 마스크]	[표 데이터 마스크]	[표 데이터 마스크]			
[표 데이터 마스크]	[표 데이터 마스크]	[표 데이터 마스크]	SSO	홍길동 [식별자 마스크]	상세 수정
[표 데이터 마스크]	[표 데이터 마스크]	[표 데이터 마스크]	SSO	김서연 [식별자 마스크]	상세 수정
[표 데이터 마스크]	[표 데이터 마스크]	[표 데이터 마스크]	SSO	박민수 [식별자 마스크]	상세 수정
[표 데이터 마스크]	[표 데이터 마스크]	[표 데이터 마스크]	SSO	이지훈 [식별자 마스크]	상세 수정
[표 데이터 마스크]	[표 데이터 마스크]	[표 데이터 마스크]	로컬	[민감정보 마스크] [식별자 마스크]	상세 수정

1-5 / 5건 < 1 > 20 / 페이지

서비스 연결됨

v1.2.18

관리자 사용자 — 인증 방식과 연결된 레거시 사용자

보안·권한 → 관리자 사용자에서 계정 상태(active , locked , disabled)와 역할을 바꿉니다. 지금 로그인한 자기 계정은 스스로 비활성화할 수 없습니다. 인증 방식은 로컬 또는 sso 로 표시되고, 연결된 레거시 사용자도 함께 보입니다.

4.3 API 키와 scope 정책

AI

데모 회사 AI 포털

개인화

[민감정보 마스크]

서비스 관리

대시보드

서비스 운영

콘텐츠 정책

AI 관리

보안·권한

감사 로그

관리자 사용자

레거시 사용자

부서 디렉터리

레거시 관리자

API 키 관리

역할·권한

작업 모니터링

검토·승인

레거시 스키마

시스템 설정

서비스 연결됨

v1.2.18

서비스 관리 / API 키 관리

API 키 관리

새로고침

+ 키 발급

즉시 완료된 발급·회전은 키 원문을 한 번만 표시합니다. 승인 대상 고권한 키는 최종 승인 후 원문을 한 번만 받을 수 있습니다.

전체

활성

회전됨

폐기

만료

키 이름, 접두사 또는 소유자 검색

검색

총 3개

키 이름	소유자	권한 범위	상태	최근 사용	작업
MCP 클라이언트 - 데모 [API 키 마스크] 칭].....	[민감정보 마스크]	ai:chat	활성	-	회전
주간 리포트 배치 [API 키 마스크] 칭].....	[민감정보 마스크]	ai:chat	활성	-	회전
분석 자동화 - 개발 [API 키 마스크] 칭].....	[민감정보 마스크]	ai:chat	활성	-	회전

<

1

>

20 / 페이지

API 키 권한 정책

새로고침

키에 부여할 수 있는 scope의 표시 이름, 개인 선택 가능 여부와 사용 상태를 변경합니다. admin:read, admin:write, legacy:config는 보호된 관리자 전용 scope 이므로 개인 선택을 허용할 수 없습니다.

