CLUe

관리자 가이드

버전 R_2026-09-28

한국어
KO 102.00

suprema
SECURITY & BIOMETRICS

목차

CLUe 웹 포털 시작하기 5

관리자 레벨 이해 5

하위 항목 추가 5

관리자 초대 7

서비스 설정하기 9

고객사 API 연동하기 12

시작하기 전에 12

고객사 API 연동 13

주요 작업 워크플로우 14

설정 워크플로우 14

입력 규칙 요약 25

문제 해결 26

펌웨어 변경하기 30

CLUe 지원 모드로 전환 30

문제 해결 32

장치 추가하기 33

장치 등록(브랜치 관리자) 33

장치 할당 34

테스트 공간 설정(브랜치 관리자) 36

장치 셀프 등록하기 38

지원하는 장치 및 펌웨어 버전 38

관리자 준비 단계 38

현장 등록 단계 39

참고 사항 43

출입문 추가하기 44

출입문 설정 44

슬레이브 장치 릴레이 사용 45

펌웨어 업그레이드하기 47

공간으로 이동 47

펌웨어 업그레이드 48

장치 웹훅(Webhook) 설정하기 50

지원 장치 50

주요 장점 50

웹훅 설정 50

참고 사항 43

감사 로그 확인하기 54

감사 로그 조회 54

상세 정보 확인 54

조회 기간 설정 55

검색 55

모바일 앱 사용하기 57

CLUe 모바일 앱 관리자 초대 57

CLUe 앱 다운로드 58

로그인 59

CLUe 앱 주요 기능 62

CLUe API 가이드 64

API 키란 64

API 키 발급 64

CLUe API 기본 65

API 호출 제한 67

Dynamic QR 코드 연동하기 68

CLUe Dynamic QR 코드란 68

시작하기 전에 12

API 키 발급 64

서비스 설정 69

다음 단계 0

다음 단계 0

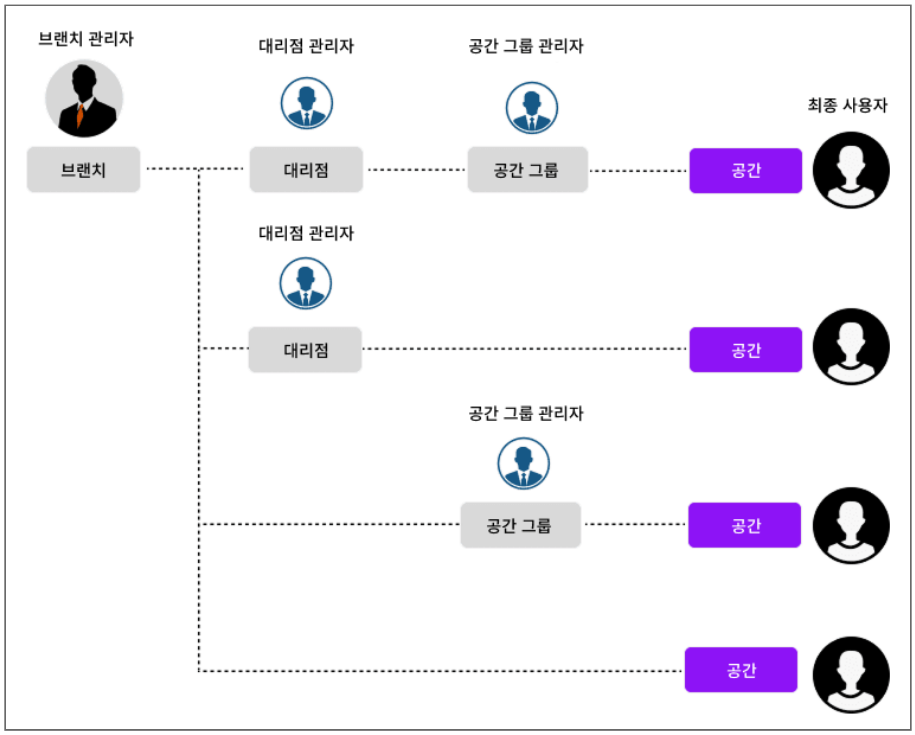
다음 단계 0

CLUe 웹 포털 시작하기

CLUe 웹 포털을 처음 사용한다면, 관리자 권한 구조를 이해하는 것부터 시작하세요. 이 문서에서는 브랜치 하위에 대리점, 공간 그룹, 공간을 추가하는 방법을 안내합니다.

관리자 레벨 이해

CLUe는 여러 지점에서 고객 서비스를 운영하는 유통 채널 환경을 위해 설계된 3단계 계층 구조의 멀티 테넌트 시스템입니다.



- **브랜치 관리자**(Branch Admin): 브랜치 관리자는 **대리점**/**공간 그룹**/**공간**을 하위 항목으로 생성할 수 있습니다.
- **대리점 관리자**(Disti Admin): 대리점 관리자는 **공간 그룹**/**공간**을 하위 항목으로 생성할 수 있습니다.
- **공간 그룹 관리자**(Place Group Admin): 공간 그룹 관리자는 **공간**을 하위 항목으로 생성할 수 있습니다.

이메일을 통해 고객을 초대하고, 초대받은 고객은 이메일에 포함된 링크를 통해 가입한 후 초대받은 공간 그룹에 액세스할 수 있습니다.

하나의 브랜치는 여러 대리점을 가질 수 있고, 하나의 대리점 역시 여러 공간 그룹을 가질 수 있습니다. 대리점 관리자 레벨이라면, 자신의 대리점과 하위 항목만 볼 수 있습니다.

> **고객이나 최종 사용자는 어느 항목에 해당하나요?**
>
> 위 계층 구조에서 **공간 그룹**(Place Group)이 고객 또는 서비스 제공자에게 할당되는 항목입니다. 공간 그룹은 여러 공간을 운영하는 고객 단위를 나타내므로, 공간 생성 시 해당 고객의 관리자 이메일을 입력해야 합니다.

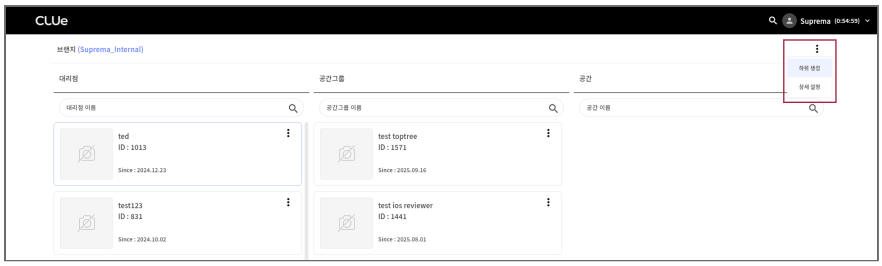
하위 항목 추가

1. CLUe 웹 포털에 로그인하세요.

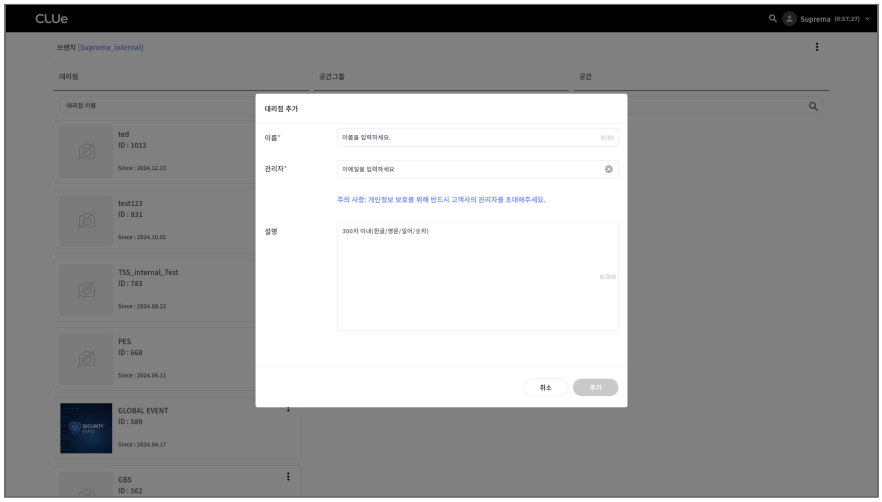
2. 로그인하면 초대받은 브랜치 목록을 확인할 수 있습니다. 원하는 브랜치를 선택하세요.

3. 선택한 브랜치의 하위 항목인 대리점/공간 그룹/공간 목록이 표시되면 화면 오른쪽 상단의 ⋮ 버튼을 클릭하세요.

4. 팝업 메뉴에서 **하위 생성**을 클릭하세요.



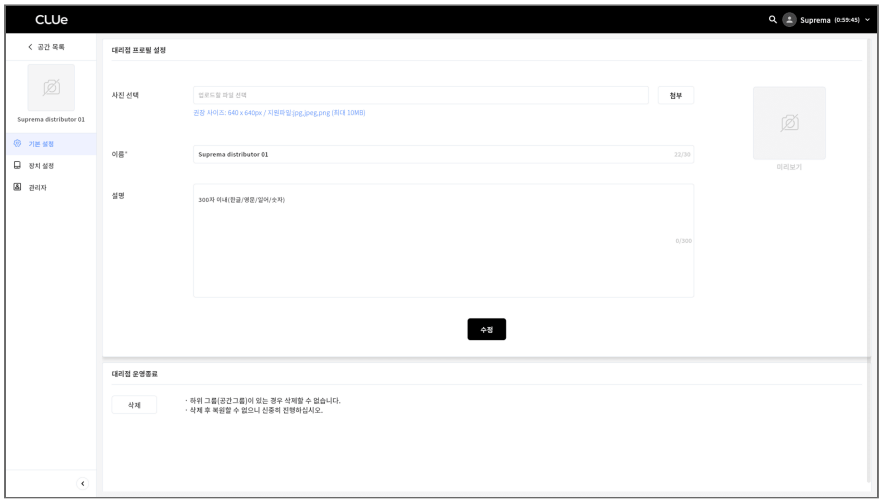
5. **대리점 추가** 팝업이 나타나면 각 필드를 입력하세요.



> **관리자 이메일을 입력해야 하는 이유**
>
> 기본적으로 최고 관리자는 장치 또는 출입문 설정과 같이 고객 개인 정보와 관련 없는 메뉴에만 접근할 수 있습니다. 고객 개인 정보에 접근하려면 고객의 동의가 필요하므로 먼저 고객 관리자를 초대해야 합니다.
>
> 이후 개인 정보 접근이 필요하다면, 고객은 최고 관리자를 추가로 초대할 수 있습니다. 초대된 최고 관리자는 사용자, 관리자, 모니터링 등 개인 정보가 포함된 메뉴에 접근할 수 있습니다.

6. 입력을 모두 완료한 후 하단의 **추가** 버튼을 클릭하세요.

7. 항목이 추가되면 자동으로 **기본 설정** 페이지로 이동되며, 이름이나 사진을 변경할 수 있습니다.

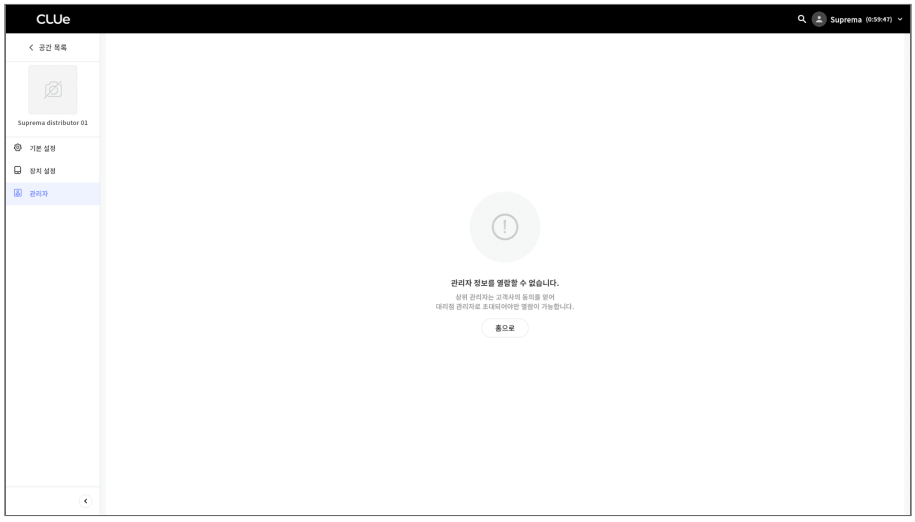


알아두기

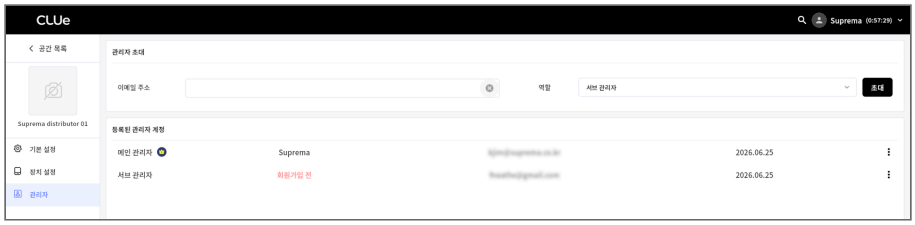
마찬가지로 대리점, 공간 그룹, 공간 목록에서 ⋮ → **하위 생성**을 클릭하면 하위 항목을 추가할 수 있습니다.

관리자 초대

관리자 메뉴는 표시되지만, 고객사의 동의 없이는 관리자 정보를 열람할 수 없습니다. 고객사(대리점 또는 공간 그룹 관리자)가 상위 관리자를 초대해야만 열람이 가능합니다.



관리자 메뉴에서 이메일 주소를 입력해 같은 레벨의 관리자를 쉽게 초대할 수 있습니다. 초대받은 사용자가 가입을 완료하면 동일한 수준의 관리자 권한을 갖게 됩니다.



알아두기

메인 관리자 / **서브 관리자**: 기능적인 차이는 없습니다. 이는 최소 한 명의 메인 관리자가 유지되도록 보장하기 위한 것입니다. 다만, 서브 관리자는 메인 관리자를 삭제할 수 없습니다.

서비스 설정하기

공간 그룹 단위로 출입 서비스 방식을 설정합니다. 공간 그룹에서 설정한 서비스 타입과 크리덴셜은 하위 공간 전체에 자동으로 적용되므로, 개별 공간마다 반복해서 설정할 필요가 없습니다.

CLUe는 두 가지 출입 서비스 방식을 지원합니다.

- **고객사 확인**: 외부 API를 통해 클라이언트에 출입 승인을 요청하는 방식입니다.
- **멤버쉽 관리**: 외부 연동 없이 CLUe가 독립적으로 출입을 제어하는 방식입니다.

공간 그룹 설정의 왼쪽 사이드바에서 **서비스 설정**을 클릭하세요.



