

moyro

관리자 가이드

설치·설정·운영과 장애 대응

버전 v0.2.27

작성일 2026-09-10

문서 관리자 가이드

moyro 관리자 가이드

대상 버전: **v0.2.27** · 이 문서는 저장소 정본입니다. PDF: [ADMIN_GUIDE.pdf](#)

화면을 쓰는 쪽 내용은 [사용자 가이드](#)에 있습니다. 같은 내용을 두 번 쓰지 않고 필요한 곳에서 가리킵니다. 오프라인 설치의 더 자세한 절차는 [오프라인 배포](#)에 있습니다.

이 문서의 화면 캡처는 v0.2.27 이미지를 실제로 띄워 브라우저로 찍은 것입니다. 캡처에 보이는 계정·주소·값은 모두 검증용 가짜 데이터입니다.

1. 구성 요소

moyro는 애플리케이션 컨테이너 한 개 + 외부 PostgreSQL로 동작합니다. 웹 UI는 같은 이미지 안에 들어 있어 별도 웹 서버가 필요 없습니다.

구성 요소	형태	필수	하는 일
moyro 애플리케이션	Docker 이미지 moyro:v0.2.27	필수	HTTP API(/api/v4 , /api/moyro/v1), WebSocket, 웹 UI 정적 파일, 백그라운드 워커
PostgreSQL	조직이 운영하는 외부 서비스	필수	모든 상태. 메시지, 사용자, 설정, 작업/결정, 알림함, 감사 로그
데이터 볼륨 moyro-data	Docker 볼륨 → /var/lib/moyro	필수	업로드 파일(files/)과 플러그인(plugins/)
리버스 프록시	조직 표준	권장	TLS 종료. moyro 자체는 평문 HTTP로 8065를 듣습니다
Keycloak	외부 OIDC 공급자	선택	SSO 로그인과 그룹 기반 팀·채널 매핑
OpenAI 호환 AI endpoint	내부 서비스	선택	AI 요약·브리핑·지식 답변

주고받는 것은 다음과 같습니다.

방향	상대	내용
들어옴	브라우저·클라이언트 → :8065	HTTP/WebSocket
들어옴	외부 시스템 → /hooks/{hookID}	Incoming Webhook (인증 없이 URL만으로 POST)
나감	moyro → PostgreSQL	모든 상태 읽기/쓰기
나감	moyro → Outgoing Webhook 대상	허용 목록에 넣은 host 만
나감	moyro → Keycloak / AI endpoint	컨 경우에만

v0.2.27이 지원하지 않는 것을 먼저 확인하세요. 애플리케이션 컨테이너 다중 복제, Redis fan-out, S3 파일 저장, SMTP 발송, 외부 링크 미리보기는 이 릴리즈의 범위 밖입니다. 파일은 로컬 볼륨에 저장됩니다.

2. 설치

릴리즈 자산으로 처음부터 끝까지 따라가는 절차입니다. 인터넷이 없는 망을 기준으로 합니다.

2.1 이미지 가져오기

릴리즈 아카이브를 조직의 승인된 매체로 옮긴 뒤 릴리즈 노트의 SHA-256과 비교합니다.

```
sha256sum moyro-v0.2.27.tar.gz
docker load --input moyro-v0.2.27.tar.gz
docker image inspect moyro:v0.2.27
```

지원 플랫폼은 linux/amd64 입니다.

2.2 PostgreSQL 준비

전용 데이터베이스와 최소 권한 계정을 만듭니다. 이 계정은 기동 시 스키마 마이그레이션을 적용해야 하므로 테이블 생성·변경 권한이 필요합니다. PostgreSQL 트래픽은 보호된 내부망 안에 두세요.

2.3 환경 파일

애플리케이션이 환경 변수에서 읽는 값은 정확히 네 개입니다. 나머지 설정은 로그인 뒤 관리자 화면에서 저장하며 PostgreSQL에 보관됩니다.

```
POSTGRES_DSN=postgres://moyro:replace-me@postgres.internal:5432/moyro?sslmode=require
BOOTSTRAP_ADMIN=admin@example.internal
BOOTSTRAP_ADMIN_PASSWORD=replace-with-12-to-72-byte-secret
ENCRYPTION_KEY=replace-with-standard-base64-for-32-random-bytes
```

암호화 키는 신뢰할 수 있는 관리 워크스테이션에서 만듭니다.

```
openssl rand -base64 32
```

파일은 데이터 볼륨 밖에 두고 권한을 줍니다.

```
chmod 600 /etc/moyro/moyro.env
```

2.4 실행

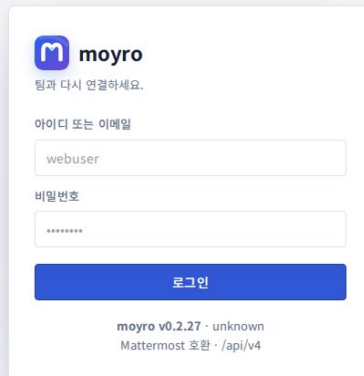
```
docker volume create moyro-data

docker run -d \
  --name moyro \
  --restart unless-stopped \
  --read-only \
  --tmpfs /tmp:rw,noexec,nosuid,size=64m \
  --cap-drop ALL \
  --security-opt no-new-privileges \
  --env-file /etc/moyro/moyro.env \
  --mount type=volume,src=moyro-data,dst=/var/lib/moyro \
  --publish 8065:8065 \
  moyro:v0.2.27
```

2.5 기동 확인과 최초 관리자

```
curl --fail http://127.0.0.1:8065/healthz
docker logs --tail 100 moyro
```

브라우저로 `http://<서버>:8065/` 를 열고 `BOOTSTRAP_ADMIN` 계정으로 로그인합니다. 부트스트랩은 **사용자가 한 명도 없을 때만** 관리자 계정을 만들며, 재기동해도 기존 비밀번호를 덮어쓰지 않습니다.



로그인 화면 — 아래쪽에 배포된 서비스 버전이 표시된다

로그인 화면 아래에 보이는 버전이 배포한 태그와 같은지 확인하세요.

2.6 포트·볼륨·자원

항목	값	비고
컨테이너 포트	8065/tcp	HTTP + WebSocket. 리버스 프록시 뒤에 두세요
볼륨	moyro-data → /var/lib/moyro	files/ (업로드), plugins/ (플러그인)
실행 사용자	65532:65532 (non-root)	이미지는 distroless
파일시스템	--read-only + /tmp tmpfs	볼륨만 쓰기 가능
PostgreSQL	외부 5432	마이그레이션 권한 필요

3. 설정

3.1 환경 변수 전수 표

이 넷이 전부입니다. 하나라도 비면 기동이 중단되고 `config: missing required environment variables: ...` 로 끝납니다.