API 키 관리 — 사용자별 키 목록과 아래쪽 API 키 권한 정책

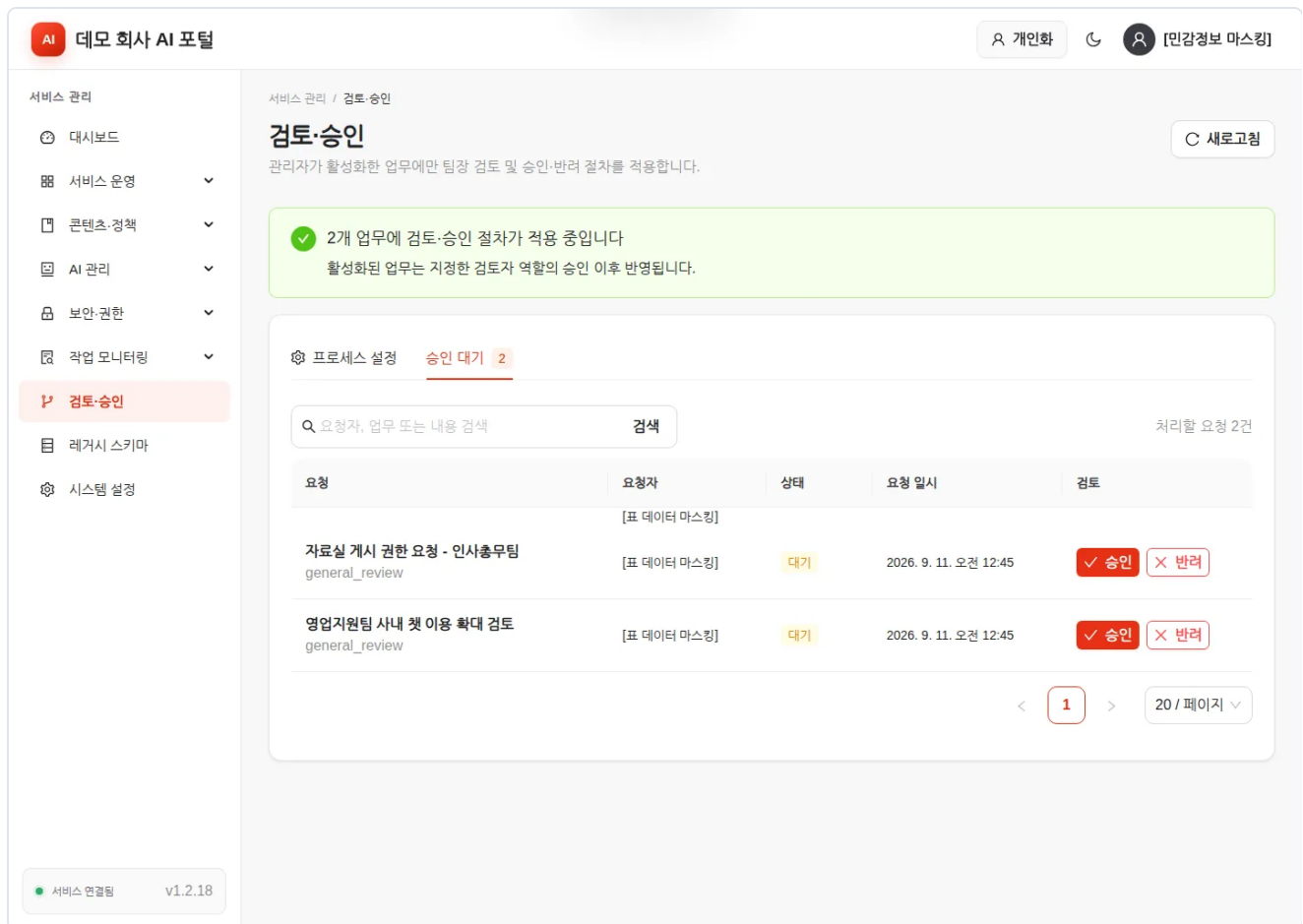
보안·권한 → API 키 관리에서 전체 사용자 키를, 사용자는 개인화 → 내 API 키에서 자기 키를 다룹니다. 발급 절차와 사용자 쪽 안내는 [사용자 가이드](#)에 있습니다.

- 일반 키 회전은 기존 키를 즉시 `rotated` 로 바꾸고 새 원문을 한 번만 표시합니다.
- 고권한 scope가 포함된 키는 `api_key_privileged` 승인이 켜져 있으면 회전도 대기로 전환되고, 최종 승인 전까지 기존 키를 계속 쓸 수 있습니다. 최종 승인 후 기존 키가 폐기되고 새 원문은 요청자가 한 번만 받습니다.
- API 키 권한 정책에서 scope별 표시 이름·설명·개인 선택 가능 여부·사용 여부를 바꿉니다.
- `admin:read` , `admin:write` , `legacy:config` 의 개인 선택 금지는 보호되어 바꿀 수 없습니다.
- `legacy:config` 는 레거시 managed YAML export 전용 관리자 scope입니다. 개인 선택을 허용하지 말고, `settings.export` 역할 권한이 있는 배포 자동화 전용 계정·키에만 최소 기간으로 부여하세요.