고객사 확인 설정

고객사 확인 방식은 출입문을 열기 전에 외부 클라이언트 API를 호출하여 출입 승인 여부를 결정합니다. QR 코드와 얼굴 인증을 지원합니다.

QR 방식

QR 코드를 스캔하면 CLUe 서버가 클라이언트 API를 호출하여 출입 허용 여부를 직접 받습니다. 사용하는 QR 코드 유형에 따라 다음 두 가지 방식 중 하나를 선택하세요.

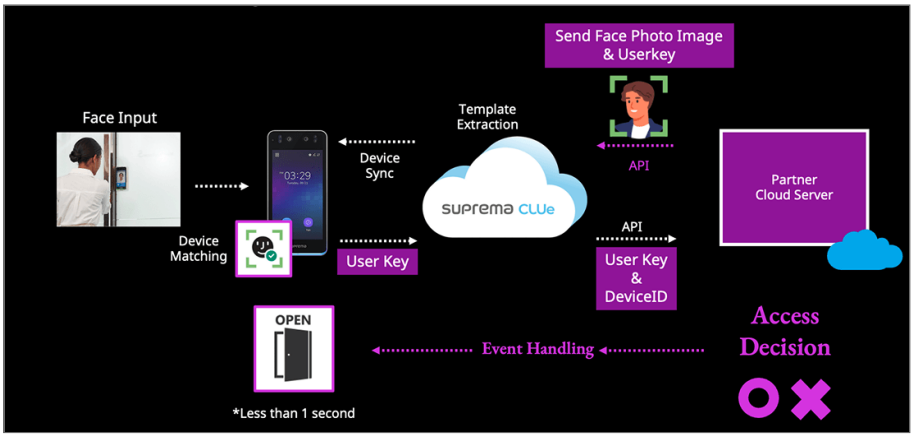
- **CLUe QR**: CLUe에서 직접 발급하는 동적 QR 코드입니다.
- **Customer QR**: 고객이 자체적으로 QR 코드를 생성·운영하는 경우 선택합니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

얼굴 인증 방식

얼굴 인증을 사용한다면, 이미지만 등록하여 CLUe 서버가 템플릿을 추출하고 장치와 동기화합니다. 얼굴 매칭에 성공하면 QR 방식과 동일하게 클라이언트 API를 통해 출입 여부를 결정합니다. 얼굴 사용자 등록 방법은 CLUe API 문서를 참고하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

고객사 확인 코드 설정

고객사 확인 방식을 사용하려면 CLUe 서버가 고객 또는 파트너 API를 어디서, 어떻게 호출하는지 고객사 확인 코드와 함께 입력해야 합니다.

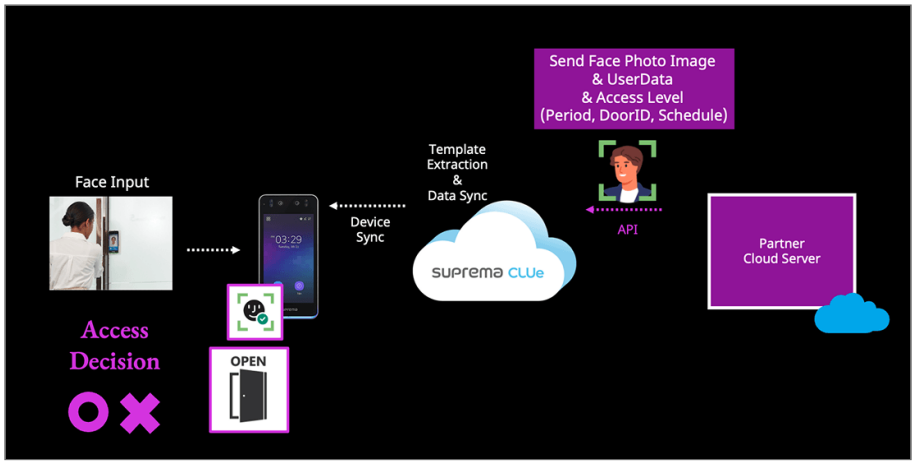


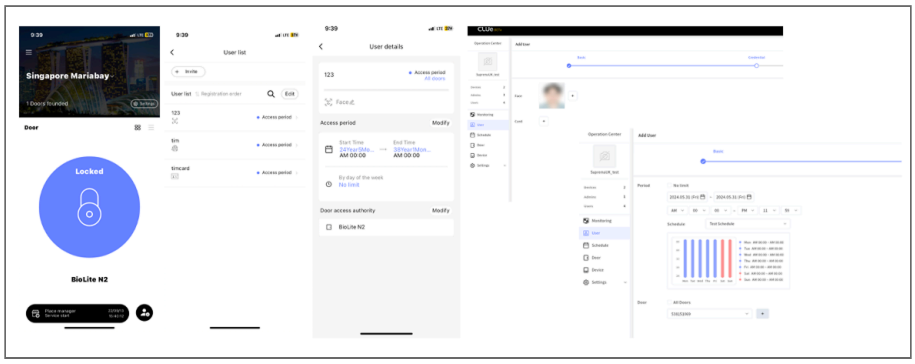
고객사 확인 코드는 슈프리마 CLUe 팀이 어떤 클라이언트의 API를 호출할지 결정하기 위해 사전에 테스트하고 개발한 코드 형식입니다. 이 코드를 입력하면 하위 공간에서 추가 설정 없이도 각 인증 방식에 맞는 API를 자동으로 호출하고, 지정된 응답 값을 기반으로 출입 제어를 수행합니다.

> **고객사 확인 코드 얻는 방법**
>
> 다른 클라이언트의 코드가 노출되지 않도록 CLUe 팀에서 별도로 관리합니다. 고객사 확인 코드 생성은 API 스펙 검토 후 별도로 처리되며, 자세한 내용은 CLUe 팀에 직접 문의하세요.

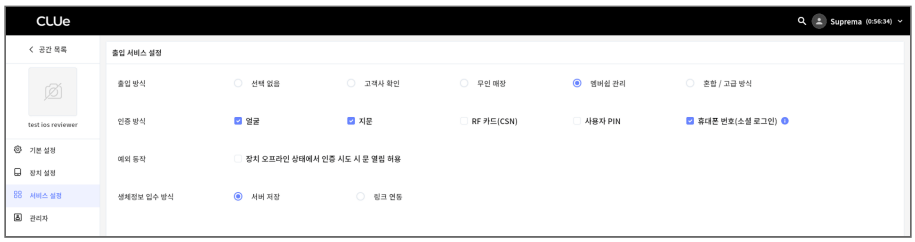
멤버쉽 관리 설정

멤버쉽 관리 방식은 외부 클라이언트나 제3자의 개입 없이 CLUe 시스템이 독립적으로 출입 제어를 결정합니다. 웹 포털이나 모바일 애플리케이션만으로 CLUe를 운영하는 경우에도 적용할 수 있습니다.





멤버쉽 관리 설정을 통해 하위 공간에 적용할 크리덴셜을 선택할 수 있습니다.



> **공간 그룹과 다르게 공간 설정을 변경할 수 있나요?**
>
> 네, 공간 설정 페이지에서 인증 방식을 구성할 수 있습니다. 다만 출입 방식을 **멤버쉽 관리**에서 **고객사 확인**으로, 또는 그 반대로 변경할 수 없습니다. 따라서 같은 공간 그룹의 고객이 서로 다른 출입 방식을 필요로 한다면 각 용도에 맞게 별도의 공간 그룹을 만드는 것을 권장합니다.

다음 단계

CLUe 공간 그룹에서 고객사(Vendor) API를 등록하고 크리덴셜에 연결하여, 고객사의 출입 판정 로직을 CLUe 출입 제어와 연동하는 방법을 확인하세요.

고객사 API 연동하기

고객사 API 연동은 CLUe 장치가 인식한 크리덴셜(얼굴, 지문, RF 카드, PIN, CLUe QR, 커스텀 QR 등)을 고객사가 운영하는 외부 API로 전달하고, 그 응답에 따라 출입을 허용하거나 거부하는 출입 방식입니다. 이 방식을 사용하면 출입 권한, 근태, 방문자 관리 등 고객사 고유의 정책을 별도 개발 없이 CLUe 출입 제어에 직접 반영할 수 있습니다.

CLUe는 크리덴셜을 인식해 고객사 API로 전달하는 역할만 수행하며, 실제 출입 허용 여부는 고객사 API의 응답에 따라 결정됩니다.

시작하기 전에

대상

이 문서는 **공간 그룹 관리자**와 **공간 관리자**를 대상으로 합니다.

- **공간 그룹 관리자**: 고객사(Vendor) API를 등록 및 수정, 삭제하고, 크리덴셜 타입과 API를 매핑하며, 설정을 하위 공간에 적용합니다.
- **공간 관리자**: 공간 그룹에서 상속받은 설정을 검토하고, 필요할 때 공간별로 재정의를 적용합니다.

> **알아두기**
> 이 문서는 **HTTPS**, **HTTP 상태 코드**, **Webhook**(HTTP POST), **JSON**, **JSONPath**에 익숙한 IT 관리자를 대상으로 합니다.
> 고객사 API 스펙(URL, 인증 헤더, 요청/응답 JSON 구조)은 사전에 고객 담당자와 협의하세요.

사전 준비

- 이 메뉴에 접근하려면 대상 공간 그룹(또는 공간)에 관리자로 초대되어야 합니다.
- 고객사의 인증용 Webhook URL(**HTTPS 필수**, **HTTP POST 수신**)과 필요한 인증 헤더 값을 미리 확보하세요.

주요 용어

용어	설명
고객사 API 연동(Customer API Integration)	사용자가 장치에 크리덴셜을 제시하면 크리덴셜 데이터를 고객사(Vendor)가 운영하는 외부 API로 전송해 검증하는 출입 방식입니다.
크리덴셜(Credential)	얼굴 / 지문 / RF 카드 / 사용자 PIN / CLUe QR / 커스텀 QR
웹훅 URL	CLUe로부터 인증 요청(HTTP **POST**, `Content-Type: application/json`)을 받기 위해 고객사 서버가 개방하는 HTTPS 엔드포인트입니다.
요청 헤더(Request Header)	인증 및 권한 부여를 위해 요청과 함께 전송하는 Key/Value 쌍입니다. (예: `Authorization` 토큰)
자동 필드	시스템이 요청 본문에 자동으로 채우는 값입니다. 필요한 필드만 선택하세요.
수동 필드	관리자가 요청 본문에 포함하기 위해 직접 입력하는 고정 값입니다.

용어	설명
판정 기준(Judgment Criteria)	고객사 응답을 출입 허용 또는 거부로 해석하는 규칙 집합(statusCode, 성공 결과 Key/Value, 성공/실패 메시지 키)입니다. 화면에는 **응답 파싱** 섹션으로 표시됩니다.
판정 모드(Judgment Mode)	판정 기준을 구성하는 요소입니다. HTTP 응답 코드만 사용 / 응답 본문 필드만 사용 / 두 가지 조합 중 하나를 선택합니다.

고객사 API 연동

고객사 API 연동은 CLUe 장치가 인식한 크리덴셜 데이터를 고객사가 운영하는 HTTPS API로 전달하고, 그 응답을 기반으로 출입 허용/거부를 판정하는 출입 방식입니다. 이를 통해 출입 권한, 근태, 방문자 관리 등 고객사 고유의 정책을 CLUe 출입 제어에 직접 반영할 수 있습니다.

- 얼굴, 지문, RF 카드, PIN, CLUe QR, 커스텀 QR 등 각 크리덴셜 타입마다 서로 다른 고객사 API를 연결할 수 있습니다.
- 등록을 저장하기 전에 테스트 호출로 연동 동작을 미리 확인할 수 있습니다.
- CLUe는 크리덴셜을 식별해 전달하는 역할만 하며, 실제 허용 또는 거부 결정은 고객사 API의 응답에 따라 결정됩니다.

지원 크리덴셜

- 얼굴
- 지문
- RF 카드
- 사용자 PIN
- CLUe QR
- 커스텀 QR

공간 그룹과 공간의 역할

레벨	역할	담당 업무
공간 그룹	공간 그룹 관리자	고객사 API 등록/수정/삭제, API와 크리덴셜 연결
공간	공간 관리자	상속된 설정 검토, 필요 시 공간별 재정의 적용

적용 규칙

- **공간 그룹 레벨에서 저장**: 동일한 설정이 해당 공간 그룹의 모든 하위 공간에 즉시 적용됩니다. 기존에 적용되어 있던 공간별 재정의는 공간 그룹 값으로 덮어쓰기됩니다.
- **공간 레벨에서 저장**: 해당 공간에만 적용됩니다. 다른 공간이나 상위 공간 그룹에는 영향을 주지 않습니다.

주요 작업 워크플로우

고객사 API 연동은 크게 두 가지 워크플로우(Workflow)로 구성됩니다. 관리자가 먼저 수행하는 **설정 워크플로우**와 사용자가 실제로 출입을 시도할 때 진행되는 **출입 이벤트 워크플로우**입니다.

설정 워크플로우 개요

관리자가 수행하는 단계입니다. 각 단계는 4장부터 자세히 설명합니다.

1. (공간 그룹) 출입 방식을 선택하세요.
    - **고객사 확인** 또는 **혼합 / 고급 방식**
    - 왼쪽 사이드바에서 **고객사 API 연동** 항목이 활성화됩니다.
2. (공간 그룹) **고객사 API 연동**에서 API 등록하세요.

    기본 정보 → 커스텀 헤더 → 자동 필드 → 수동 필드 → 테스트 실행 → 응답 파싱 구성 → 저장
3. (공간 그룹) 등록한 API를 각 크리덴셜에 연결하세요.

    저장하면 동일한 설정이 모든 하위 공간에 자동 적용됩니다.
4. (선택 사항) 공간별 재정의 설정하세요.

    선택한 공간에만 적용됩니다. 기본값은 공간 그룹 설정을 그대로 사용합니다.

출입 이벤트 워크플로우 개요

설정을 마친 후 사용자가 실제로 출입을 시도할 때 처리되는 순서입니다.

1. 사용자가 장치에 크리덴셜을 제시합니다. (얼굴 / 지문 / RF 카드 / PIN / CLUe QR / 커스텀 QR)
2. 장치 → CLUe 서버로 검증 요청을 전송합니다.
3. CLUe 서버 → 고객사 서버로 검증 요청을 전송합니다.

    등록된 Webhook URL, 커스텀 헤더, 자동 필드, 수동 필드 포함
4. CLUe 서버가 고객사 응답을 기반으로 출입 여부를 판정합니다.

    설정한 판정 기준에 따라 허용/거부 결정합니다.
5. 결과를 장치로 반환합니다.

    응답에 메시지가 포함되어 있으면 장치 화면에 표시됩니다.