이름	기본값	필수	설명
POSTGRES_DSN	없음	필수	PostgreSQL 연결 문자열. 파싱할 수 없으면 기동 중단(<code>config: invalid POSTGRES_DSN</code>).
BOOTSTRAP_ADMIN	없음	필수	최초 system admin 이메일. 이름 없는 순수 주소여야 합니다(<code>config: BOOTSTRAP_ADMIN must be a plain email address</code>).
BOOTSTRAP_ADMIN_PASSWORD	없음	필수	최초 생성에만 쓰는 12 - 72바이트 비밀번호. 범위를 벗어나면 기동 중단.
ENCRYPTION_KEY	없음	필수	32바이트 키의 표준 base64. 저장 secret 보호와 세션 서명 키 유도에 씁니다. 전부 0인 키는 거부합니다.

`ENCRYPTION_KEY` 는 바꾸거나 잃어버리면 암호화된 설정과 자격 증명을 다시 읽을 수 없습니다. 이 릴리즈에는 온라인 루트 키 재암호화 절차가 없습니다. 인스턴스마다 고정하고 데이터 백업과 분리해서 보관하세요.

고정된 런타임 기본값(환경 변수로 바꿀 수 없습니다):

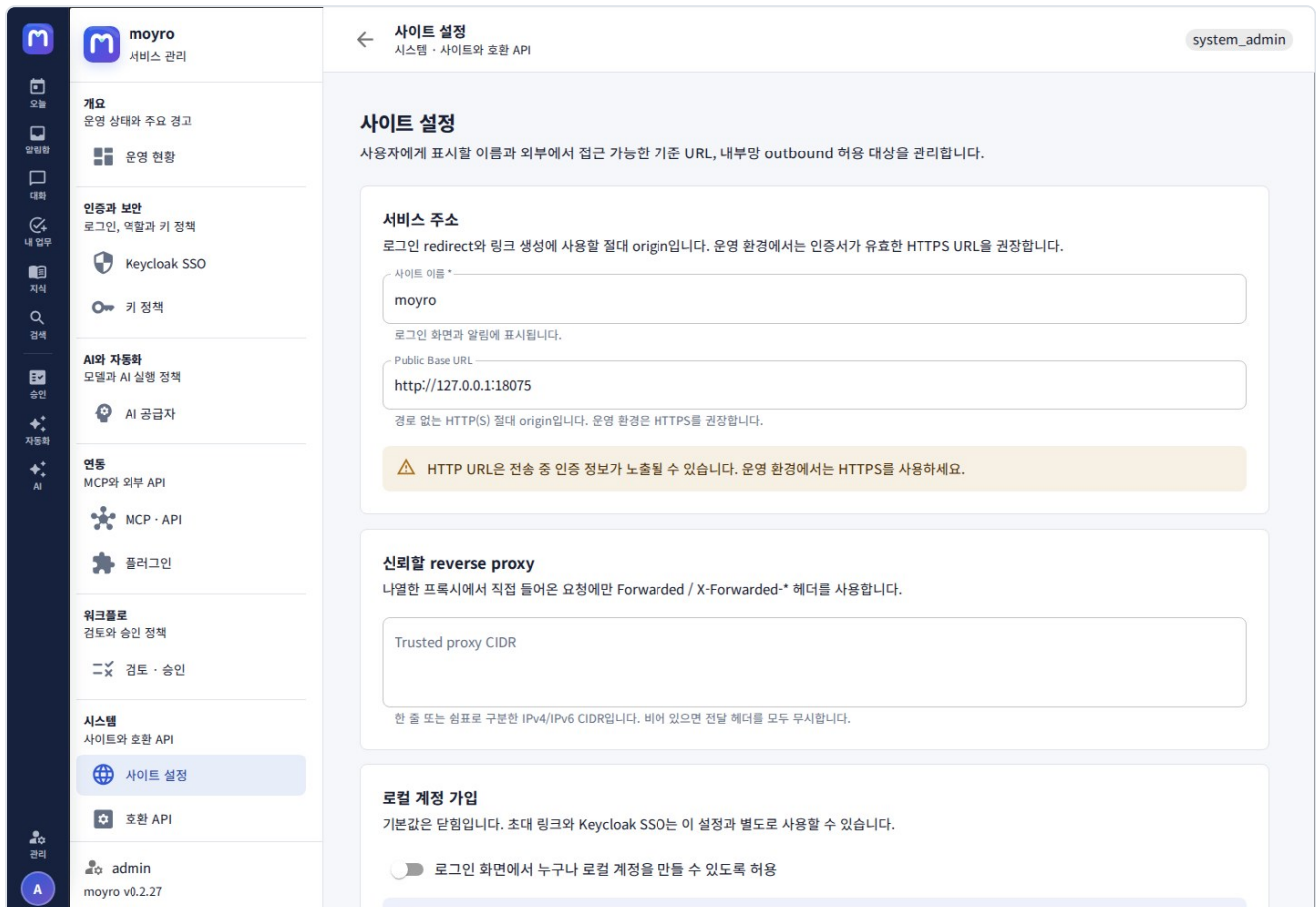
항목	값
Listen 주소	<code>:8065</code>
플러그인 디렉터리	<code>/var/lib/moyro/plugins</code>
파일 저장 경로	<code>/var/lib/moyro/files</code>
세션 TTL	24시간
파일 백엔드	로컬 파일시스템
외부 링크 미리보기	꺼짐

3.2 관리자 화면

프로필 메뉴의 서비스 관리로 들어갑니다. 권한이 있는 사용자에게만 보입니다. 왼쪽 메뉴는 다음과 같이 묶여 있습니다.

운영 현황은 애플리케이션, PostgreSQL(pool·migration), Worker, Webhook 전달, 파일 저장소, 인증, AI, MCP, 승인, 이메일 알림 카드를 실제 조회값으로 채웁니다. 각 카드에는 **정상 · 확인됨 · 미확인 · 미설정 · 비활성** 배지가 붙습니다. heartbeat나 연결 확인을 얻을 수 없는 항목은 정상으로 추정하지 않고 **미확인**으로 표시합니다 — 화면 설명 그대로 "표시되지 않는 지표를 정상으로 추정하지 않습니다".