4.4 검토·승인 흐름

승인은 두 스위치가 모두 켜져야 적용됩니다.

- 시스템 설정의 전역 `workflow.enabled`
- 검토·승인 → 프로세스 설정의 개별 정책 `enabled`



검토·승인 — 적용 중인 업무 수와 승인 대기 목록

기본 정책

코드	대상
api_key_privileged	관리자 전용 scope를 가진 키의 발급·회전
ai_provider_change	AI 공급자 생성·수정·삭제
legacy_data_change	허용된 레거시 리소스 변경
legacy_runtime_config	레거시 Java 재시작형 설정 게시
general_review	별도 작업을 실행하지 않고 기록만 남기는 일반 운영 검토

앞의 네 실행형 정책은 대상 작업을 승인 대기로 바꾸고, 최종 승인 후 서버가 실제 작업을 실행합니다. 정책마다 승인 단계 (1~3)와 검토 역할을 지정하며, 지정하지 않으면 요청은 승인 단계를 만들지 않고 즉시 우회됩니다.

- 요청자는 자기 요청을 승인할 수 없고, 반려에는 사유가 필요합니다.
- 다단계 승인은 마지막 단계가 끝나야 작업을 실행합니다.
- AI 공급자의 새 API 키와 레거시 비밀번호는 승인 payload와 분리해 암호화 저장하며 검토 화면에 원문으로 노출하지 않습니다.

- 승인 목록의 중첩 payload도 비밀번호·secret·token은 항상 가립니다. 레거시 본문·사용자 ID·IP·경로는 기본 마스킹되고, `legacy.sensitive.read` 가 있는 검토자만 원문을 볼 수 있으며 그 조회 자체가 감사됩니다.
- 승인 스위치를 끄더라도 이미 대기 중인 요청은 취소되지 않습니다. 먼저 목록을 승인 또는 반려로 정리하세요.

5. 운영

5.1 상태 점검

경로	메서드	DB 필요	의미
<code>/health/live</code>	GET · HEAD	아니요	프로세스가 HTTP 요청을 처리하는지
<code>/health/ready</code>	GET · HEAD	예	PostgreSQL ping까지 성공해 트래픽을 받을 준비가 됐는지
<code>/api/v1/health/live</code>	GET · HEAD	아니요	위와 동일 (API 접두사 경로)
<code>/api/v1/health/ready</code>	GET · HEAD	예	위와 동일 (API 접두사 경로)
<code>/api/v1/meta</code>	GET · HEAD	아니요	빌드 버전·commit·빌드 시각
<code>/api/v1/openapi.json</code>	GET · HEAD	아니요	OpenAPI 문서

`ready` 를 readiness probe로, `live` 를 liveness probe로 씁니다. 위 경로는 모두 HEAD도 받으므로 HEAD로 확인하는 가동 감시 도구나 로드 밸런서를 그대로 연결할 수 있습니다.

5.2 로그

Go 서버는 stdout에 JSON 구조 로그를 씁니다. HTTP 로그에는 method, path, status, byte 수, 소요 시간, request ID가 들어갑니다. 컨테이너 런타임에서 rotation과 보존 기간을 정하세요.

```
docker logs --tail 100 ai-admin
docker logs --since 30m ai-admin
docker logs --follow ai-admin
```

조사 목적이라도 민감정보를 로그로 복사하지 말고, 오류 응답의 내부 세부사항은 외부 티켓에 올리기 전에 가리세요.

5.3 감사

AI

데모 회사 AI 포털

개인화

민감정보 마스크

서비스 관리

대시보드

서비스 운영

콘텐츠 정책

AI 관리

보안·권한

감사 로그

관리자 사용자

레거시 사용자

부서 디렉터리

레거시 관리자

API 키 관리

역할·권한

작업 모니터링

검토·승인

레거시 스키마

시스템 설정

서비스 연결됨

v1.2.18

서비스 관리 / 감사 로그

감사 로그

ai-admin의 로그인, 권한, 키, 설정, 승인과 관리 변경을 원자적 감사 이벤트로 추적합니다.