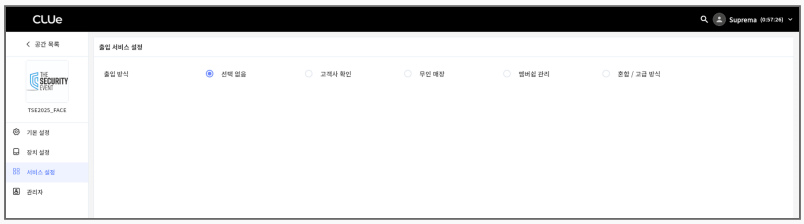
설정 워크플로우

1단계 — 고객사 API 연동 활성화

1. CLUe 웹 포털에 로그인하세요.
2. 공간 그룹을 선택하세요.
3. 화면 오른쪽 상단의 ⋮ → **상세 설정**을 클릭하세요.

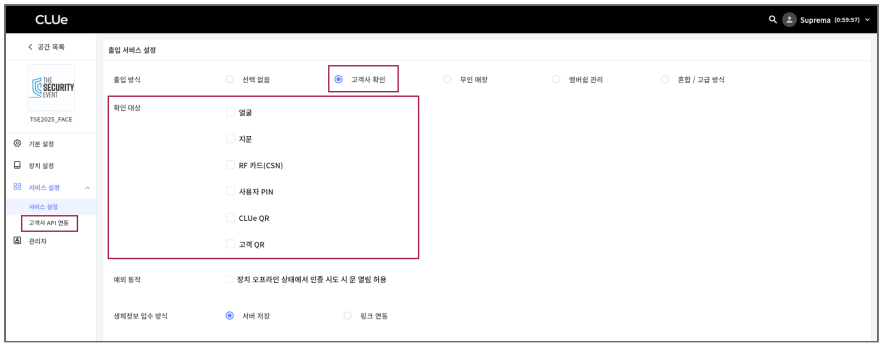


4. 화면 왼쪽 사이드바에서 **서비스 설정**을 클릭하세요.

> 초기 상태에서는 **출입 방식**이 **선택 없음**으로 설정되어 있습니다. 이 상태에서는 아무 설정도 활성화되지 않습니다.
>
> 
>

5. **출입 방식**에서 **고객사 확인**을 선택하세요.

6. **확인 대상** 섹션이 나타납니다.



확인 대상 섹션에는 지원하는 6개 크리덴셜이 모두 표시됩니다. 이후 각 크리덴셜에 등록한 고객사 API를 연결할 수 있습니다.

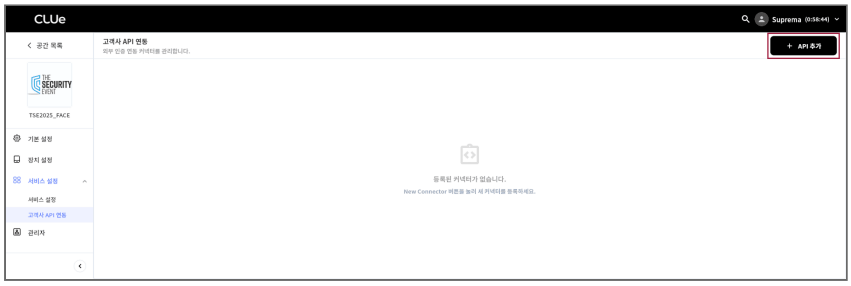
7. 왼쪽 사이드바에서 **고객사 API 연동**이 활성화되면 클릭하세요.

> **알아두기**
>
> - **고객사 API 연동**은 **출입 방식**이 **고객사 확인** 또는 **혼합 / 고급 방식**으로 설정되어 있을 때 활성화됩니다.
> - 이 단계에서는 저장할 필요가 없습니다. 연결할 API를 등록하려면 2단계 — 고객사 API 등록을 참고하세요.

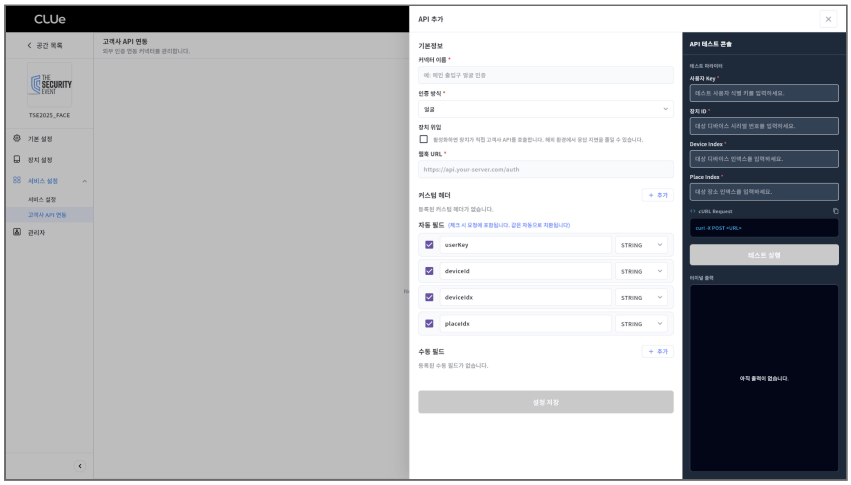
2단계 — 고객사 API 등록

1 API 추가

1. 화면 오른쪽 상단의 **API 추가** 버튼을 클릭하세요.



2. **API 추가** 패널이 나타나면 필요한 정보를 입력하세요.



2 기본 정보 입력

필드	설명	필수 여부	입력 규칙
커넥터 이름	이 연동을 식별할 이름을 입력하세요.	필수	최대 64자까지 입력할 수 있습니다.
인증 방식	이 API를 사용할 크리덴셜을 선택하세요.	필수	6개 타입 중 하나를 선택하세요.
웹훅 URL	고객사 Webhook URL입니다.	필수	`https://`로 시작해야 하며 최대 512자입니다. `http://` URL은 저장할 수 없습니다.

> **알아두기**
> **인증 방식**은 한 번 설정하면 변경할 수 없습니다. 다른 크리덴셜 타입에 사용하려면 새 API를 등록하세요.

3 요청 규격

CLUe는 등록된 URL에 **HTTP POST**, `Content-Type: application/json` 요청만 전송합니다. 고객사 API는 이 형식의 요청을 받을 수 있어야 하며, `GET`, `PUT` 등 다른 메서드만 허용하는 엔드포인트는 사용할 수 없습니다.

4 응답 규격

고객사 API는 응답 헤더에 `Content-Type: application/json`을 포함해야 하며, 응답 본문을 JSON 형식으로 반환해야 합니다. HTML 오류 페이지, 일반 텍스트, XML 등 JSON이 아닌 응답은 CLUe가 파싱할 수 없어 테스트와 실제 출입 검증이 모두 실패합니다.

Example response body

```
{
  "valid": true,
  "message": "Access granted."
}
```

위 예시에서는 판정 기준의 `Key`를 `$.valid`로, `Value`를 `true`(`BOOLEAN`)로 설정해 성공 조건을 정의하고, **성공 메시지 JSONPath**를 `$.message`로 설정해 성공 메시지를 표시할 수 있습니다. 실제 키 이름과 구조는 고객사 API 스펙에 맞춰야 합니다.

> **등록 제한**
>
> 크리덴셜 타입당 최대 **3개**의 API를 등록할 수 있습니다. 즉 얼굴, 지문, RF 카드, PIN, CLUe QR, 커스텀 QR, 6개 타입을 합쳐 공간 그룹당 최대 18개의 API를 등록할 수 있습니다. 이미 3개가 등록된 크리덴셜 타입에는 추가로 등록할 수 없습니다. 각 크리덴셜에 실제로 사용할 API는 3단계 — 각 크리덴셜에 API 할당에서 선택합니다.

5 커스텀 헤더 추가

고객사 API에서 **Authentication/Authorization headers**를 요구한다면 커스텀 헤더를 추가하세요.

> *예: `Authorization` 토큰, API 키*



필드	설명
헤더 이름	헤더 이름(예: `Authorization`)을 입력하세요. 중복된 이름은 허용되지 않습니다.
헤더 값	헤더 값을 입력하세요.

- 커스텀 헤더는 최대 **10개**까지 추가할 수 있습니다.
- 고객사 API가 공개 엔드포인트이거나 별도 헤더가 필요 없다면 이 섹션은 비워 두세요.
- 행을 삽입하려면 **추가** 버튼을 클릭하고, 삭제하려면 ✕ 버튼을 클릭하세요.

고정 헤더는 설정할 수 없음

`Content-Type`과 `Accept`는 커스텀 헤더로 추가할 수 없습니다. CLUe가 내부적으로 `Content-Type: application/json`과 `Accept: application/json`을 고정 값으로 전송하므로 관리자가 별도로 지정할 필요가 없습니다. 이 이름으로 헤더를 추가하려고 하면 저장되지 않습니다. 고객사 API는 이 두 헤더를 전제로 설계해야 합니다.

6 자동 필드 선택

자동 필드는 시스템이 요청 본문에 **자동으로 채우는 값**입니다. 사용할 수 있는 자동 필드는 크리덴셜 타입에 따라 달라집니다. 각 필드의 값 위치는 `{{...}}` **플레이스홀더**로 표시되며, 요청 시점에 실제 장치/사용자 값으로 대체됩니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

기본 키	플레이스홀더(값 위치)	사용 가능 대상	실제 값
`deviceId`	`{{DEVICE_SERIAL}}`	모든 크리덴셜 타입	요청한 장치의 일련번호
`userKey`	`{{USER_KEY}}`	얼굴 / 지문 / CLUe QR	CLUe가 관리하는 사용자 식별자
`rfCard`	`{{CARD_NUMBER}}`	RF 카드	제시한 카드 번호
`uniquePin`	`{{UNIQUE_PIN}}`	사용자 PIN	입력한 PIN 값
`qrCode`	`{{QR_CODE}}`	커스텀 QR	QR 페이로드

필드 선택 규칙

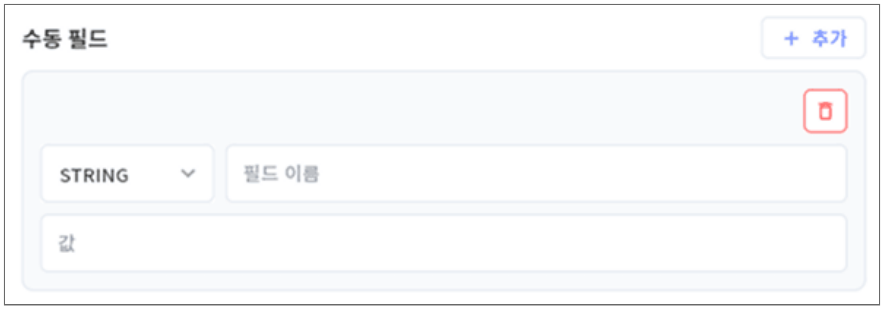
- 각 필드 왼쪽의 체크박스로 **요청에 포함할지 여부를 결정**합니다.
- 모두 선택할 필요는 없습니다. 고객사 API가 판정에 실제로 필요로 하는 값만 선택하세요. 불필요한 데이터를 줄이면 문제 진단이 쉬워집니다.
- 키(필드 이름)는 수정할 수 있습니다. 고객사 API가 요구하는 이름(예: `userKey → employeeId`)에 맞게 변경하세요. 값 위치의 플레이스홀더는 시스템이 고정하므로 변경할 수 없습니다.
- 각 필드의 데이터 형식(예: `STRING`)은 필드 오른쪽에 표시됩니다.

알아두기

- 5가지 외에 다른 플레이스홀더는 추가할 수 없습니다. 고객사 API가 추가 값을 요구한다면 수동 필드 추가를 참고하여 고정 값을 추가하거나, 고객사와 협의해 장치 일련번호나 사용자 키를 통해 고객사 측에서 파생하도록 처리하세요.
- 자동 필드와 수동 필드를 합쳐 요청 본문에 최대 **10개** 필드를 포함할 수 있습니다. 자동 필드를 많이 선택할수록 사용할 수 있는 수동 필드 수는 줄어듭니다.

7 수동 필드 추가

고객사 API가 고정 값을 요청에 포함하도록 요구할 때 수동 필드를 추가하세요.



필드	설명
필드 이름	필드 이름은 고유해야 하며, 자동 필드 이름과도 달라야 합니다.
필드 타입	`STRING`, `NUMBER`, `BOOLEAN` 중 선택하세요.
값	이 필드의 값을 입력하세요. 선택한 타입에 따라 적절한 JSON 데이터 타입으로 변환됩니다. 예: `NUMBER: 123`, `STRING: "123"`, `BOOLEAN: true/false`

- 자동 필드와 수동 필드를 합쳐 최대 **10개**까지 포함할 수 있습니다.
- 추가된 수동 필드가 없으면 **등록된 수동 필드가 없습니다.** 메시지가 표시됩니다.
- 행을 삽입하려면 **추가** 버튼을 클릭하고, 삭제하려면  버튼을 클릭하세요.

8 API 테스트 실행

기본 정보, 커스텀 헤더, 자동 필드, 수동 필드를 완료했다면, 판정 기준(judgment criteria)을 구성하기 전에 먼저 테스트를 실행하세요. 테스트로 얻은 실제 응답(response)은 판정 기준 구성(응답 파싱 구성)에 필요합니다.

API 추가 패널 오른쪽의 **API 테스트 콘솔**을 사용하세요.

9 테스트 파라미터

테스트 콘솔에 표시되는 입력 필드는 크리덴셜 타입에 따라 달라집니다. **장치 ID**(장치 일련번호)는 모든 타입에서 필수이며, 나머지 입력값은 해당 크리덴셜 타입에서 사용하는 값을 고객사가 관리하는 형식 그대로 입력합니다.

인증 방식	입력할 값	대응하는 플레이스홀더
모든 타입	**장치 ID** — 9~12자리 숫자, 장치 일련번호	{{DEVICE_SERIAL}}
얼굴 / 지문 / CLUe QR	**사용자 Key** — 1~64자, CLUe가 관리하는 사용자 식별자	{{USER_KEY}}
RF 카드	고객사가 관리하는 **카드 번호**	{{CARD_NUMBER}}
사용자 PIN	고객사가 관리하는 **사용자 PIN**	{{UNIQUE_PIN}}
커스텀 QR	고객사가 관리하는 **QR 페이로드**	{{QR_CODE}}

테스트 콘솔에 입력한 값은 자동 필드 플레이스홀더를 대체해 실제 요청 본문으로 전송됩니다. 테스트할 때는 고객사 데이터베이스에 실제로 존재하는 값을 입력해 허용과 거부 응답을 모두 확인하세요. 실제 운영 환경에서는 장치가 인식한 값이 자동으로 대입됩니다.

10 테스트 실행

1. 콘솔 하단의 **테스트 실행** 버튼을 클릭하세요.
2. 테스트를 실행하는 동안 진행 표시가 나타납니다.
3. 결과를 받으면 요청/응답 내용이 **터미널 출력** 콘솔 영역에 표시됩니다.