3.3 사이트 설정



사이트 설정 — 사이트 이름·공개 URL·가입·초대·outbound 허용 목록

- **서비스 주소** — **사이트 이름**(로그인 화면과 알림에 표시)과 **Public Base URL** (로그인 redirect와 링크 생성에 쓰는 절대 origin)입니다. 경로 없는 HTTPS origin을 권장하며, HTTP를 넣으면 화면이 경고합니다. Keycloak을 컨 동안에는 비울 수 없습니다.
- **신뢰할 reverse proxy** — **Trusted proxy CIDR** 칸에 moyro로 직접 들어오는 프록시 주소만 한 줄 또는 침표로 구분해 넣습니다(IPv4/IPv6 CIDR). 비어 있으면 전달 헤더를 모두 무시합니다. 프록시가 외부에서 온 Forwarded · X-Forwarded-For 를 먼저 제거하도록 구성한 뒤에 저장하세요. 신뢰한 peer에서 온 체인만 오른쪽부터 해석해 감사 로그와 단계별 로그인 rate limit에 원본 IP를 씁니다.
- **로컬 계정 가입** — 기본값은 닫힘입니다. 초대 링크와 Keycloak SSO는 이 설정과 별개로 동작합니다.
- **사용자 초대** — 워크스페이스, 만료 기간, 최대 사용 횟수를 정해 링크를 발급합니다. 외부 협업자는 게스트로 발급해 허용 채널, 접근 만료, 원본 파일 다운로드 허용 여부를 함께 지정합니다.
- **Outbound host allowlist** — Outgoing Webhook이 호출할 hostname 또는 IP만 한 줄씩 넣습니다. scheme·port·path·사용자 정보는 넣지 않습니다. 비어 있으면 outbound callback이 차단되며, HTTP redirect는 다른 목적지로 따라가지 않습니다.

- **메시지 초안 보안** — 브라우저 저장 방식을 local / 현재 세션만 / 저장 안 함 중에서 고릅니다. local 보존 기간은 1 - 30일이고 기본값은 7일입니다. 로그아웃 시 이 기기의 현재 사용자 초안을 지우는 옵션을 권장합니다.

3.4 Keycloak SSO (OIDC)

The screenshot shows the 'Keycloak SSO' configuration page in the 'moyro' system. The page is divided into several sections:

- Keycloak SSO**: Overview section with a description: 'Issuer URL의 OIDC discovery 문서를 이용해 로그인 endpoint와 키를 자동 구성합니다.'
- 연결 정보**: Connection information section. It includes a toggle for 'Keycloak 로그인을 사용합니다' (checked). Fields include 'Issuer URL *', 'Client ID *', 'Client Secret', and 'Callback URL' (with a '복사' button). A note says 'realm까지 포함한 Issuer 또는 discovery 문서 주소를 입력하세요.'
- Claim 매핑**: Claim mapping section. It includes a note: '기본값으로 대부분의 Keycloak realm과 바로 연동됩니다.' Fields include 'Scopes' (with 'openid profile email' selected), 'Username claim' (with 'preferred_username' selected), 'Email claim' (with 'email' selected), and 'Groups claim' (with 'groups' selected). There are also checkboxes for '처음 로그인한 사용자를 자동 생성' (checked) and '검증된 이메일 claim 필수' (checked). A note at the bottom says 'Keycloak ID token의 그룹 백열 claim'.

Keycloak SSO — issuer·client·claim·그룹 매핑 설정

순서가 중요합니다.

1. 사이트 설정에 브라우저가 실제로 쓰는 공개 URL을 먼저 저장합니다.
2. Keycloak에 confidential OIDC client를 만듭니다.
3. realm을 포함한 Issuer URL(또는 정확한 `.well-known/openid-configuration` 주소), Client ID, Client Secret 을 입력합니다.
4. 화면에 표시된 Callback URL을 Keycloak client의 valid redirect URI에 그대로 넣습니다.
5. **연동 확인**으로 OIDC discovery와 JWKS 서명 키를 확인합니다. 이 확인은 client secret이나 redirect 등록까지 검증하지 않으므로 실제 로그인 테스트도 하세요.
6. 기본 scope `openid profile email` 과 `username·email·groups claim`을 확인합니다.
7. 필요하면 그룹 이름을 팀·채널·계정 역할에 매핑합니다. 같은 로그인을 반복해도 멤버십은 중복되지 않고 필요한 것만 추가됩니다. 기존 수동 권한은 제거하지 않습니다.
8. 매핑된 그룹과 매핑되지 않은 그룹의 테스트 사용자로 각각 로그인해 봅니다.

Client Secret은 저장 뒤 다시 표시되지 않으며 새 값으로만 교체합니다.

내부망 조건 — moyro 컨테이너에서 discovery·token·JWKS에 달아야 하고, 사용자 브라우저에서 authorization endpoint에 달아야 합니다. front-channel과 back-channel이 서로 다른 origin이어도 됩니다. HTTPS issuer가 광고하는 HTTP token·JWKS·UserInfo는 기본적으로 거부하며, **신뢰할 수 있는 내부망의 HTTP back-channel 허용**을 켜 경우에만 받아들입니다. 이때 client secret과 authorization code가 평문으로 오갑니다. 브라우저용 authorization endpoint는 이 옵션과 무관하게 HTTPS여야 합니다. Keycloak과 moyro 호스트의 시각도 맞춰야 합니다(내부 NTP).

콜백은 재사용 가능한 세션 토큰을 URL이나 JavaScript 응답에 넣지 않습니다. 5분짜리 브라우저 바인딩 코드를 교환 하면 자격 증명은 HttpOnly·SameSite 쿠키로만 설정됩니다. 응답이 유실되면 같은 브라우저가 60초 안에 재시도해 정확히 같은 세션을 받습니다.

3.5 AI 공급자

The screenshot shows the 'AI 공급자' (AI Provider) configuration page in the moyro interface. The left sidebar lists various system components like '개요' (Overview), '인증과 보안' (Authentication and Security), 'AI와 자동화' (AI and Automation), '연동' (Integration), '워크플로' (Workflow), and '시스템' (System). The main content area is titled 'AI 공급자' and includes a subtitle 'AI와 자동화 · 모델과 AI 실행 정책'. The '공급자 연결' (Provider Connection) section has a toggle for '서비스에서 AI 기능을 사용합니다' (Use AI features from the service) and fields for '표시 이름' (Display name), 'API 형식' (API type), 'Base URL', and 'API Key'. The 'Streaming과 token' (Streaming and token) section has a toggle for 'Streaming 기본 사용 (필수)' (Use streaming by default (required)) and fields for 'Context window tokens', 'Max output tokens', and 'Timeout (초)'. The 'Context window tokens' field is set to 262144, 'Max output tokens' is set to 16384, and 'Timeout (초)' is set to 120. There are buttons for '연결 확인' (Check connection) and '설정 저장' (Save settings).