새로고침

CSV 내보내기

전체

성공

실패

거부

사용자, 작업, 결과 또는 IP 검색

검색

총 200건

행위자	계정	작업	리소스	대상 ID	결과	작업
[표 데이터 마스크]	[표 데이터 마스크]			[표 데이터 마스크]		
[표 데이터 마스크]	[표 데이터 마스크]	legacy.sensitive.read	admin_resource	[표 데이터 마스크]	SUC	상세
[표 데이터 마스크]	[표 데이터 마스크]	legacy.sensitive.read	admin_resource	[표 데이터 마스크]	SUC	상세
[표 데이터 마스크]	[표 데이터 마스크]	legacy.sensitive.read	admin_resource	[표 데이터 마스크]	SUC	상세
[표 데이터 마스크]	[표 데이터 마스크]	legacy.sensitive.read	admin_resource	[표 데이터 마스크]	SUC	상세
[표 데이터 마스크]	[표 데이터 마스크]	legacy.sensitive.read	admin_resource	[표 데이터 마스크]	SUC	상세
[표 데이터 마스크]	[표 데이터 마스크]	legacy.sensitive.read	admin_resource	[표 데이터 마스크]	SUC	상세
[표 데이터 마스크]	[표 데이터 마스크]	legacy.sensitive.read	admin_resource	[표 데이터 마스크]	SUC	상세
[표 데이터 마스크]	[표 데이터 마스크]	legacy.sensitive.read	admin_resource	[표 데이터 마스크]	SUC	상세
[표 데이터 마스크]	[표 데이터 마스크]	legacy.sensitive.read	admin_resource	[표 데이터 마스크]	SUC	상세

감사 로그 — 결과별 탭, 검색, CSV 내보내기

로그인·로그아웃, 설정·공급자·키·역할·사용자·승인 변경, 권한 거부와 AI 호출이 감사 이벤트로 남습니다. **보안·권한** → **감사 로그**에서 검색어·결과·시작·종료 시각으로 거르고, `audit.export` 권한이 있으면 현재 필터를 그대로 CSV로 내보냅니다. SSO 실패는 처리 단계·실패 코드·HTTP 추적 ID를 별도 컬럼으로 보여 주므로 로그인 화면의 추적 ID로 바로 검색할 수 있습니다.

5.4 백업과 복구

반드시 함께 보호할 것

- PostgreSQL의 `ai_admin` 스키마
- 실제 운영 대상인 레거시 스키마
- `ENCRYPTION_KEY` 의 원본 32바이트 값
- 배포에 쓴 이미지 아카이브와 `SHA256SUMS`
- 릴리즈 버전과 운영 설정 변경 기록

```
pg_dump --format=custom --schema=ai_admin --file=ai-admin-schema.dump "$POSTGRES_DSN"
```

위 명령은 셸 기록과 프로세스 목록에 DSN을 노출할 수 있습니다. 운영에서는 `.pgpass` , 단기 credential 또는 승인된 백업 에이전트를 쓰세요. 복구는 별도 DB에서 먼저 연습하고, 암호화 키가 맞는지 OIDC secret과 AI 공급자 연결 시험으로 확인합니다.

ENCRYPTION_KEY 를 잃으면 저장된 비밀값을 복호화할 방법이 없습니다. OIDC client secret과 공급자 API 키를 모두 다시 입력해야 합니다.