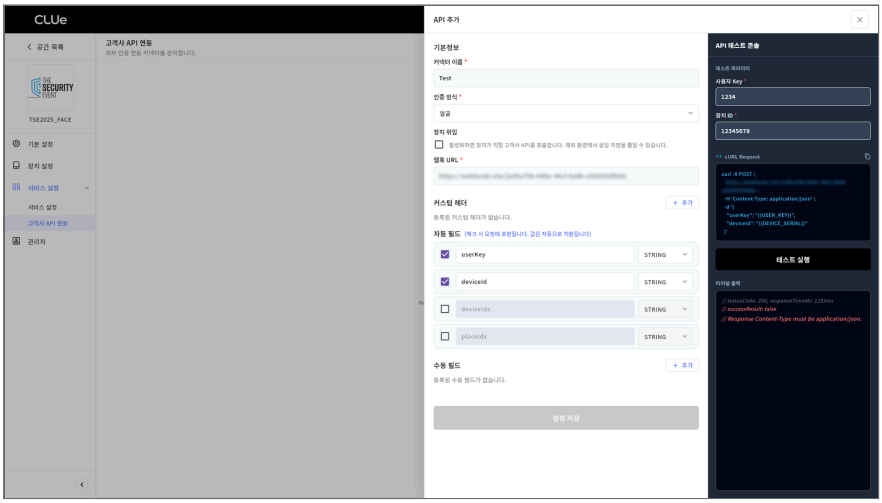
실행 중 패널을 닫거나 이전 단계로 이동하면 테스트가 중단됩니다.

응답을 성공적으로 받으면 다음 단계로 이동해 응답 내용을 기반으로 판정 기준(judgment criteria)을 구성하세요. URL, 헤더, 필드 설정 문제로 응답을 받지 못했다면 해당 입력값을 검토한 후 다시 테스트하세요.

> **저장하기 전 필수 조건**
>
> **설정 저장** 버튼은 최소 한 번 테스트에 성공해야 활성화됩니다. 여기서 성공이란 고객사 서버로부터 어떤 형태로든 HTTP 응답(4xx, 5xx 포함)을 받은 것을 의미합니다. 네트워크 오류로 응답을 받지 못했다면 저장할 수 없습니다.

11 테스트 실패 예시 — 응답 본문이 JSON이 아닐 때

고객사 서버가 응답을 반환하더라도 본문이 JSON 형식이 아니거나 응답 헤더의 `Content-Type`이 `application/json`이 아니면, 테스트 콘솔에 오류와 함께 실패 로그가 표시되고 **설정 저장** 버튼은 활성화되지 않습니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

응답 규격을 참고하여 고객사 담당자와 함께 API가 다음 두 조건을 모두 충족하는지 확인하세요.

- 응답 헤더에 `Content-Type: application/json`이 포함되어 있는지
- 응답 본문이 유효한 JSON인지(HTML 오류 페이지, 일반 텍스트, XML 등이 아닌지)

12 응답 파싱 구성

받은 응답을 기준으로, 이 단계에서 어떤 응답을 출입 허용(성공)으로 해석할지 정의합니다. 설정한 기준에 일치하는 응답은 출입 허용으로, 나머지는 모두 출입 거부로 처리합니다.

판정 모드는 입력한 필드에 따라 자동 결정됩니다. **statusCode**와 **성공 결과 JSONPath** 중 최소 하나는 반드시 입력해야 하며, 둘 다 비워두면 저장할 수 없습니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

#	모드	입력	성공 기준
1	응답 코드 검증	**statusCode** only	HTTP 상태 코드가 목록의 값 중 하나와 일치하면 성공합니다.
2	응답 본문 검증	**성공 결과 JSONPath** only	HTTP 응답 코드와 관계없이 본문의 `Key = Value` 조건을 충족하면 성공합니다. 조건을 충족하면 4xx/5xx 응답이라도 허용됩니다.

#	모드	입력	성공 기준
3	결합 검증	둘 다	상태 코드가 일치하고 동시에 본문 조건도 충족할 때 성공합니다. 상태 코드가 일치하지 않으면 본문은 평가하지 않습니다.

statusCode (모드 1, 3에서 사용)

- 100~399 범위의 정수만 지정할 수 있습니다. `4xx`, `5xx` 코드는 성공으로 지정할 수 없습니다.
- 최대 3개까지 지정할 수 있으며, 중복된 값은 허용되지 않습니다.
- 여러 값을 지정하면 그중 하나라도 일치하면 성공(예: `200`, `201`)으로 처리합니다.

성공 결과 JSONPath (모드 2, 3에서 사용)

- 성공 응답을 식별할 `Key`, `Value`, 데이터 형식(`BOOLEAN`, `STRING`, `NUMBER`)을 입력합니다.
- 성공 키 조건은 1개만 설정할 수 있습니다.
- 이 조건에 일치하지 않는 응답은 출입 거부로 처리됩니다.

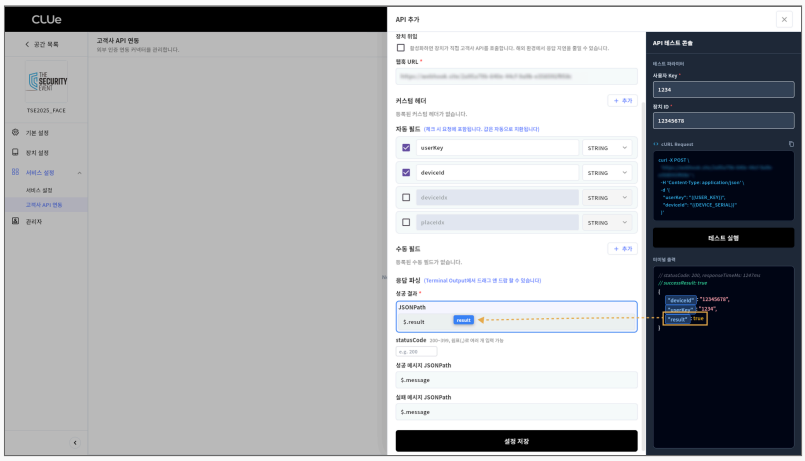
성공 메시지 JSONPath / **실패 메시지 JSONPath** (선택 사항)

- 인증 성공/실패 시 각각 장치 화면에 표시할 문자열을 추출할 키를 지정합니다. 일반적으로 `$.message`를 사용합니다.
- 지정하지 않아도 저장할 수 있습니다. 비워두면 허용/거부만 판정하고 장치 화면에는 메시지가 표시되지 않습니다.
- 성공과 실패에 서로 다른 키를 지정할 수 있습니다.
- 지정한 키의 값은 반드시 문자열이어야 하며, 장치 화면 크기를 고려해 너무 길지 않아야 합니다.

팁

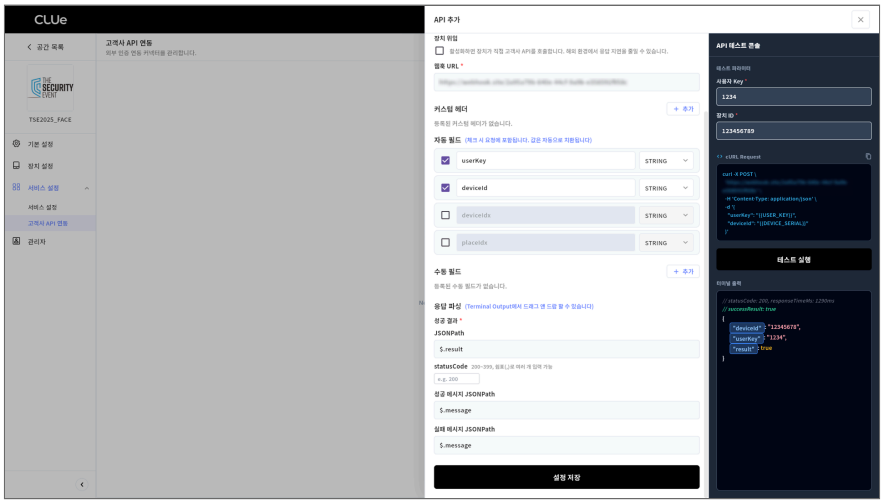
JSONPath를 직접 입력하기 어렵다면

응답 영역에서 필드를 **성공 결과 JSONPath**, **성공 메시지 JSONPath**, **실패 메시지 JSONPath** 입력란에 드래그 앤 드롭하면 JSON 경로가 자동으로 채워집니다. JSONPath를 직접 작성할 필요가 없습니다.



13 저장

API 추가 패널 하단의 **설정 저장** 버튼은 모든 필수 항목과 판정 기준이 올바르게 입력되고, API 테스트가 최소 한 번 성공했을 때 활성화됩니다.



- 필수 필드 누락, URL 형식 오류, 지정한 타입으로 변환할 수 없는 수동 필드 값, 판정 기준 미입력, 테스트 미성공(네트워크 오류 포함) 중 하나라도 해당하면 **설정 저장** 버튼은 비활성화된 상태로 유지됩니다.

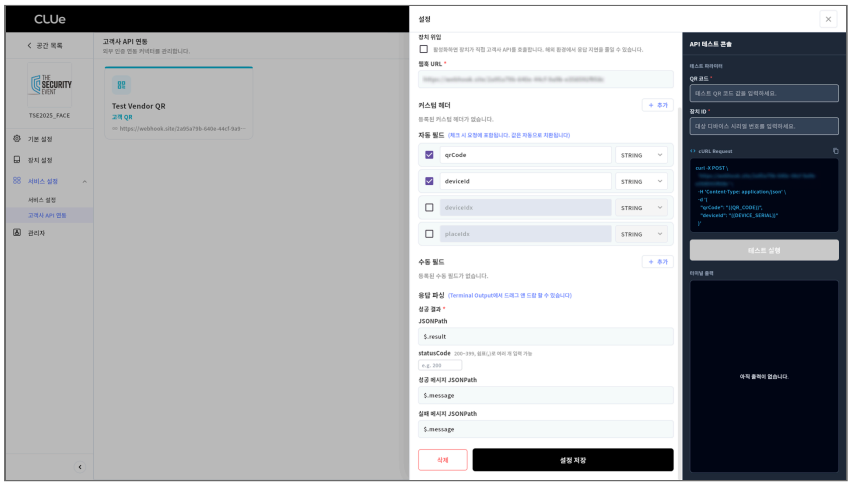
- 등록을 완료하려면 **설정 저장** 버튼을 클릭하세요.

API를 저장하면 패널이 닫히고 새로 등록한 API가 목록에 카드로 표시됩니다. 카드에는 이름, 크리덴셜 타입, 등록된 URL 등의 정보가 표시됩니다.



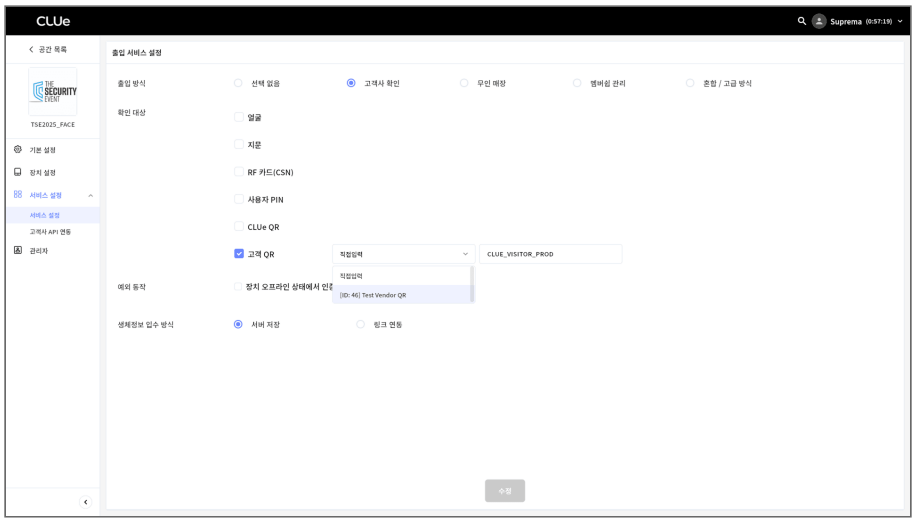
- API를 수정하려면 카드를 클릭하세요. 수정 패널이 열립니다. **커넥터 이름**, **웹훅 URL**, **자동 필드**, **수동 필드**, **응답 파싱**을 수정할 수 있습니다. **인증 방식**은 수정할 수 없습니다.

- **삭제**: 등록한 API를 삭제합니다. 이 API가 크리덴셜에 연결되어 있었다면 해당 연결도 자동으로 해제되며 변경 사항이 즉시 장치에 적용됩니다. 연결이 해제된 크리덴셜은 이후 고객사 검증 없이 장치 자체 인증만으로 동작합니다. 운영 공백이 우려된다면 삭제하기 전에 대체 API를 먼저 등록하고 연결하세요.



3단계 — 각 크리덴셜에 API 할당

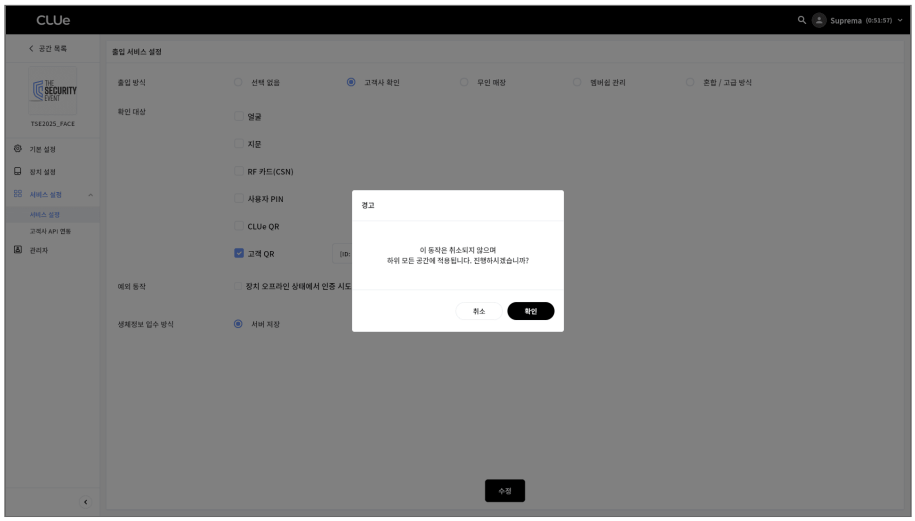
화면 왼쪽 사이드바에서 **서비스 설정** → **서비스 설정**을 클릭하세요. **확인 대상** 섹션에서 각 크리덴셜에 사용할 API를 지정하세요.