AI 공급자 — 내부 endpoint·모델·토큰·타임아웃 설정

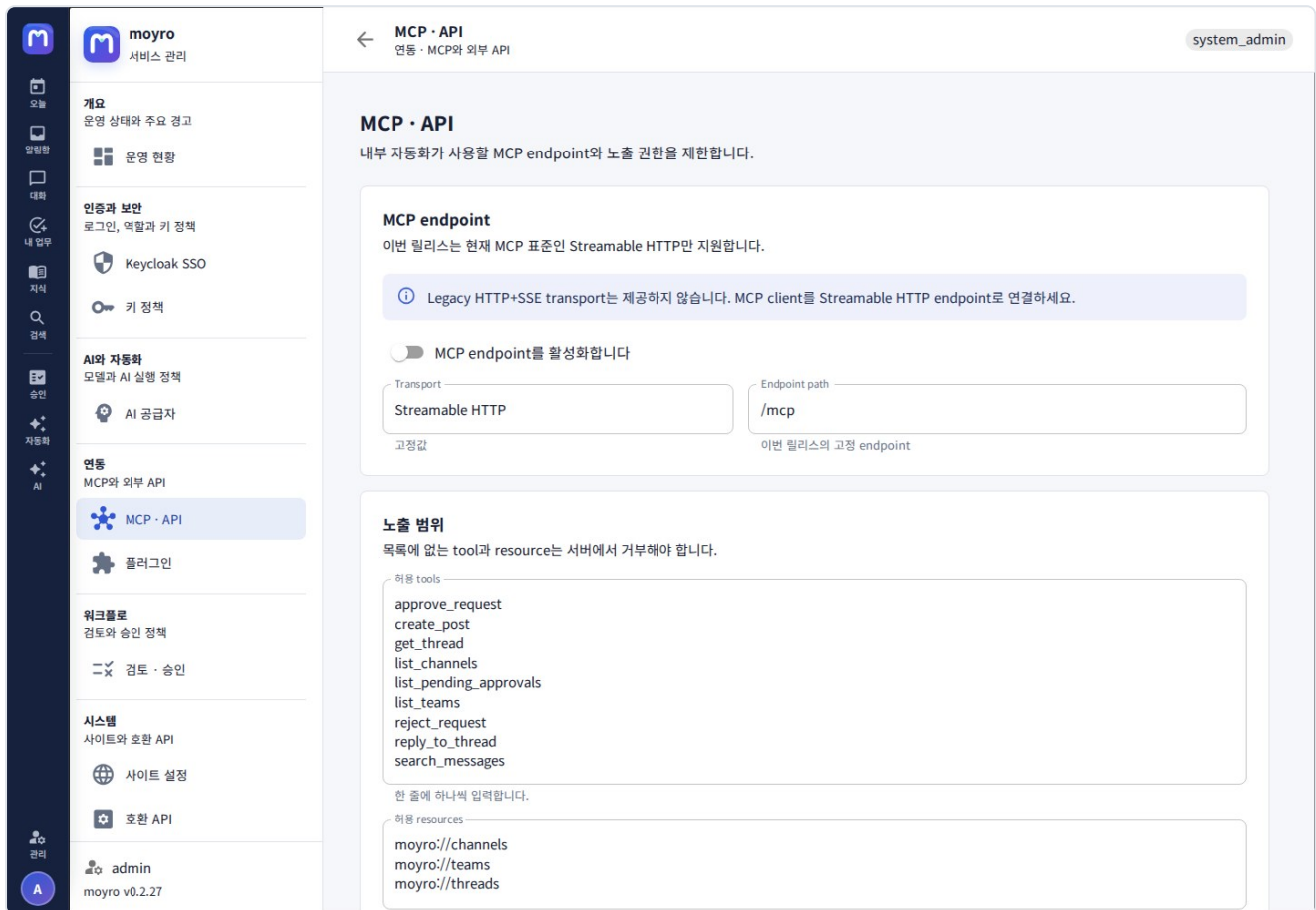
카드의 **공급자 연결**과 **Streaming과 token** 둘입니다. 내부 Base URL, 모델, 선택적 API key를 넣고 **연결 확인** 버튼으로 확인합니다. 외부 인터넷이 없는 배포에서는 내부 endpoint를 쓰세요.

- 응답 스트리밍은 항상 기본으로 켜져 있습니다.
- Context window와 max output은 각각 262,144까지 입력할 수 있지만 실제 모델 한계 안에서 설정해야 합니다.
- Timeout은 5 - 3,600초입니다.

- API key 원문은 저장 뒤 설정 조회에 반환되지 않습니다.

지식 검색의 원문은 PostgreSQL이 현재 팀·채널 멤버십을 먼저 확인한 것만 씁니다. 공급자가 없거나 실패해도 원문 검색과 대화 문서화는 계속 동작합니다.

3.6 MCP · API



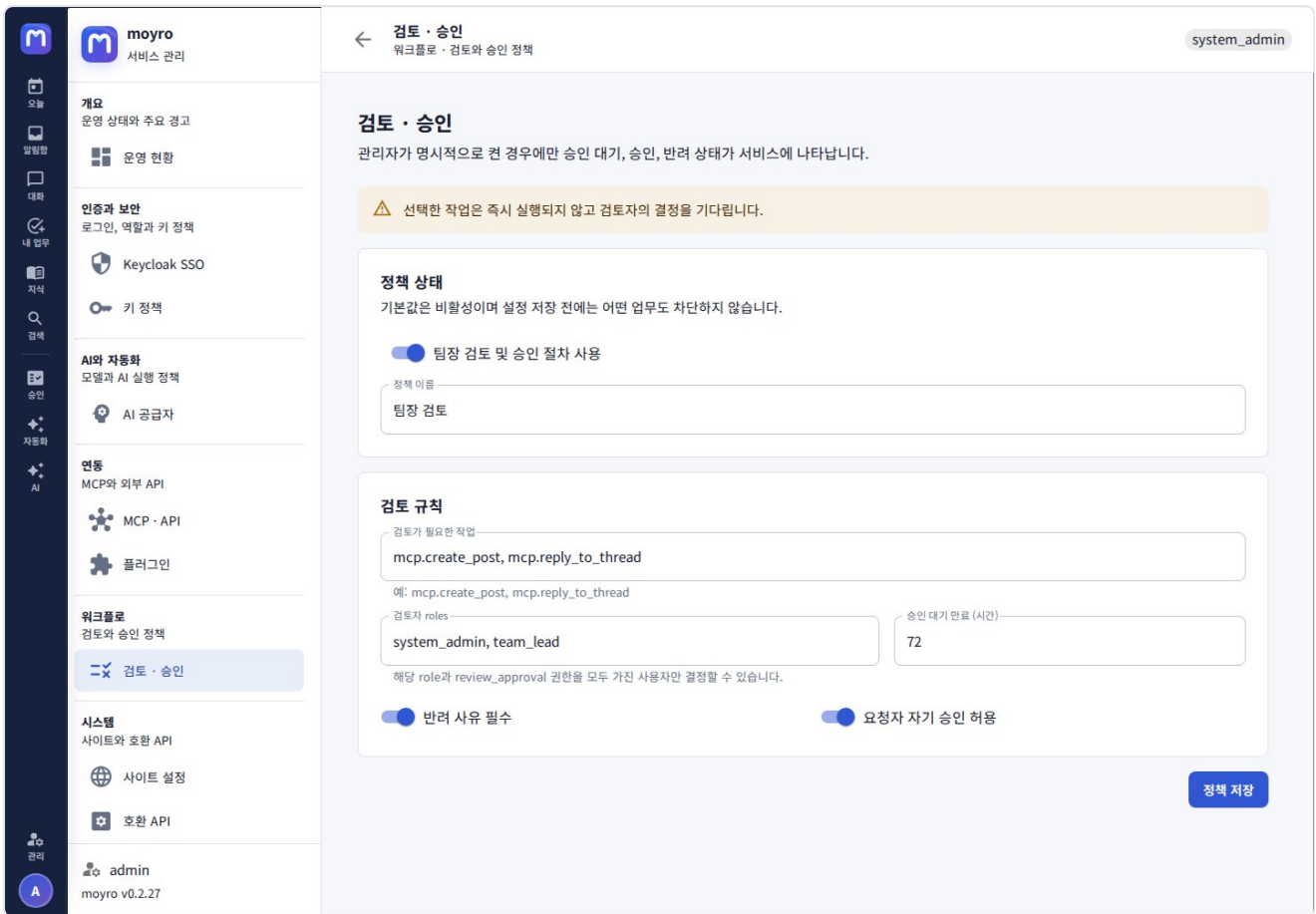
MCP · API — Streamable HTTP endpoint와 허용 범위 설정