5.5 업그레이드와 되돌리기

1. 새 릴리즈의 tarball과 체크섬을 반입합니다.
2. 기존 DB와 암호화 키를 백업합니다.
3. staging 복제본에서 migration과 핵심 경로를 검증합니다.
4. 새 이미지를 load하고 태그를 확인합니다.
5. compose.offline.yml 의 이미지 버전을 새 값으로 바꿉니다.
6. 컨테이너를 재생성하고 readiness, 로그인, 설정 복호화, AI 스트리밍을 확인합니다.

```
sha256sum -c SHA256SUMS
gzip -dc ai-admin-v1.2.18.tar.gz | docker load
docker image inspect ai-admin:v1.2.18 --format '{{.RepoTags}}'
docker compose --env-file .env -f compose.offline.yml up -d --force-recreate
```

되돌리는 법: migration은 시작할 때 전진 적용만 하며 자동 down migration은 없습니다. downgrade하려면 이전 이미지뿐 아니라 **그 버전과 호환되는 DB 백업**도 함께 준비해야 합니다. 이전 이미지만 되돌리면 새 스키마 위에서 뜨게 되므로 안전하지 않습니다.

종료는 다음과 같이 합니다. SIGTERM을 받으면 새 요청을 중단하고 최대 20초 동안 정상 종료를 시도합니다. 같은 명령으로 PostgreSQL까지 내리지 마세요.

```
docker compose -f compose.offline.yml stop ai-admin
```

5.6 정기 점검

- **매일:** readiness, 오류율, AI 공급자 상태, 승인 대기 건수
- **매주:** 감사 이벤트와 legacy.sensitive.read 사용, 비활성 사용자, 만료 예정 키, DB 용량

작업 모니터링 메뉴로 레거시 쪽 작업 실패도 함께 봅니다.

AI 데모 회사 AI 포털

개인화

[민감정보 마스크]

서비스 관리

대시보드

서비스 운영

콘텐츠 정책

AI 관리

보안 권한

작업 모니터링

OCR 작업

STT 작업

이미지 생성 작업

배치 오류

검토 승인

레거시 스키마

시스템 설정

서비스 연결됨

v1.2.18

서비스 관리 / 배치 오류

배치 오류 모니터링

새로고침

사용자·부서 동기화와 통계 배치에서 발생한 오류를 개인정보 없이 조회합니다.

Q 부서, 프로젝트 또는 오류 메시지 검색

검색

총 3건

발생 일시	부서	프로젝트	오류 요약	작업
2026. 9. 8. 오후 3:44	인사총무팀	데모 문서 색인	INDEX_LOCKED	상세
2026. 9. 10. 오전 9:44	영업지원팀	데모 통계 집계	STATS_SOURCE_EMPTY	상세
2026. 9. 10. 오후 2:44	AI 플랫폼팀	데모 요약 배치	SUMMARY_TIMEOUT	상세

1~3 / 3건

1

20 / 페이지

배치 오류 모니터링 — 부서·프로젝트별 실패 이력

6. 장애 대응

컨테이너가 뜨자마자 죽는다

`docker logs ai-admin` 의 첫 줄을 봅니다.

로그 메시지	확인할 것
<code>configuration rejected</code>	네 환경 변수 누락, 12자 미만 Bootstrap 비밀번호, 잘못된 Base64 또는 32바이트가 아닌 암호화 키
<code>database startup failed</code>	DNS, 라우팅, PostgreSQL 계정, TLS/DSN
<code>database migration failed</code>	<code>ai_admin</code> 스키마 DDL 권한, 이전에 실패한 트랜잭션
<code>database bootstrap failed</code>	unique 제약, 역할 seed, bcrypt 처리 오류

같은 아이디의 비로컬(OIDC) 계정과 `BOOTSTRAP_ADMIN` 이 충돌해도 시작을 거부합니다.

live 는 되는데 ready 가 503

DB 연결 문제입니다. 풀은 최대 20 · 최소 2 연결을 씁니다. PostgreSQL의 연결 한도와 네트워크 정책을 확인하세요.