- 각 크리덴셜 옆의 드롭다운을 클릭하면 등록된 API 목록이 표시됩니다. 선택한 크리덴셜과 **인증 방식**이 일치하는 API만 표시됩니다.
- 얼굴, 지문, RF 카드, PIN, CLUe QR, 커스텀 QR, 각 크리덴셜에 사용할 API를 선택하세요. 크리덴셜마다 서로 다른 API를 지정할 수 있습니다.
- API를 지정하지 않은 크리덴셜은 장치 자체 인증만으로 동작합니다. 해당 크리덴셜에는 고객사 API로 검증 요청이 전송되지 않습니다. 고객사 검증이 필요 없다고 판정한 크리덴셜만 지정하지 않은 채로 두세요.

저장과 적용 규칙

크리덴셜에 등록한 API를 지정하고 **수정** 버튼을 클릭하면 변경 사항을 하위 공간에 적용할지 묻는 확인 대화상자가 나타납니다.



- **확인**: 동일한 설정이 현재 공간 그룹의 모든 하위 공간에 즉시 적용됩니다. 기존의 공간별 재정의는 공간 그룹 값으로 덮어쓰기됩니다.
- **취소**: 변경 사항을 저장하지 않습니다.

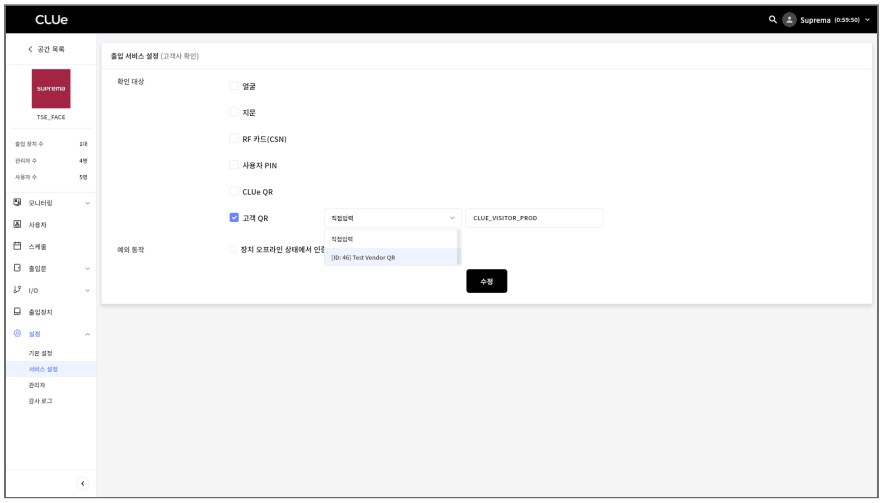
대부분 공간 그룹 레벨 설정만으로 모든 하위 공간을 동일하게 운영할 수 있습니다. 특정 공간에 다른 API를 재정의하려면 4단계 — 공간별 재정의 설정(선택 사항)를 참고하세요.

4단계 — 공간별 재정의 설정(선택 사항)

공간 그룹에서 상속받은 설정과 다르게 특정 공간에만 다른 API를 지정하는 방법을 안내합니다. 특정 공간에만 적용한 설정은 다른 공간이나

상위 공간 그룹에 영향을 주지 않습니다.

1. 공간 그룹 하위의 특정 공간으로 이동하세요.
2. 화면 왼쪽 사이드바에서 **설정** → **서비스 설정**을 클릭하세요.



3. **확인 대상** 섹션의 각 크리덴셜 드롭다운에서 **이 공간에만 사용할 다른 API**를 선택하세요.
4. 변경 사항을 저장하려면 **수정** 버튼을 클릭하세요.

변경 사항은 현재 공간에만 저장됩니다. 다른 공간에는 적용되지 않습니다.

> **알아두기**
> 해당 공간에 관리자로 초대된 공간 관리자만 **설정** → **서비스 설정**에 접근할 수 있습니다.

> **주의**
> 특정 공간에 API를 지정한 이후 상위 공간 그룹에서 크리덴셜-API 지정을 변경하고 저장하면, 공간별 재정의가 공간 그룹 값으로 덮어쓰기됩니다. 공간 그룹 변경 후에도 공간별 설정을 유지해야 한다면, 공간 그룹 업데이트 이후 특정 공간의 **설정** → **서비스 설정**에서 다시 지정해야 합니다.

입력 규칙 요약

필드	필수 여부	규칙
커넥터 이름	필수	최대 64자
인증 방식	필수	저장 후 변경 불가
웹훅 URL	필수	`https://` 필수 / 최대 512자 / CLUe는 이 URL에 **HTTP POST**/ `application/json` 요청만 전송
인증 방식 API 개수	-	크리덴셜 타입당 최대 **3개**의 API 등록 가능
커스텀 헤더	선택 사항	Key/Value 쌍 최대 10개 / 중복 이름 불가(대소문자 구분 없음)

필드	필수 여부	규칙
자동 필드	선택 사항	체크한 항목만 요청에 포함 / 키(이름)는 수정 가능 / 값은 시스템이 자동으로 채움
수동 필드	선택 사항	자동 필드와 합쳐 최대 **10개** 등록 / 중복 이름 불가 / 값은 지정한 타입(`STRING` / `NUMBER` / `BOOLEAN`)에 따라 JSON 데이터로 변환됨
사용자 Key(테스트)	**인증 방식**에 따라 다름	1~64자
장치 ID(테스트)	필수	9~12자리 숫자만
응답 파싱	-	**statusCode** 또는 **성공 결과 JSONPath** 중 최소 하나 **필수**(둘 다 입력하면 결합 검증 활성화)
statusCode	-	100~399 범위의 정수 / 최대 3개 / 중복 불가
성공 결과 JSONPath	-	1개 항목: `Key` + `Value` + 데이터 형식(`BOOLEAN` / `STRING` / `NUMBER`)
성공 메시지 JSONPath/**실패 메시지 JSONPath**	선택 사항	지정하면 응답 본문에서 추출할 키(값은 문자열이어야 하며 장치 화면 크기 고려 필요), 지정하지 않으면 장치에 메시지가 표시되지 않음
저장 조건	-	테스트에 성공해야만 저장 가능

문제 해결

출입 문제(단계별 진단)

설정 워크플로우 개요를 참고하여 문제 영역을 좁혀 나가세요.

단계	증상	확인 사항
1	특정 크리덴셜이 인식되지 않음	크리덴셜이 장치에 등록되고 활성화되어 있는지 확인하세요.
2	장치-서버 간 통신 실패	네트워크 연결 상태, 장치 등록 상태를 확인하세요.
3	요청이 고객사 서버에 도달하지 않음	등록된 URL(HTTPS), 커스텀 헤더, 방화벽 규칙을 확인하세요.
4	고객사가 응답하지만 모든 시도가 거부됨	판정 기준(판정 모드, 성공 키/값, HTTP 상태 코드)을 확인하세요.
5	허용/거부는 올바르게 동작하지만 메시지가 표시되지 않음	**성공 메시지 JSONPath**/**실패 메시지 JSONPath**, 응답 본문의 메시지 문자열을 확인하세요.

설정 저장 버튼 비활성화

설정 저장 버튼을 클릭할 수 없다면 다음 항목을 순서대로 확인하세요.

- **필수 필드**: **커넥터 이름**, **인증 방식**, **웹훅 URL** 중 비어 있는 항목이 있는지 확인하세요.

- **웹훅 URL**: `https://`로 시작하는지, 최대 길이(512자)를 초과하지 않는지 확인하세요.
- **수동 필드**: 값을 지정한 타입(`STRING` / `NUMBER` / `BOOLEAN`)으로 변환할 수 있는지 확인하세요

  > *예: `NUMBER`에 숫자가 아닌 문자를 입력했을 때*

- **응답 파싱**: **statusCode** 또는 **성공 결과 JSONPath** 중 최소 하나를 입력했는지 확인하세요.
  - **성공 결과 JSONPath**를 사용한다면 `Key`, `Value`, 데이터 형식을 모두 입력했는지 확인하세요.
  - **성공 메시지 JSONPath**/**실패 메시지 JSONPath**는 선택 사항이며 저장에 영향을 주지 않습니다.
- **API 테스트**: 최소 한 번 테스트에 성공했는지 확인하세요. 테스트 성공 없이는 저장할 수 없습니다.

테스트 실패

테스트 실패는 세 가지 유형으로 나뉩니다.

- (A) 입력값 검증 단계에서 차단됨
- (B) 요청은 전송됐지만 테스트 실패
- (C) 응답은 받았지만 예상한 결과가 아님

(A) 입력값 검증 단계에서 차단됨

입력값이 규칙에 맞지 않아 요청 자체가 전송되지 않습니다.

증상	확인 사항
Webhook URL 형식 오류	**웹훅 URL**이 `https://`로 시작하고 512자를 초과하지 않는지 확인하세요.
판정 기준 키 형식 오류	**성공 결과 JSONPath**/**성공 메시지 JSONPath**/**실패 메시지 JSONPath**가 `$.`로 시작하는 JSONPath 형식(최대 128자)인지 확인하세요.
판정 기준 미지정	**statusCode** 또는 **성공 결과 JSONPath** 중 최소 하나를 입력했는지 확인하세요.
성공 상태 코드 범위/개수 오류	각 값이 100~399 범위인지, 3개 이하인지, 중복이 없는지 확인하세요.
필드 키 중복	**자동 필드**와 **수동 필드**의 키가 서로 중복 없이 고유한지 확인하세요.
요청 헤더 키 중복	요청 헤더 키가 서로 중복 없이 고유한지(대소문자 구분 없음) 확인하세요.
제한된 헤더 이름 사용	`Content-Type` 또는 `Accept`를 커스텀 헤더로 추가했는지(대소문자 구분 없이 시스템 고정 값임) 확인하세요.
필드/헤더 개수 초과	**자동 필드** 및 **수동 필드** 필드 최대 10개, 커스텀 헤더 최대 10개인지 확인하세요.
인증 방식 등록 개수 초과	해당 크리덴셜 타입에 이미 3개의 API가 등록되어 있는지 확인하세요.
사용자 Key 형식 오류	테스트 콘솔의 **사용자 Key**가 허용된 문자(영문, 숫자, `-`, `_`, `@`, `.`) 범위와 1~64자 길이를 충족하는지 확인하세요.

증상	확인 사항
장치 ID 형식 오류	테스트 콘솔의 **장치 ID**가 9~12자리 숫자인지 확인하세요.

(B) 요청은 전송됐지만 테스트 실패

테스트 결과가 `success = false`로 표시되며, 이 상태에서는 저장할 수 없습니다.

증상	확인 사항
연결 실패/네트워크 오류(고객사 서버로부터 응답을 받지 못함)	고객사 서버의 외부 접근 가능 여부, HTTPS 인증서 유효성, 방화벽/포트 설정, 커스텀 헤더(만료된 토큰, 오타)
타임아웃(응답 없음)	고객사 서버의 응답 지연, 네트워크 상태. 테스트는 몇 초 내에 응답이 없으면 실패로 처리함
응답은 받았지만 본문이 JSON이 아님	고객사가 JSON 응답을 반환하는지, 응답 `Content-Type`이 `application/json`으로 설정되어 있는지. HTML 오류 페이지, 빈 텍스트 등이 여기에 해당함

(C) 응답은 받았지만 예상한 결과가 아님

`success = true`와 함께 실제 HTTP 상태 코드가 **statusCode**에, 고객사의 원본 응답이 **터미널 출력**에 표시됩니다. 저장 가능하며, 이 단계에서 응답을 기준으로 응답 파싱을 구성해야 합니다.

증상	확인 사항
상태 코드는 받았지만 모든 출입이 거부됨	**모드 1, 3**: 성공으로 인정하는 상태 코드 목록 확인하세요. **모드 2**: 본문의 키/값 조건을 확인하세요. 상태 코드는 무시됩니다.
본문 필드 조건이 일치하지 않음	**성공 결과 JSONPath**에 입력한 `Key`, `Value`, 데이터 형식(`BOOLEAN` / `STRING` / `NUMBER`)을 다시 확인하세요. 응답이 `"true"`(STRING)인지 `true`(BOOLEAN)인지 확인하세요. 타입이 일치해야 합니다.
수동 필드가 요청 본문에서 잘못된 형식으로 표시됨	**수동 필드** 타입(`STRING` / `NUMBER` / `BOOLEAN`)이 실제 입력값과 일치하는지 다시 확인하세요.

> **알아두기**
>
> - 테스트 API는 응답 본문을 파싱하지 않고 그대로 표시하므로, **터미널 출력**에 표시된 실제 응답 JSON을 참고해 JSONPath, 키, 값 설정을 맞추세요.
> - 장치 쪽에서 실패 원인을 찾아내려면 출입 문제(단계별 진단)를 참고하세요.

이름 중복 문제

자동 필드와 **수동 필드**의 키 이름은 서로 중복될 수 없습니다. 요청 헤더 키도 서로 중복될 수 없습니다. **자동 필드** 키 이름을 변경했다면 **수동 필드**와 충돌하지 않는지 확인하세요.

장치에 메시지 표시되지 않음

- 응답 본문에 **성공 메시지 JSONPath** 또는 **실패 메시지 JSONPath**로 지정한 필드가 실제로 존재하는지 확인하세요.
- 해당 키의 값이 **문자열**인지 확인하세요. 숫자, 객체, 배열은 표시되지 않습니다.
- 설정한 **성공 메시지 JSONPath** / **실패 메시지 JSONPath** 이름이 실제 응답의 키와 정확히 일치하는지 확인하세요.

펌웨어 변경하기

CLUe에서 지원하는 장치는 다음과 같습니다. 펌웨어 한 번의 업데이트만으로 기존 BioStar 지원 모드에서 CLUe 지원 모드로 전환할 수 있습니다.

- BioStation 3, BioEntry W3, BioEntry W2, BioLite N2, X-Station 2, XPass 2

> **주의**
> 펌웨어 업데이트를 수행하기 전에 **장치에 사용자 정보가 남아 있지 않도록 확인하세요.** 사용자 데이터가 남아 있으면 CLUe 시스템에서 동기화되는 사용자 정보와 충돌이 발생할 수 있습니다.

CLUe 지원 모드로 전환

> **알아두기**
> 펌웨어 업데이트 전에 장치를 미리 등록하려면 장치 시리얼 번호(SN)와 모델명(예: BS3-DB)을 슈프리마 기술 지원팀(CS@suprema.co.kr)에 제공해 주세요. 사전 등록 절차를 진행해 드립니다.

1 CLUe 지원 펌웨어 버전 준비

슈프리마 현지 지사 또는 CLUe 팀을 통해 제공받을 수 있습니다. 장치에 적용할 수 있는 버전은 아래와 같습니다.

- *xpass2_v1_x_CL-AU.bin*
- *bs3-all_v1.x._CL-AU.bin*
- *xs2-all_v1.x CL-AU.zip*
- *bln2-oab_v1.x CL-AU.bin*
- *bln2-odb_v1.x CL-AU.bin*
- *bln2-pab_v1.x CL-AU.bin*
- *bew3-all_v1.x CL-AU.bin*
- *bew2_oa/d/hp_v1.x CL-AU.bin*

> **알아두기**
> 접미사 `AU`는 'Auto Update to CLUe FW'를 의미합니다.