카드는 MCP endpoint와 노출 범위 둘입니다.

- endpoint는 `/mcp` 의 stateless Streamable HTTP입니다. legacy HTTP+SSE transport는 제공하지 않습니다.
- 기본값은 비활성입니다. 켜 뒤 허용 tool, resource URI prefix, 필요한 key scope를 최소 범위로 지정합니다.
- 클라이언트는 `kind=mcp` 개인 키를 씁니다. 목록에 없는 tool·resource는 서버가 거부하고, 팀·채널 멤버십과 키의 resource 제약도 함께 적용됩니다.
- 비활성 상태에서 접근하면 MCP transport가 비활성화되어 있습니다. 가 표시됩니다.

API 계약은 두 벌입니다. Mattermost 호환 `/api/v4` 는 `openapi-v4.yaml` , moyro 전용 `/api/moyro/v1` 은 `openapi-moyro.yaml` 에 있습니다.

3.7 검토 · 승인

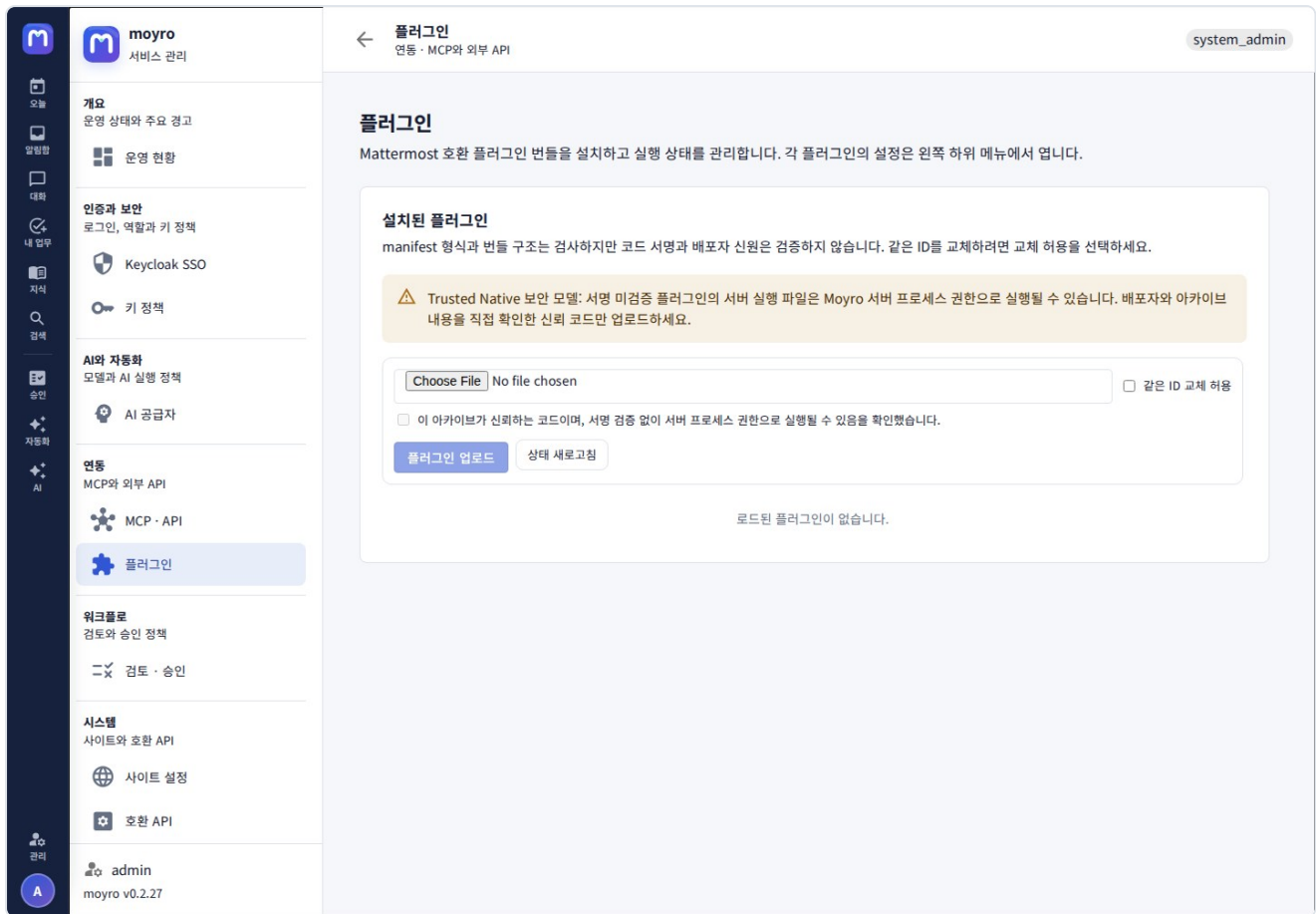


검토 · 승인 — 보호 작업과 검토자 역할 정책

카드는 **정책 상태**와 **검토 규칙** 둘입니다. 기본값은 **비활성**이며, 저장 전에는 어떤 업무도 차단하지 않습니다. 활성화하면 지정한 MCP 작업만 검토 대기로 바뀝니다.

- 정책 이름, 보호 작업, 검토자 역할, 대기 만료, 반려 사유 요구, 자기 승인 허용 여부를 정합니다.
- 검토자는 지정된 역할과 `review_approval` 권한을 **모두** 가져야 합니다.
- 승인 목록과 결정 응답은 실행 JSON 원본이 아니라 서버가 allowlist로 만든 제목·위험 수준·주체·대상·변경 내용·정책 근거를 씁니다. 표시 문자열은 `secret` 패턴을 가리고 길이를 제한합니다.