로그인이 안 된다

- 계정 상태가 `active` 인지 확인합니다.
- 같은 사용자명의 실패가 반복되면 지수 backoff로 429가 돌아옵니다. `Retry-After` 뒤에 다시 시도하고, 무차별 대입 인지 감사 로그에서 확인합니다.
- 사용자에게 `서비스에 연결할 수 없습니다`가 보인다면 자격 증명 문제가 아니라 인증 조회 자체가 실패한 상태입니다. DB와 readiness를 먼저 봅니다.
- SSO 장에는 로컬 관리자 세션에서 `시스템 설정` → `Keycloak SSO` → `저장된 설정 진단`을 실행합니다. `Client Secret` 실패는 Keycloak confidential client credential을, `Callback URL` 실패는 Valid redirect URI를, `discovery·endpoint` 실패는 사내 CA·DNS·라우팅을 먼저 봅니다.
- 로그인 화면의 `처리 단계`와 `추적 ID`를 감사 로그에서 같은 ID로 검색합니다. 계정 준비 는 사용자 생성·역할 매핑, 토큰 교환 · 토큰 검증 은 `client·code·issuer/JWKS`, 세션 생성 은 계정 상태와 DB session 저장을 조사합니다.
- 복구가 필요하다면 SSO를 켜기 전 확보해 둔 로컬 관리자 세션으로 SSO를 끄고 설정을 되돌립니다.

저장된 비밀값을 쓸 수 없다

최근 배포에서 `ENCRYPTION_KEY` 가 바뀌지 않았는지 확인합니다. 원래 키를 복구할 수 없으면 복호화가 불가능하므로 OIDC client secret과 공급자 API 키를 다시 입력해야 합니다.

AI 응답이 중간에 끊긴다

사용자에게는 ****AI 응답이 완료되기 전에 연결이 끊어졌습니다.****가 보입니다. 서버는 끝까지 전달하지 못한 중계를 감사에 `failure` 와 사유(`upstream_read_failed` , `upstream_timeout` 등)로 남기고 응답을 중단합니다. 확인 순서는 다음과 같습니다.

- 공급자의 제한 시간과 리버스 프록시의 버퍼링·읽기 제한 시간
- upstream 엔드포인트가 실제로 SSE를 지원하는지
- 요청 토큰이 공급자별 최대 출력 토큰 이하인지
- 프록시에서 버퍼링을 끄고 장기 HTTP 응답을 허용했는지

레거시 설정을 저장했는데 Java 동작이 그대로다

- 그 설정의 적용 방식이 `재시작 대기`(`legacy-restart`)인지 확인합니다.
- 승인 정책이 켜져 있으면 요청이 최종 승인됐는지 확인합니다.
- 최신 YAML을 다시 export해 overlay 대상과 Spring 설정 우선순위를 확인합니다.
- Java 프로세스가 실제로 재시작됐는지, 시작 로그의 `profile·schema`를 확인합니다.
- YAML 원문이나 비밀값을 ai-admin 로그·티켓에 붙이지 마세요.

레거시 값이 [MASKED] 로 보인다

민감 필드의 정상 기본 동작입니다. 일반 관제·참조 확인에는 마스킹 상태를 그대로 쓰세요. 원문 확인이 업무상 꼭 필요하다면 보안 승인 후 기간을 제한한 `legacy.sensitive.read` 역할을 부여하고 작업 직후 회수한 다음, 감사 로그의 `legacy.sensitive.read` 이벤트를 확인합니다. 도메인 `allowlist`에서 제외된 원문은 이 권한으로도 반환되지 않습니다.

목록 저장이 409 충돌로 거부된다

레거시 관리 화면의 수정·삭제는 목록에서 읽은 32자 `_rowVersion` 으로 동시 변경을 확인합니다. 제출을 반복하지 말고 새 로고침한 뒤 최신 row를 검토하세요. AI 공급자 화면도 같은 원리로 `updatedAt` 을 비교합니다.

새로고침하면 404가 난다

리버스 프록시가 SPA fallback을 ai-admin으로 전달하는지 확인합니다. 서버는 알 수 없는 경로를 SPA로 넘겨주므로, 프록시가 먼저 404를 만들고 있는지 봅니다.