2 인터넷 연결 확인

펌웨어를 업데이트하기 전에 장치가 인터넷과 CLUe 서버에 연결할 수 있는지 확인하세요.

CLUe 펌웨어 업데이트 후 장치는 CLUe 서버에서 인증서를 자동으로 가져와 적용한 뒤 연결을 시도하므로, 인터넷 연결이 반드시 필요합니다. 또한 장치는 기본적으로 DHCP를 통해 IP 주소를 할당받으므로, 동적 IP 주소를 할당할 수 있는지 확인하세요.

- 기본 네트워크 설정은 DHCP입니다.
- 8.8.8.8 DNS 서버를 사용합니다.

3 펌웨어 업데이트 진행

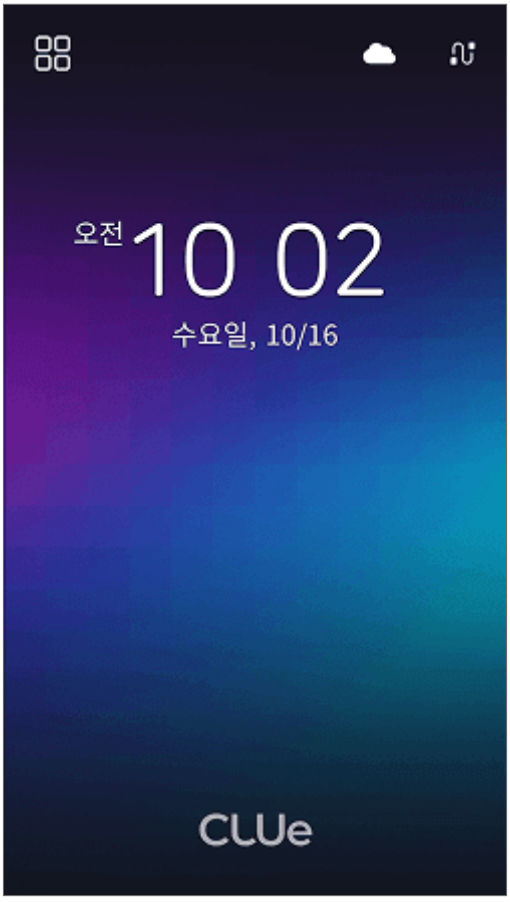
업데이트 과정에서 장치는 최소 2~3회 재부팅됩니다.

메인 펌웨어 업데이트에는 다소 시간이 걸릴 수 있으며, 인증서 및 설정 펌웨어를 가져오는 과정은 비교적 짧게 완료됩니다. 전체 과정은 약 3~5분이 소요되므로, 업데이트가 완료될 때까지 장치의 전원과 인터넷 연결 상태를 유지하세요.

> **알아두기**
> BioStar 2 또는 USB를 이용해 펌웨어를 업데이트할 수도 있습니다.

4 업데이트 완료 확인

모든 업데이트가 완료되면 장치 메인 화면에 CLUe 아이콘이 표시됩니다.



디스플레이가 없는 장치는 CLUe 포털에서 시리얼 번호를 입력하여 장치 등록 상태를 확인할 수 있습니다.

5 장치 등록

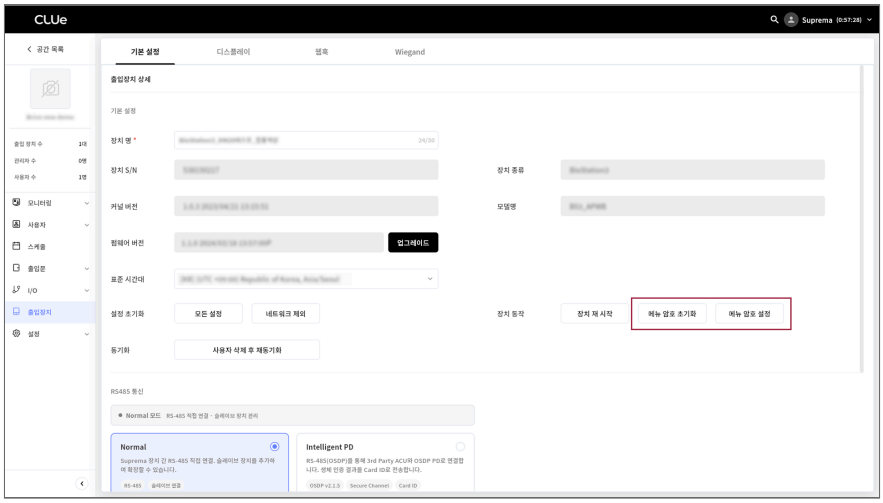
슈프리마 담당자에게 포털을 통해 장치를 계정에 할당해 달라고 요청하세요.

그런 다음 지정된 공간에 장치를 배정하고 출입문 설정과 함께 사용할 수 있습니다. 안전한 장치 관리를 위해 CLUe 시스템은 각 브랜치 관리자가 장치를 해당 공간 그룹에 할당하도록 요구합니다.

6 장치 메뉴 비밀번호 설정

펌웨어 업데이트 후 LCD 디스플레이가 있는 장치는 메뉴 비밀번호를 설정하라는 메시지가 표시됩니다. 화면의 안내에 따라 비밀번호를 설정하세요. 비밀번호는 CLUe 포털을 통해서도 설정할 수 있습니다.

BioStar 장치와 달리 CLUe 장치는 사용자 데이터 없이 사용되는 경우가 많습니다. 따라서 메뉴 설정을 무단으로 변경하지 않도록 메뉴 비밀번호를 설정해야 합니다.



문제 해결

장치 화면에 클라우드 아이콘이 표시되지 않는다면 다음 사항을 확인하세요.

- 먼저 인터넷 연결 상태를 확인하세요. 장치가 클라우드 서버에 직접 연결되므로 반드시 인터넷에 연결되어 있어야 합니다. 또한 CLUe 펌웨어는 아웃바운드 통신에 표준 HTTPS 포트 443을 사용합니다.
- 클라우드 아이콘이 여전히 표시되지 않는다면 장치에서 **Ping 테스트**를 실행해 인터넷 연결 상태를 확인하세요.

장치	경로
BioStation 3	메뉴() → **설정** → **통신** → **이더넷** → **Ping 테스트**
BioLite N2	**ESC** → **네트워크** → **TCP/IP** → **Ping 테스트**
X-Station 2	메뉴() → **통신** → **이더넷** → **Ping 테스트**

  - **Ping 테스트 성공** 팝업이 표시되면 인터넷 연결에는 문제가 없는 상태입니다.
  - **알 수 없음(Unknown)** 또는 **실패(Fail)** 팝업이 표시되면 해당 DNS 사용을 네트워크에서 차단하고 있는지 확인하세요.

장치 추가하기

CLUe 장치를 사용하려면 웹 포털에서 **등록**과 **할당**을 완료해야 합니다. 장치 등록은 브랜치 관리자만 수행할 수 있으며, 등록이 완료된 장치는 대리점 관리자 또는 공간 그룹 관리자가 담당 공간에 할당합니다.

신규 장치를 구매한 고객은 CLUe 펌웨어와 인증서가 적용되었는지 확인한 후, 슈프리마 지점에 장치 등록을 요청하세요.

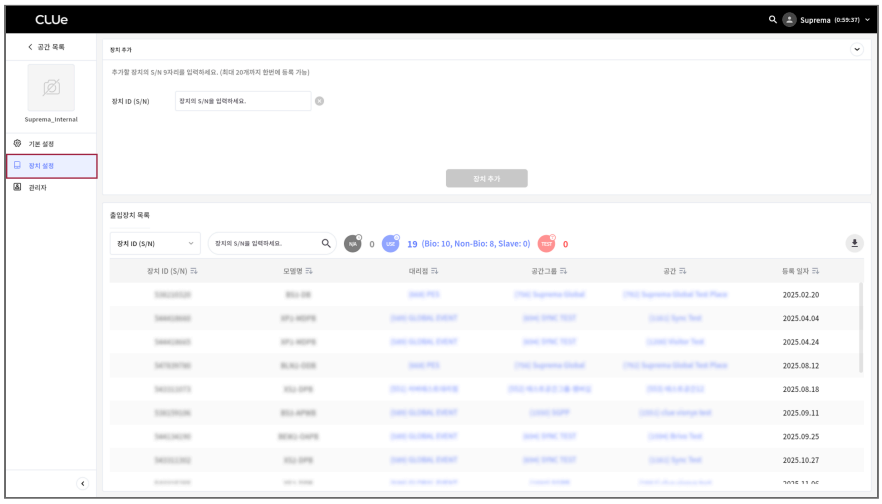
장치 등록(브랜치 관리자)

브랜치 관리자만 장치를 등록할 수 있습니다. 장치를 등록하기 전에 장치 시리얼 번호를 확인하세요. 시리얼 번호는 장치 뒷면에 부착된 스티커에서 확인할 수 있습니다.

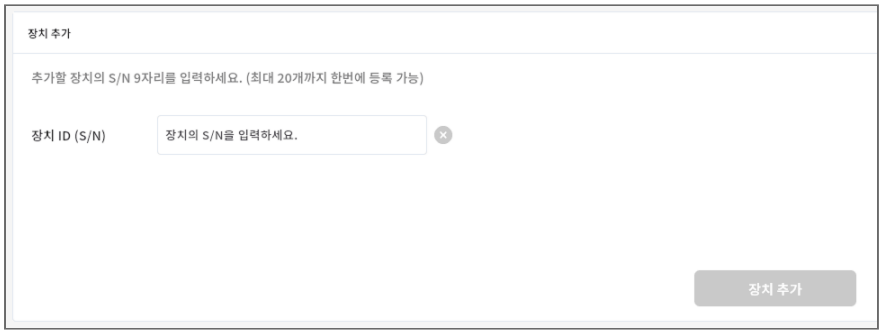
1. CLUe 웹 포털에 로그인하세요.
2. 초기 화면에서 장치를 등록할 브랜치를 선택하세요.
3. 화면 오른쪽 상단에서 ⋮ → **상세 설정**을 클릭하세요.



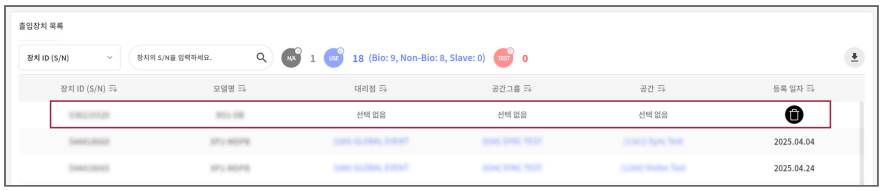
4. 화면 왼쪽 사이드바에서 **장치 설정**을 클릭하세요.



5. **장치 추가** 섹션의 **장치 ID (S/N)** 입력 필드에 장치 시리얼 번호를 입력하고 **추가** 버튼을 클릭하세요.



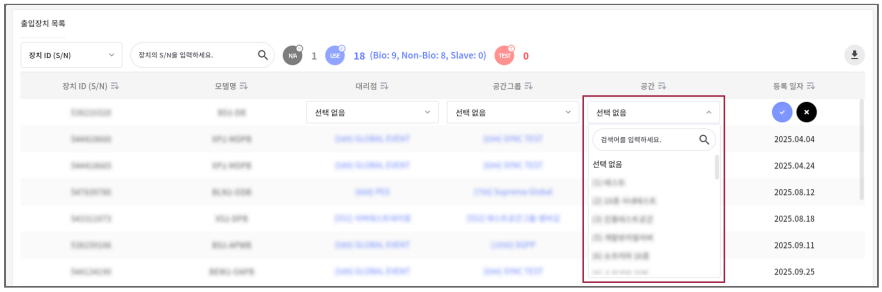
6. **출입장치 목록**에 추가한 장치가 표시됩니다.



7. 편집 모드를 활성화하려면 **선택 없음** 필드를 클릭하고  버튼을 선택하세요.



8. 장치를 할당할 대리점, 공간그룹, 공간을 선택하세요.



9. 선택한 항목을 적용하려면  버튼을 클릭하세요.

장치 할당 성공 메시지가 화면 상단에 표시됩니다. 각 필드를 클릭하면 해당 대리점, 공간그룹, 공간으로 이동할 수 있는  버튼이 활성화됩니다. 버튼을 클릭하면 해당 위치로 이동한 후 장치와 출입문을 설정할 수 있습니다.



장치 할당

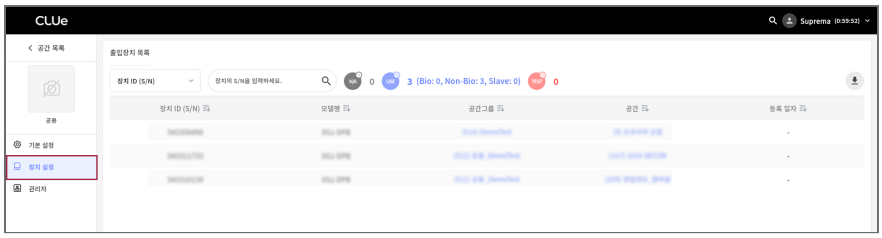
대리점 관리자

대리점 관리자는 자신에게 할당된 장치를 하위 공간 그룹 또는 개별 공간에 배정할 수 있습니다. 등록이 필요한 장치가 목록에 표시되지 않는다면 해당 슈프리마 지사 또는 본사에 문의하세요.

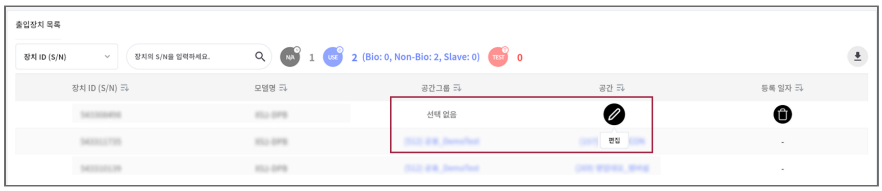
1. CLUe 웹 포털에 로그인하세요.
2. 초기 화면에서 장치를 할당할 대리점을 선택하세요.
3. 화면 오른쪽 상단에서 ⋮ → **상세 설정**을 클릭하세요.



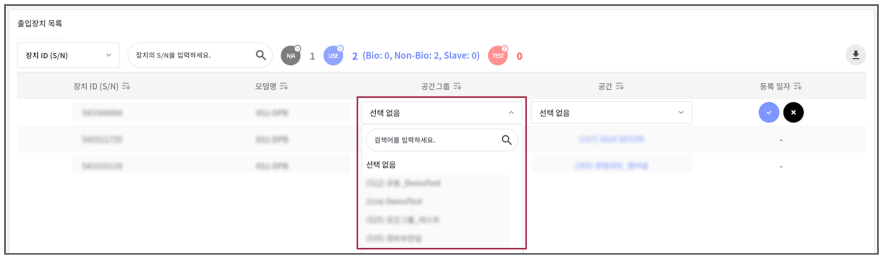
4. 화면 왼쪽 사이드바에서 **장치 설정**을 클릭하세요.