3.8 플러그인



플러그인 — Mattermost 형식 tar.gz 업로드와 런타임 관리

`manage_plugins` 권한이 있으면 **연동** → **플러그인** 에서 Mattermost 형식 `.tar.gz` 를 업로드하고 활성화·비활성화·교체·삭제할 수 있습니다. 설치가 끝나면 왼쪽 **플러그인** 아래에 manifest 표시명으로 하위 메뉴가 생기며, 비활성이나 실행 실패 상태에서도 진단과 설정 접근을 위해 메뉴는 남습니다.

1. 출처와 빌드 과정을 직접 검토한 번들만 고릅니다.
2. 서명 미검증 완전 신뢰 코드라는 경고를 읽고 확인합니다.
3. 처음 설치는 **플러그인 업로드**, 같은 ID의 버전 교체는 **같은 ID 교체 허용**을 씁니다.
4. 상태가 `running` 인지 확인합니다.
5. 하위 메뉴 또는 목록 행의 **설정**에서 플러그인별 설정을 저장합니다.
6. 장애가 나면 비활성화한 뒤 서버 로그와 플러그인 상태 오류를 확인합니다.

격리 경계 — 플러그인은 sandbox나 서명 검증 없이 moyro 서비스 UID, 컨테이너 namespace, 볼륨, 네트워크를 공유합니다. 아카이브 검사는 공급망 신뢰를 대신하지 않습니다. 업로드 전에 SHA-256과 배포 출처를 별도 절차로 확인하세요.

4. 계정과 권한

4.1 계정이 생기는 세 가지 경로

경로	조건
부트스트랩 관리자	사용자가 한 명도 없을 때 BOOTSTRAP_ADMIN 으로 1회 생성
초대 링크	사이트 설정에서 발급. 만료·최대 사용 횟수를 정합니다. 게스트 링크는 채널·만료·파일 정책을 함께 지정
Keycloak SSO	첫 로그인 시 자동 생성 여부와 검증된 email claim 요구 여부를 설정

로컬 계정 가입은 기본적으로 닫혀 있습니다. 열면 URL을 아는 누구나 계정을 만들 수 있으므로 초대 링크를 권장합니다.

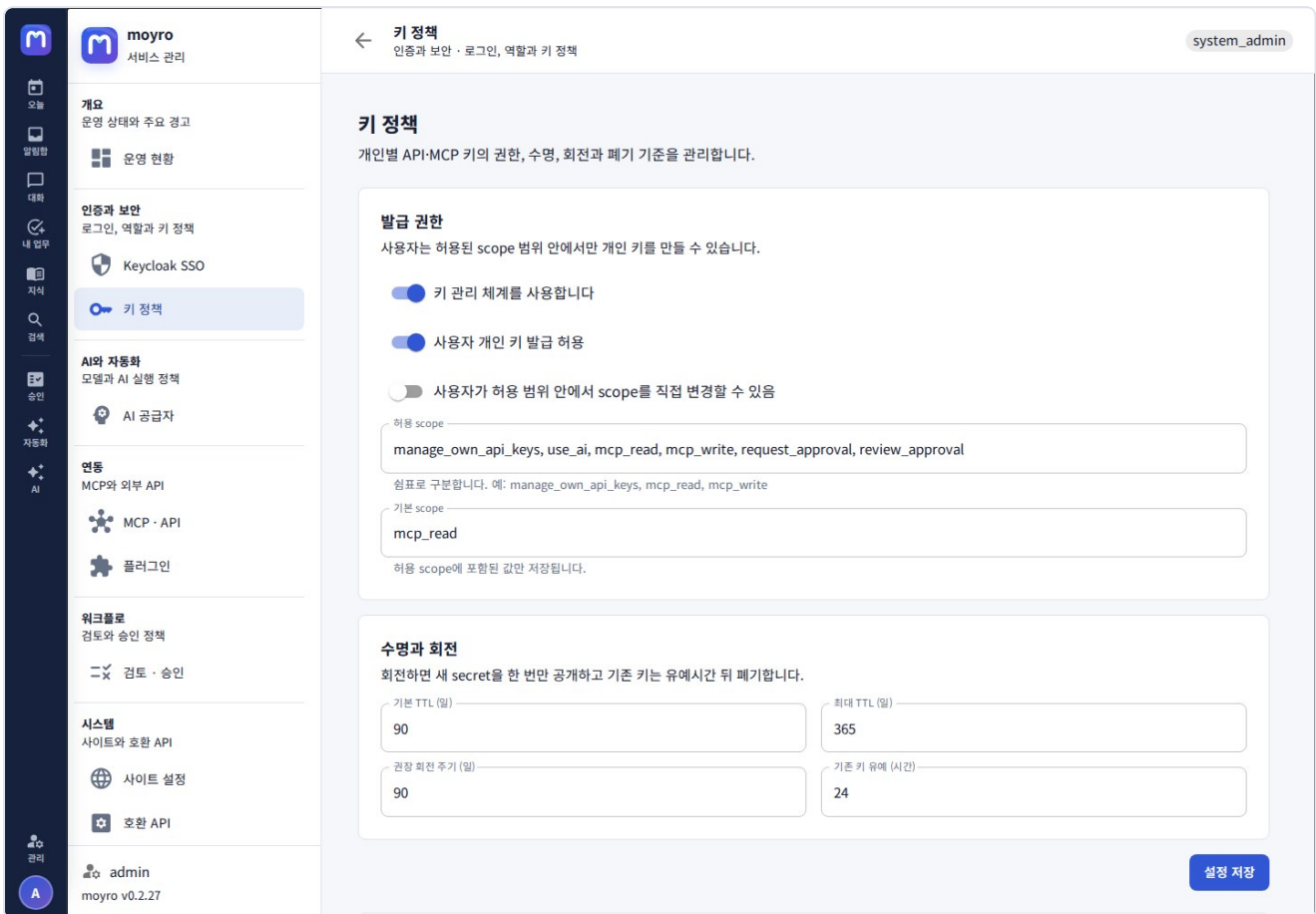
4.2 내장 역할

역할은 시스템·팀·채널 세 범위로 나뉩니다. 아래가 마이그레이션이 심는 초기값입니다.

역할	범 위	초기 권한
system_admin	시 스 템	manage_system , manage_roles , manage_settings , manage_oidc , manage_ai , manage_plugins , manage_api_keys , manage_key_permissions , manage_approval_policies , review_approval , manage_jobs , read_jobs , manage_oauth , manage_system_wide_oauth , mcp_read , mcp_write , use_ai ,채널·팀 관리 권한 등
system_user	시 스 템	create_post , create_public_channel , create_private_channel , use_channel_mentions , manage_slash_commands , manage_own_api_keys , use_ai , mcp_read , mcp_write , request_approval
system_guest	시 스 템	create_post , use_channel_mentions
team_admin	팀	manage_team , manage_public_channel_properties , manage_private_channel_properties , review_approval
team_user	팀	request_approval
channel_admin	채 널	manage_channel
channel_user	채 널	(기본 멤버십 역할)

게스트는 기본 공간이나 다른 공개 채널에 스스로 가입할 수 없고, 접근 만료 뒤에는 새 HTTP·WebSocket 인증이 거부됩니다.