7. 보안

7.1 배포 직후 바뀌야 하는 기본값

항목	기본값	조치
<code>BOOTSTRAP_ADMIN_PASSWORD</code>	없음(직접 지정)	<code>.env.example</code> 의 예시 문자열을 그대로 쓰지 말고 12자 이상 무작위 값으로
<code>ENCRYPTION_KEY</code>	없음(직접 지정)	<code>openssl rand -base64 32</code> 로 새로 만들고 별도 보관
보안·세션 → HTTPS 전용 쿠키	꺼짐	HTTPS 운영이면 켜다
Keycloak SSO → HTTP Issuer 허용	꺼짐	운영에서는 끈 채로 둔다
승인 전체 설정	꺼짐	고권한 키·공급자 변경에 검토가 필요하다면 켜다
세션 유효 시간	480분	조직 정책에 맞게 조정(15~10080분)

7.2 외부에 열면 안 되는 것

- 외부에 노출할 것은 리버스 프록시를 통한 `8080/tcp` 하나뿐입니다. PostgreSQL, Keycloak, AI 공급자 엔드포인트는 내부망에 둡니다.
- `/mcp` 와 `/v1/chat/completions` 는 API 키로 인증합니다. 인터넷에 그대로 열지 마세요.
- `/api/v1/settings/legacy/application-managed.yaml` 은 비밀값을 포함할 수 있으므로 배포 자동화 전용 키에만 허용합니다.

7.3 인증과 세션

- 브라우저 세션은 HttpOnly 세션 쿠키와 별도 CSRF 쿠키를 함께 씁니다. 변경 요청에는 `X-CSRF-Token` 헤더가 필요합니다.
- API 키 인증은 `Authorization: Bearer aia_...` 이며 변경 요청에는 `admin:write` scope가 추가로 필요합니다.
- 인증 조회 자체가 실패하면 401이 아니라 `Retry-After` 가 붙은 503으로 답합니다. 유효한 세션이 DB 장애 때문에 만료된 것처럼 보이지 않게 하기 위한 것입니다.
- 컨테이너는 `read_only` · `cap_drop: ALL` · `no-new-privileges` 로 씁니다. 이 설정을 풀지 마세요.

7.4 레거시 데이터 취급

- 민감 컬럼은 기본적으로 `[MASKED]` 로 표시되고 검색도 마스킹된 projection만 씁니다.
- 원문 조회에는 별도 `legacy.sensitive.read` 권한이 필요하며 조회 자체가 감사됩니다. 일시 부여 후 회수하세요.
- 레거시 스키마 이름은 `app_info` · `system_policy` · `user_info` 가 모두 있는 전용 스키마만 받습니다.
`ai_admin` · `information_schema` · `pg_*` 는 거부하고, 운영 중 핵심 테이블이 사라지면 fingerprint를 다시 검사해 503으로 fail-closed 처리합니다.
- 제공된 `aiportal_schema_ddl_with_data.sql` 에는 실제 식별자·내부 주소·업무 원문이 들어 있을 수 있습니다. 운영 화면·테스트·캡처·Git·릴리즈에 복사하지 마세요.

전체 보안 모델은 [보안 가이드](#)에 있습니다.

화면 캡처를 다시 만들 때

이 문서와 사용자 가이드의 캡처는 저장소의 캡처 도구로 만듭니다. **운영 DB가 아닌 합성 DB로 찍은 ai-admin**만 대상으로 삼으세요. 도구는 기본적으로 localhost만 허용하고 `SCREENSHOT_DATA_MODE=synthetic` 확인이 없으면 시작하지 않으며, 화면에 오류가 하나라도 있으면 결과를 남기지 않고 실패합니다. 자세한 사용법과 생성 파일 목록은 [docs/screenshots/README.md](#)에 있습니다.

함께 보기

- [사용자 가이드](#)
- [운영 가이드](#) · [보안 가이드](#)
- [REST·AI API](#) · [MCP](#)
- [아키텍처](#) · [레거시 관리 설계](#) · [레거시 기능 대조 점검](#) · [데이터베이스 호환성](#)