5. 편집 모드를 활성화하려면 **선택 없음** 필드를 클릭하고 버튼을 선택하세요.

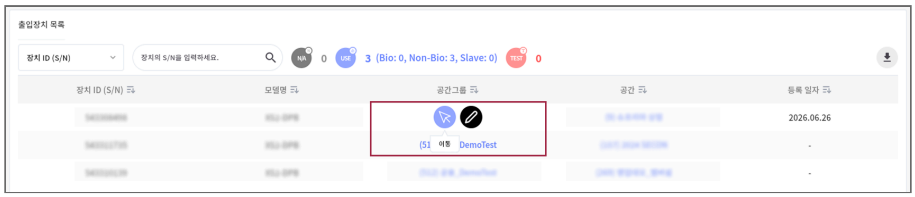


6. 장치를 할당할 공간그룹 또는 공간을 선택하세요.



7. 선택한 항목을 적용하려면 버튼을 클릭하세요.

장치 할당 성공 메시지가 화면 상단에 표시됩니다. 각 필드를 클릭하면 해당 공간그룹, 공간으로 이동할 수 있는 버튼이 활성화됩니다. 할당 후 공간으로 이동하여 출입문을 추가하는 것을 권장합니다.



알아두기

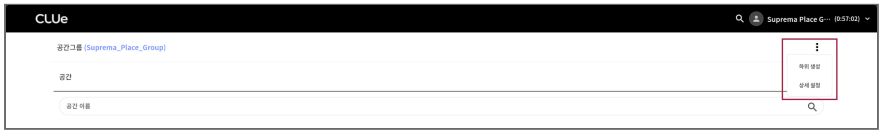
- 대리점 관리자는 개인 정보 보호 정책에 따라 기본적으로 사용자 및 모니터링 탭을 볼 수 없습니다. 접근이 필요하다면 공간그룹, 공간 관리자에게 초대를 요청하세요.
- 장치를 삭제하면 자동으로 브랜치 레벨의 장치 목록으로 돌아가며 미할당 상태가 됩니다. 실수로 장치를 삭제했다면 브랜치 관리자에게 재할당을 요청하세요.

공간 그룹 관리자

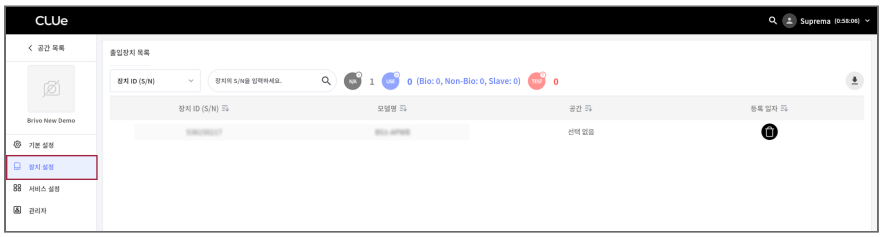
공간 그룹 관리자는 자신에게 할당된 장치를 하위 공간에 할당할 수 있습니다.

1. CLUe 웹 포털에 로그인하세요.
2. 초기 화면에서 장치를 할당할 공간 그룹을 선택하세요.

3. 화면 오른쪽 상단에서 ⋮ → **상세 설정**을 클릭하세요.



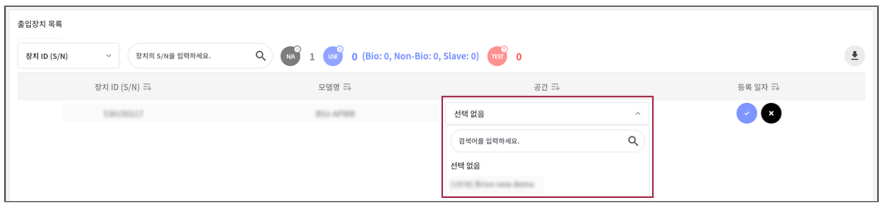
4. 화면 왼쪽 사이드바에서 **장치 설정**을 클릭하세요.



5. 편집 모드를 활성화하려면 **선택 없음** 필드를 클릭하고 ✎ 버튼을 선택하세요.



6. 장치를 할당할 공간을 선택하세요.



7. 선택한 항목을 적용하려면 ✓ 버튼을 클릭하세요.

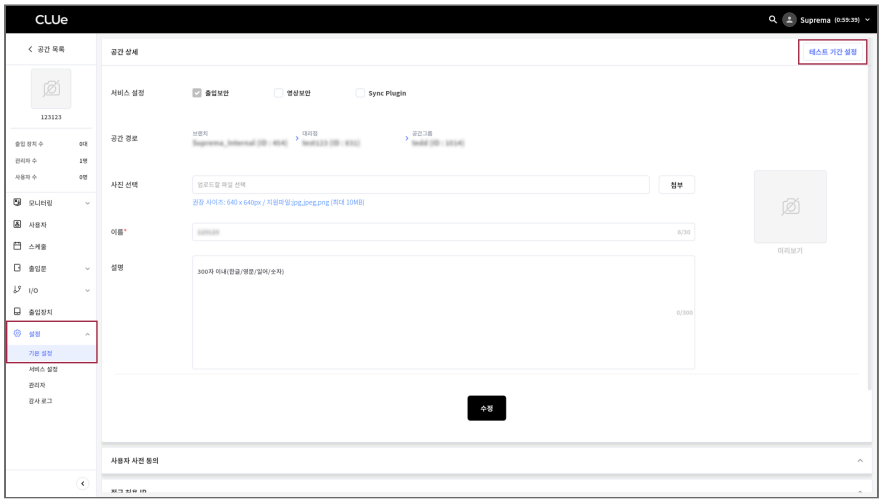
장치 할당 성공 메시지가 화면 상단에 표시됩니다. 장치 할당 후 해당 공간으로 이동하여 출입문을 추가하는 것을 권장합니다.



테스트 공간 설정(브랜치 관리자)

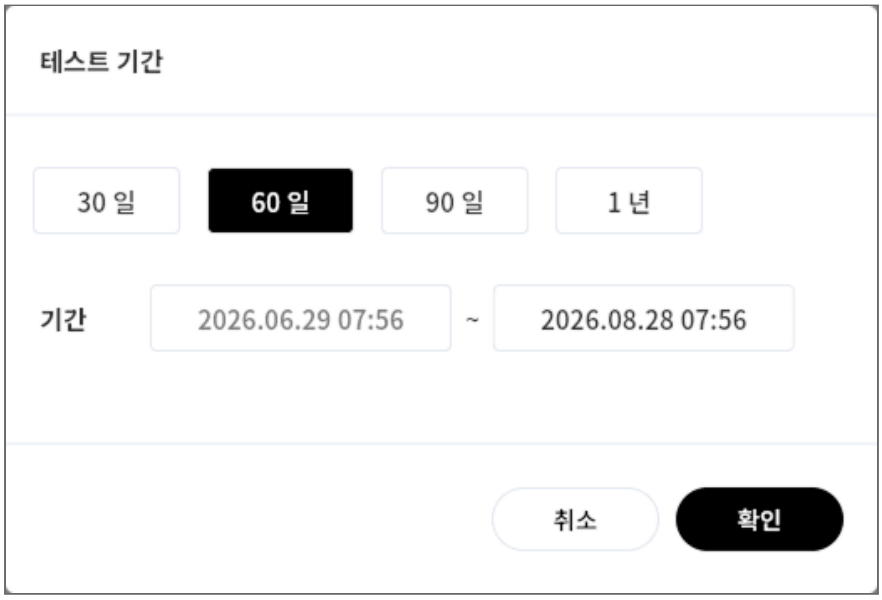
구독은 장치 수를 기준으로 하므로, 테스트 장치를 구분하여 전체 합산에서 제외해야 합니다. 이를 위해 브랜치 관리자 역할의 사용자는 공간 설정에서 특정 공간을 '테스트 공간'으로 지정할 수 있습니다.

1. CLUe 웹 포털에 로그인하세요.
2. 테스트 공간으로 지정할 공간을 선택하세요.
3. 화면 왼쪽 사이드바에서 **설정** → **기본 설정**을 클릭하세요.



4. 화면 오른쪽 상단의 **테스트 기간 설정**을 클릭하세요.

5. **테스트 기간** 팝업이 나타나면 테스트 기간을 설정하세요.



   기간 제한 없이 사용하려면 종료 날짜를 **9999.12.31 23:59**로 설정하세요.

6. 설정을 완료하려면 **확인** 버튼을 클릭하세요.

공간에 속한 모든 장치가 장치 목록에서 빨간색으로 표시되어 테스트 장치로 구분됩니다. 전체 수량 정보도 함께 확인할 수 있습니다.



다음 단계

장치의 펌웨어 업그레이드 방법을 확인하세요.

장치 셀프 등록하기

설치 기사가 CLUe 포털에 로그인할 수 없는 현장에서도, 관리자가 미리 준비해 둔 정보만으로 장치를 공간에 등록할 수 있습니다. 이 기능을 장치 셀프 등록(Device Self-Registration)이라고 하며, 관리자가 사전에 준비하는 **관리자 준비 단계**와 설치 기사가 현장에서 수행하는 **현장 등록 단계**로 나뉩니다.

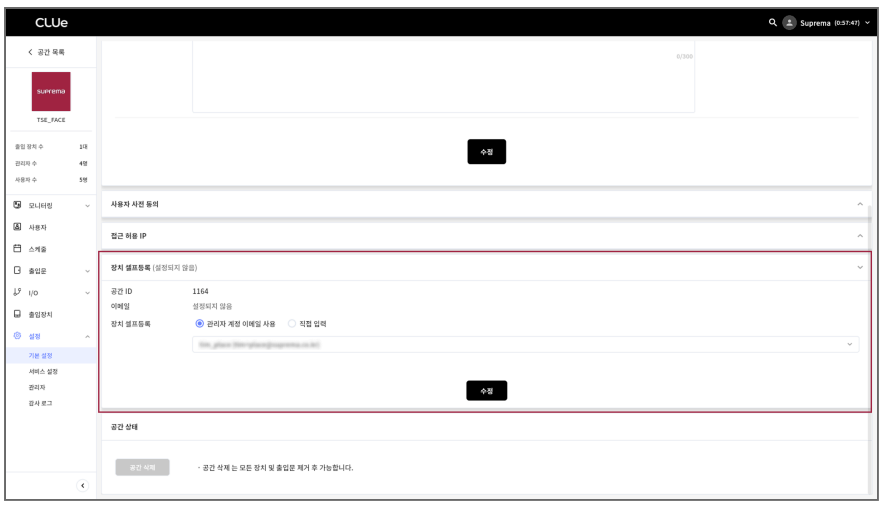
지원하는 장치 및 펌웨어 버전

장치 모델	지원 펌웨어 버전
X-Station 2	2026.06.01 이상
BioStation 3	2026.05.26 이상
BioLite N2	2026.06.01 이상
XPass 2	2026.06.01 이상
BioEntry W3	미지원
BioEntry W2	미지원

관리자 준비 단계

현장 등록을 시작하기 전에 공간 관리자는 CLUe 포털에서 공간 ID를 확인하고 장치 할당 이메일 주소를 설정해야 합니다. 설정하지 않으면 현장에서 할당 코드를 받을 수 없습니다. 공간 관리자 이상의 권한으로 초대된 관리자만 접근할 수 있습니다.

1. CLUe 웹 포털에 로그인하세요.
2. 장치를 할당할 공간으로 이동하세요.
3. 화면 왼쪽 사이드바에서 **설정** → **기본 설정**을 클릭하세요.
4. **장치 셀프등록** 섹션을 클릭하세요.



공간 구역ID(읽기 전용) 필드와 **장치 셀프등록** 이메일 주소 입력란이 있습니다.

공간 ID 확인

공간 구역ID는 읽기 전용입니다. 이 번호를 현장 설치 기사에게 전달하세요. 설치 기사는 장치에 공간 ID를 그대로 입력해 등록을 진행할 수 있습니다. 공간 ID를 잘못 입력하는 것이 등록 실패의 가장 흔한 원인이므로, 정확하게 전달해야 합니다.



장치 할당 이메일 주소 설정

장치 할당 이메일 주소는 두 가지 방법 중 하나로 설정하세요.



- **관리자 계정 이메일 사용**: 현재 로그인한 관리자 계정의 이메일 주소가 자동으로 입력됩니다.
- **직접 입력**: 임의의 이메일 주소를 직접 입력하세요. 일반적인 이메일 주소 형식(최대 254자)으로 입력할 수 있습니다.

두 방법 모두 입력한 이메일 주소가 서버에 그대로 저장됩니다. 시스템은 수신자가 관리자인지, 현장 설치 기사인지, 제3자인지 구분하지 않습니다. 공간마다 할당 이메일은 하나만 설정할 수 있습니다. 새 공간을 만들면 할당 이메일은 설정되지 않은 상태로 시작하므로, 셀프 등록 기능을 사용하려면 먼저 이메일을 설정해야 합니다.

> **이메일을 설정하지 않으면 어떻게 되나요?**
>
> 할당 이메일이 설정되지 않은 공간에서 설치 기사가 **할당 코드 전송**을 실행하면 "관리자가 먼저 할당 이메일 주소를 설정해야 합니다."라는 오류가 표시됩니다.

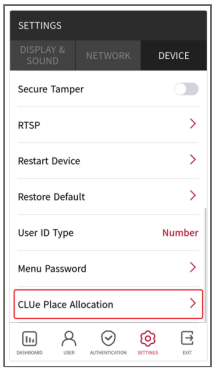
현장 등록 단계

LCD가 있는 장치(LCD 장치 셀프 등록)와 LCD가 없는 장치(LCD가 없는 장치 셀프 등록(웹 서버))의 등록 절차는 같은 원리로 동작하며 화면만 다릅니다. 먼저 공통 적용되는 개념을 설명합니다.

단계	동작	결과
할당 코드 전송	공간 ID를 입력한 후 **할당 코드 전송**을 실행하세요.	서버가 6자리 할당 코드를 생성해 공간의 할당 이메일로 전송합니다.
할당 코드 입력	지정된 시간 안에 이메일로 받은 코드를 입력하세요.	코드가 일치하면 장치가 해당 공간에 등록됩니다.

LCD 장치 셀프 등록

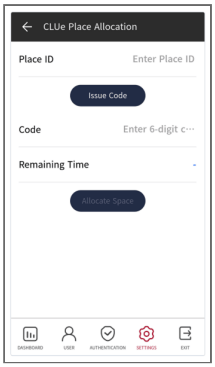
아래 화면은 예시이며, 실제 화면 구성과 버튼 이름은 장치 모델과 펌웨어 버전에 따라 다를 수 있습니다. 화면에 표시되는 안내 문구를 기준으로 진행하세요.