4.3 권한 편집과 키 정책



키 정책과 역할별 permission — 발급 범위·수명·회전과 RBAC 편집

키 정책 화면은 발급 권한 · 수명과 회전 · 발급된 키 · 역할별 권한 네 카드입니다. 앞의 둘에서 개인 키 발급 허용 여부, 허용·기본 scope, TTL, 회전 유예를 정합니다. 사용자는 그 범위 안에서만 키를 만들 수 있고 secret은 발급 시 한 번만 표시됩니다. 키 종류는 user · service · mcp 이며 상태는 active · retiring · revoked 입니다. 회전은 새 행을 만들고 이전 키를 정해진 기간 동안 retiring 으로 둡니다.

발급된 키에서는 모든 사용자의 키 메타데이터를 보고 유출되거나 불필요한 키를 즉시 폐기합니다. secret과 digest는 표시하지 않습니다. 역할별 권한에서는 RBAC 권한을 편집하며 저장 시 revision을 비교해 다른 관리자의 변경을 덮어쓰지 않습니다 (RBAC 역할 정보를 불러오지 못했습니다. 는 조회 실패입니다).

두 가지를 지키세요.

- system_admin 역할은 manage_system 을 잃을 수 없습니다. 서버가 거부합니다.
- 권한을 바꾸기 전에 복구용 관리자 세션을 다른 브라우저에 열어 두세요. 자기 권한을 잘못 줄이면 화면으로 되돌릴 수 없습니다.

마이그레이션은 관리자가 손대지 않은 역할(revision = 1)에만 초기 권한을 심습니다. 한 번 편집한 역할은 재기동·업그레이드가 조용히 되돌리지 않습니다.

5. 운영

5.1 상태 점검

확인	방법	인증
liveness	GET /healthz	없음
지표	GET /metrics (Prometheus)	없음
호환 API 응답	GET /api/v4/system/ping	없음
배포 버전	로그인 화면 하단 / 프로필 메뉴	로그인
마이그레이션 이력	schema_migrations 테이블 (번호·이름·checksum·적용 시각)	DB

/healthz 는 PostgreSQL 왕복 한 번을 포함합니다. /metrics 와 /healthz 는 인증 체인 밖에 있으므로 **외부에 노출하지 마세요**(7절 참고).

5.2 로그

애플리케이션 로그는 컨테이너 stdout으로 나갑니다.

```
docker logs --tail 200 moyro
docker logs -f moyro
```

감사 로그는 별도로 PostgreSQL에 저장되며 관리자 화면에서 조회합니다.

5.3 백업

세 가지를 한 복구 세트로 보관합니다. 하나라도 빠지면 복구가 반쪽이 됩니다.

- 1. PostgreSQL 데이터베이스 — 조직의 pg_dump 또는 물리 백업 절차
 - 2. moyro-data 볼륨 — 업로드 파일과 플러그인
 - 3. ENCRYPTION_KEY — 데이터 백업과 분리된 곳에
- 복구는 격리된 호스트에서 시험하세요. 파일 볼륨 없이 DB만 복구하면 메시지 메타데이터는 남고 첨부은 사라집니다. 인수 시험에서는 작업·결정·알림함의 소유자/멤버십 범위와 cursor 조회도 함께 확인하세요.

5.4 업그레이드와 되돌리기

- 1. PostgreSQL, moyro-data , 환경 파일을 백업합니다.

2. 새 `moyro-v<버전>.tar.gz` 를 `docker load` 합니다.
3. 기존 컨테이너를 멈춥니다 — `docker stop moyro && docker rm moyro`
4. 같은 환경 파일과 같은 볼륨으로 새 태그를 기동합니다(2.4의 명령에서 태그만 교체).
5. 확인합니다 — `/healthz` , 로그인 화면 버전, 관리자 로그인, 채널 게시, 파일 접근, WebSocket 수신, 알림함 읽음 상태, 작업·결정의 원문 링크, 예약 발송, 커 둔 webhook, Keycloak 로그인.

마이그레이션은 번호 순서, checksum ledger, PostgreSQL advisory lock, 마이그레이션별 트랜잭션을 씁니다.

되돌리기 — 새 버전이 마이그레이션을 적용한 뒤에는 이전 이미지가 미래 버전의 스키마를 거부하고 기동을 멈춥니다. 따라서 되돌리기는 **이전 이미지 + 그 시점의 데이터베이스 백업**을 함께 복원하는 절차입니다. 이미지만 되돌리지 마세요. 업그레이드 직전 백업이 반드시 필요한 이유입니다.

6. 장애 대응

증상 → 확인할 곳 → 조치 순서입니다. 괄호 안은 로그나 화면에 실제로 찍히는 문구입니다.

증상	확인할 곳	조치
컨테이너가 곧바로 죽음 (config: missing required environment variables: ...)	<code>docker logs moyro</code>	환경 파일에 네 변수가 모두 있는지 확인. <code>-env-file</code> 경로도 확인
기동 중단 (config: invalid POSTGRES_DSN: ...)	같은 로그	DSN 형식을 고칩니다
기동 중단 (config: BOOTSTRAP_ADMIN must be a plain email address)	같은 로그	표시 이름 없이 주소만 넣습니다
기동 중단 (config: BOOTSTRAP_ADMIN_PASSWORD must contain at least 12 bytes)	같은 로그	12 - 72바이트로 맞춥니다
기동 중단 (config: ENCRYPTION_KEY must be base64 for exactly 32 bytes)	같은 로그	<code>openssl rand -base64 32</code> 결과를 그대로 넣습니다
업그레이드 뒤 기동 중단, 마이그레이션 checksum 불일치	로그 + <code>schema_migrations</code>	이미지와 DB 세대가 어긋난 상태입니다. 손으로 고치지 말고 5.4의 백업 복원 절차를 따르세요
<code>/healthz</code> 실패	<code>docker logs</code> , PostgreSQL 접근성	DB 연결·자격 증명·네트워크를 먼저 봅니다
로그인은 되는데 화면이 비어 있음	브라우저 콘솔, 운영 현황	특정 API 실패는 화면에 ...을 불러오지 못했습니다 로 나옵니다. 해당 영역의 권한과 DB 상태 확인
SSO 버튼이 안 보임	<code>/admin/auth/keycloak</code>	활성화 여부와 공개 URL 저장 여부 확인
SSO 로그인 실패 (OIDC discovery 확인에 실패했습니다.)	Keycloak 도달성, issuer URL	컨테이너에서 <code>discovery·token·JWKS</code> 에 닿는지 확인
SSO 로그인 실패 (보안 상태값이 일치하지 않습니다. 다시 로그인해 주세요.)	사용자 브라우저	오래된 탭이거나 시계 어긋남. 호스트 시각 동기화 확인
SSO 후 권한이 안 붙음 (SSO 그룹 기반 팀·채널 권한을 안전하게 적용하지 못했습니다.)	그룹 매핑 설정	매핑한 그룹 이름과 실제 claim 값을 대조
AI 기능 실패 (AI endpoint 확인에 실패했습니다.)	<code>/admin/ai/providers</code>	Base URL·모델·타임아웃 확인. 내부 endpoint 도달성 확인
사용자에게 AI가 안 보임 (AI 사용 권한이 없습니다.)	키 정책 화면의 역할별 권한	해당 역할에 <code>use_ai</code> 부여

증상	확인할 곳	조치
Outgoing webhook이 안 나감	사이트 설정의 allowlist	대상 host를 scheme 없이 추가. 비어 있으면 전부 차단됩니다
MCP 클라이언트 401/403 (MCP transport가 비활성화되어 있습니다.)	/admin/integrations/mcp	endpoint 활성화, 허용 tool/resource, 키 scope 확인
플러그인이 running 이 아님	플러그인 목록의 상태 오류 + docker logs	비활성화한 뒤 manifest와 대상 플랫폼 실행 파일 확인
메일이 안 감	—	의도된 동작입니다. SMTP 설정이 없으면 이메일 capability를 false로 응답하고 digest worker를 시작하지 않습니다

운영 현황 화면의 **미확인**은 "고장"이 아니라 "확인할 수 없음"입니다. 예를 들어 Worker와 Webhook 전달은 큐 수치를 조회했다라도 heartbeat가 없으면 실행 상태를 미확인으로 둡니다. **미설정**은 아직 설정하지 않은 선택 기능(OIDC·AI 등)입니다.

호환 운영 API v0.2.27 호환 경계

레거시 Mattermost 운영 경계의 지원 상태를 안내합니다.

⚠️ 로그·클러스터·Busy 상태·백그라운드 작업의 레거시 Mattermost 운영 API는 moyro v0.2.27에서 실제 운영 기능으로 제공하지 않습니다. 관련 호환 API는 거짓 성공 대신 501 Not Implemented를 반환합니다.

사이트, Keycloak OIDC, AI, 키·권한, MCP, 승인 정책과 Trusted Native 플러그인은 서비스 관리자 메뉴에서 PostgreSQL 기반 상태로 관리합니다.

[← 서비스 관리로 돌아가기](#) [워크스페이스](#)

호환 운영 API — 레거시 Mattermost 운영 경계의 지원 상태

호환 API 화면(/admin/operations , 화면 제목은 **호환 운영 API**)은 레거시 Mattermost 운영 API의 지원 상태를 안내합니다. 로그·클러스터·Busy 상태·백그라운드 작업의 레거시 운영 API는 실제 운영 기능으로 제공하지 않으며, 거짓 성공 대신 **501 Not Implemented** 를 돌려줍니다. PUT /config , PUT /config/patch , POST /config/reload 가 여기 해당합니다. 사이트·Keycloak OIDC·AI·키·권한·MCP·승인 정책과 플러그인은 앞의 전용 관리자 화면에서 PostgreSQL 기반 상태로 관리합니다.

모바일 쪽에서도 같은 관리자 화면을 쓸 수 있습니다.

사이트 설정

사용자에게 표시할 이름과 외부에서 접근 가능한 기준 URL, 내부망 outbound 허용 대상을 관리합니다.

서비스 주소

로그인 redirect와 링크 생성에 사용할 절대 origin입니다. 운영 환경에서는 인증서가 유효한 HTTPS URL을 권장합니다.

사이트 이름 *

moyro

로그인 화면과 알림에 표시됩니다.

Public Base URL

http://127.0.0.1:18075

경로 없는 HTTP(S) 절대 origin입니다. 운영 환경은 HTTPS를 권장합니다.



HTTP URL은 전송 중 인증 정보가 노출될 수 있습니다. 운영 환경에서는 HTTPS를 사용하세요.

신뢰할 reverse proxy

나열한 프록시에서 직접 들어온 요청에만 Forwarded / X-Forwarded-* 헤더를 사용합니다.

Trusted proxy CIDR



오늘



대화



알림함



검색



더보기

7. 보안

7.1 기본값 중 바꿔야 하는 것

항목	기본값	해야 할 일
TLS	없음(평균 8065)	리버스 프록시에서 TLS 종료
Public Base URL	<code>http://localhost:8065</code>	실제 공개 HTTPS origin으로 저장
Trusted proxy CIDRs	비어 있음	프록시가 외부 헤더를 제거하도록 구성한 뒤 그 CIDR만 추가
부트스트랩 관리자 비밀번호	환경 파일 값	최초 로그인 뒤 화면에서 변경
환경 파일 권한	—	<code>chmod 600</code> , 데이터 볼륨 밖에 보관

`ENCRYPTION_KEY` 는 그대로 두어야 합니다. 바꾸면 기존 암호화 설정을 읽을 수 없습니다.

7.2 외부에 열면 안 되는 것

대상	이유
<code>GET /metrics</code>	인증 없이 운영 지표를 노출합니다. 내부 스크레이퍼만 달게 하세요
<code>GET /healthz</code>	인증이 없습니다. 프로브 범위로 제한하세요
<code>POST /hooks/{hookID}</code>	URL만 알면 게시할 수 있습니다. 필요한 대역에서만 달게 하세요
PostgreSQL 5432	내부망 안에만
컨테이너 8065 직접 노출	프록시 뒤에 두세요

7.3 인증 연동과 계정

- 로컬 가입은 닫아 두고 초대 링크나 SSO를 씁니다.
- 외부 협업자는 게스트 초대로 채널·만료·파일 다운로드를 제한합니다.
- 개인 키는 정책으로 scope와 TTL을 좁히고 회전을 강제합니다.
- 승인 정책을 켜면 지정한 MCP 작업이 검토를 거칩니다. 검토자에게는 지정 역할과 `review_approval` 권한이 모두 필요합니다.

7.4 플러그인은 신뢰 경계 밖이 아닙니다

`/var/lib/moyro/plugins` 의 실행 파일과 런타임에 업로드한 아카이브는 **완전 신뢰 코드**입니다. `sandbox`도 서명 검증도 없고 서비스 UID·namespace·볼륨·네트워크를 공유합니다. 검토하고 승인한 것만 설치하세요. 업로드한 번들은 서버뿐 아니라 로그인한 사용자의 브라우저에서도 실행될 수 있습니다.

더 볼 것

- [사용자 가이드](#) — 화면 사용법과 자주 하는 작업
- [오프라인 배포](#) — 릴리즈 자산 설치의 상세 절차
- [아키텍처 · 플러그인 시스템](#)
- `openapi-v4.yaml` · `openapi-moyro.yaml`