1 공간 등록으로 이동

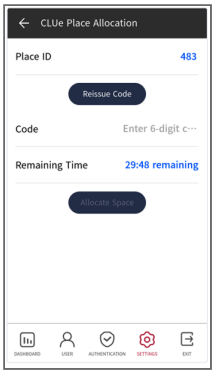
장치 설정 메뉴에서 **DEVICE → CLUe Place Allocation**을 선택하세요. 공간 등록 화면으로 이동합니다.

> **알아두기**
>
> - 메뉴 이름과 위치는 장치 모델과 펌웨어 버전에 따라 다를 수 있습니다.
> - 장치가 이미 특정 공간(또는 공간 그룹, 대리점, 브랜치)에 속해 있다면 등록 화면에 들어갈 수 없으며 이미 등록되었다는 메시지가 표시됩니다.



2 공간 ID 입력

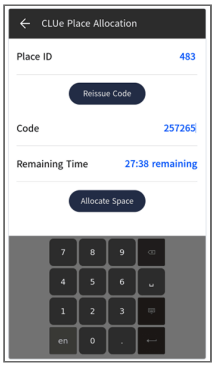
관리자로부터 받은 공간 ID를 숫자 키패드로 입력하세요. 존재하지 않는 ID나 공간이 아닌 브랜치, 대리점, 공간 그룹 ID를 입력하면 오류 메시지가 표시됩니다. 공간 ID를 다시 확인한 후 입력하세요.



3 할당 코드 전송

공간 ID를 입력하고 **Issue Code**를 실행하세요. 서버가 6자리 할당 코드를 생성해 해당 공간의 할당 이메일로 전송합니다. 장치는 할당 코드 입력 화면으로 전환됩니다.

> **알아두기**
>
> 할당 이메일이 설정되어 있지 않으면 오류 메시지가 표시됩니다. 이때는 관리자에게 할당 이메일 설정을 요청하세요.



4 할당 코드 입력

할당 이메일로 받은 6자리 코드를 30분 안에 입력하세요. 코드가 만료되었거나 일치하지 않으면 오류 메시지가 표시됩니다.

> **알아두기**
>
> - 코드를 다시 입력하거나 새 코드를 요청하려면 **Reissue Code** 버튼을 탭하세요.
> - 코드를 5회 연속 잘못 입력하면 발급된 코드는 폐기됩니다. 이전 단계로 돌아가 새 코드를 요청하세요.

5 등록 완료

Allocate Space 버튼을 탭하세요. 코드가 일치하면 장치가 해당 공간에 등록되고 화면에 등록 완료(성공) 메시지가 표시됩니다. 이후 장치는 일반 출입 동작 화면으로 전환됩니다.

등록된 장치는 현장에서 공간을 변경할 수 없습니다. 변경이 필요하다면 CLUe 포털에서 진행하세요.

LCD가 없는 장치 셀프 등록(웹 서버)

LCD가 없는 장치는 장치 본체에서 공간을 등록할 수 없습니다. 장치와 같은 네트워크에 연결된 PC나 모바일 기기의 웹 브라우저를 통해 장치의 웹 서버로 접속해 등록을 진행해야 합니다.

장치 웹 서버 접속

대상 장치와 같은 네트워크에 연결된 기기의 웹 브라우저 주소창에 다음 주소를 입력해 접속하세요.

> *https://* `{device_IP_address}` : `{port}` — 예: *https://192.168.0.27:8443*

- 장치의 IP 주소와 포트를 확인하는 방법은 기기별 설치 가이드를 참고하세요.
- 자체 서명 인증서를 사용한다면 브라우저에 "안전하지 않음(Not Secure)"이라는 보안 경고가 표시될 수 있습니다. 계속 진행하면 등록 화면이 열립니다.

장치가 아직 어떤 공간에도 등록되지 않았다면 공간 등록 화면(**CLUe Device Web Panel**)이 표시됩니다. 장치가 특정 공간에 속해 있다면 이미 등록되었다는 메시지가 표시되며 등록 화면에 접근할 수 없습니다.

웹에서 등록

다음 안내에 따라 장치 셀프 등록을 진행하세요.



1 공간 ID 입력

관리자로부터 받은 공간 ID를 **Place ID** 입력 필드에 입력하세요. 존재하지 않는 ID나 최하위 공간이 아닌 ID를 입력하면 오류 메시지가 표시됩니다. 공간 ID를 다시 확인한 후 입력하세요.

2 할당 코드 전송

공간 ID를 입력하고 **Issue Code** 버튼을 클릭하세요. 서버가 6자리 할당 코드를 생성해 해당 공간의 할당 이메일로 전송합니다.

> **알아두기**
> 할당 이메일이 설정되어 있지 않으면 오류 메시지가 표시됩니다. 이때는 관리자에게 할당 이메일 설정을 요청하세요.

3 할당 코드 입력

할당 이메일로 받은 6자리 코드를 30분 안에 입력하세요. 코드가 만료되었거나 일치하지 않으면 오류 메시지가 표시됩니다.

> **알아두기**
>
> - 현재 등록 상태를 확인하려면 **Check Status** 버튼을 클릭하세요.
> - 코드를 다시 받으려면 **Reissue Code** 버튼을 클릭하세요. 단, 같은 장치는 이전 코드 전송 이후 60초가 지나야 다시 전송할 수 있습니다.
> - 코드를 5회 연속 잘못 입력하면 발급된 코드는 폐기됩니다. 이전 단계로 돌아가 새 코드를 요청하세요.

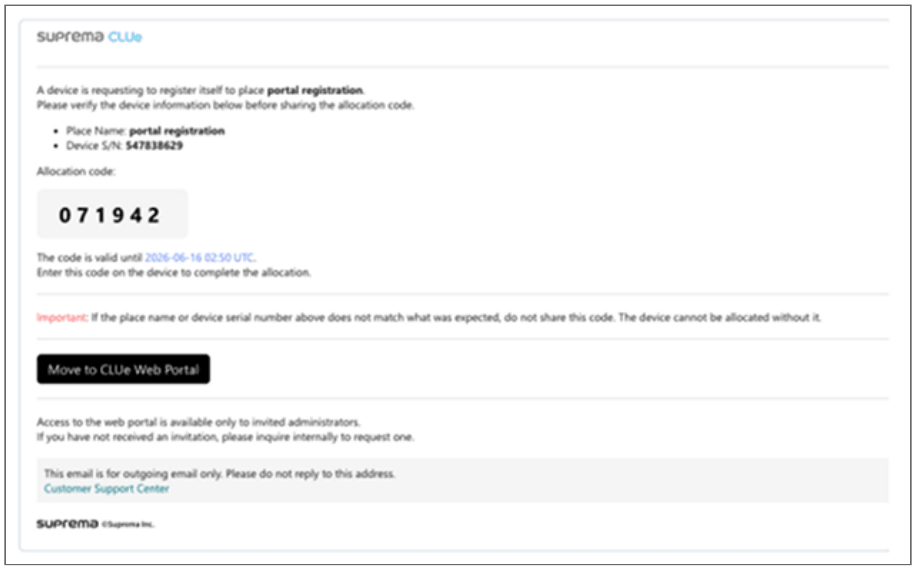
4 등록 완료

Allocate Space 버튼을 클릭하세요. 코드가 일치하면 장치가 해당 공간에 등록되고 완료 메시지가 표시됩니다. 등록을 완료하면 웹 서버는 약 3분간만 더 동작한 후 자동 종료됩니다. 이후 같은 주소로 접속을 시도해도 연결되지 않습니다. 이는 불필요한 리소스 소모를 막고 보안을 강화하기 위한 정상 동작입니다. 등록 후 공간을 변경하려면 CLUe 포털에서 진행하세요.

참고 사항

할당 코드 이메일 확인

할당 코드 전송(Issue Code)을 실행하면 공간에 설정된 할당 이메일 주소로 할당 코드 이메일을 발송합니다. 할당 코드를 입력하기 전에 수신자는 이메일 본문을 통해 등록 대상이 올바른지 확인해야 합니다.



이메일 제목에는 장치 시리얼 번호(deviceSn)가 포함되어 있습니다. 받은 편지함 목록에서 제목만 보고도 어떤 장치의 코드인지 확인할 수 있습니다. 여러 장치를 동시에 설치할 때는 제목의 시리얼 번호로 해당 장치의 이메일을 구분하세요.

이미 등록된 장치(재등록 제한)

이미 특정 공간(또는 공간 그룹, 대리점, 브랜치)에 속한 장치는 현장에서 다시 등록할 수 없습니다. LCD 장치에서 등록 메뉴(**CLUe Place Allocation**)에 들어가거나 LCD가 없는 장치의 웹 서버에 접속하면 다음 메시지가 표시되며 등록 화면 접근이 차단됩니다.

> *This device is already registered. Changes can be made from the CLUe portal.*

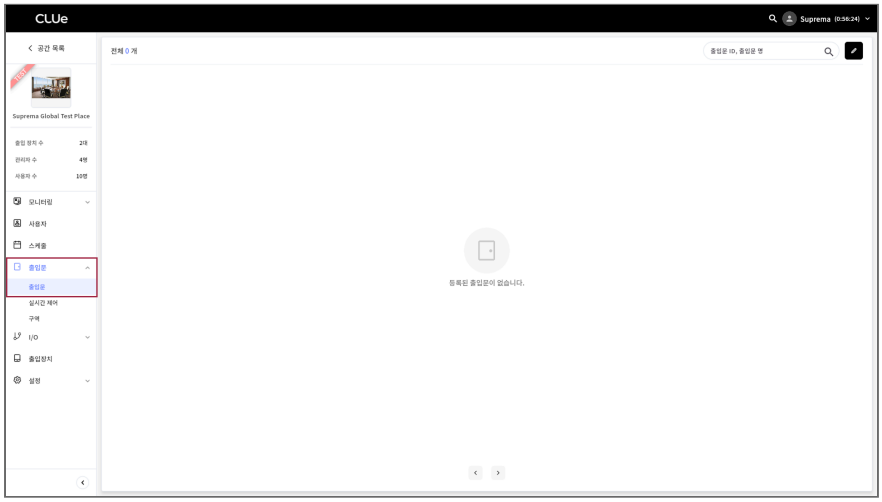
공간 변경이나 해제는 CLUe 포털에서만 가능하며 현장에서는 수행할 수 없습니다. 드물게 장치 자체는 특정 공간에 속하지 않은 것처럼 보여도 서버에는 이미 등록된 경우(예: 포털에서 사전 등록된 경우)가 있습니다. 이때도 **할당 코드 전송**을 실행하면 동일하게 이미 등록되었다는 오류 메시지가 표시됩니다. 마찬가지로 포털에서 변경을 진행해야 합니다.

출입문 추가하기

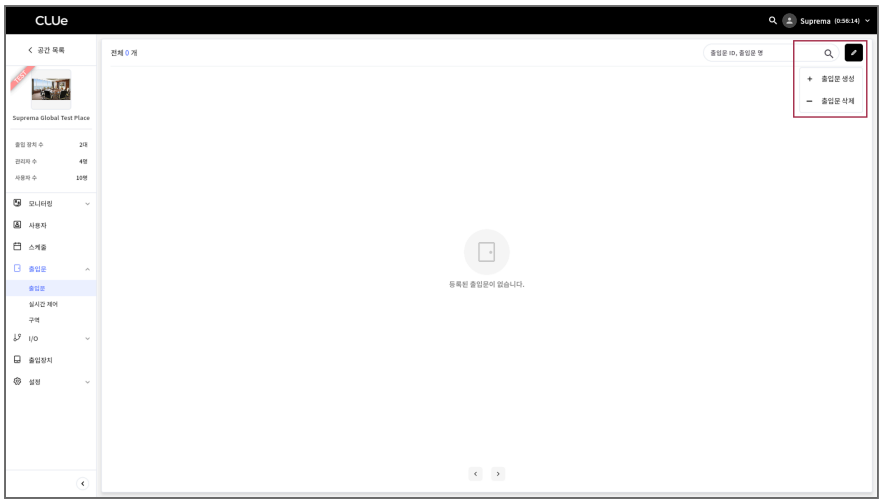
CLUe에서 출입문 설정은 필수입니다. 출입문을 설정하지 않으면 사용자 동기화를 포함한 서버와의 통신이 정상 동작하지 않으므로, 서비스 시작 전에 반드시 완료하세요.

출입문 설정

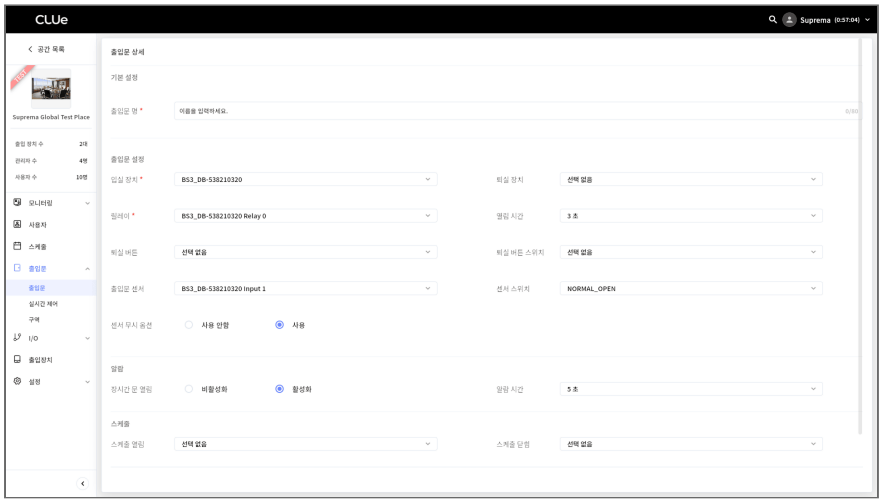
1. CLUe 웹 포털에 로그인하세요.
2. 출입문을 추가할 공간을 선택하세요.
3. 화면 왼쪽 사이드바에서 **출입문** → **출입문**을 클릭하세요.



4. 화면 오른쪽 상단의  → **출입문 생성**을 클릭하세요.



5. 출입문 이름을 입력하고 입실 장치, 릴레이, 퇴실 버튼 등 기타 필요한 설정을 선택하세요.



6. 출입문 설정을 완료한 후 **생성** 버튼을 클릭하세요.

> **알아두기**
>
> **센서 무시 옵션**
>
> - **사용**: 출입문 센서 상태와 관계없이 잠금 시간이 경과된 후 출입문 릴레이의 상태가 전환됩니다.
> - **사용 안함**: 출입문 센서가 열림 상태를 감지해도 출입문 릴레이가 원래 상태로 전환되지 않습니다. 자동문을 구성한다면 이 옵션을 선택하세요.

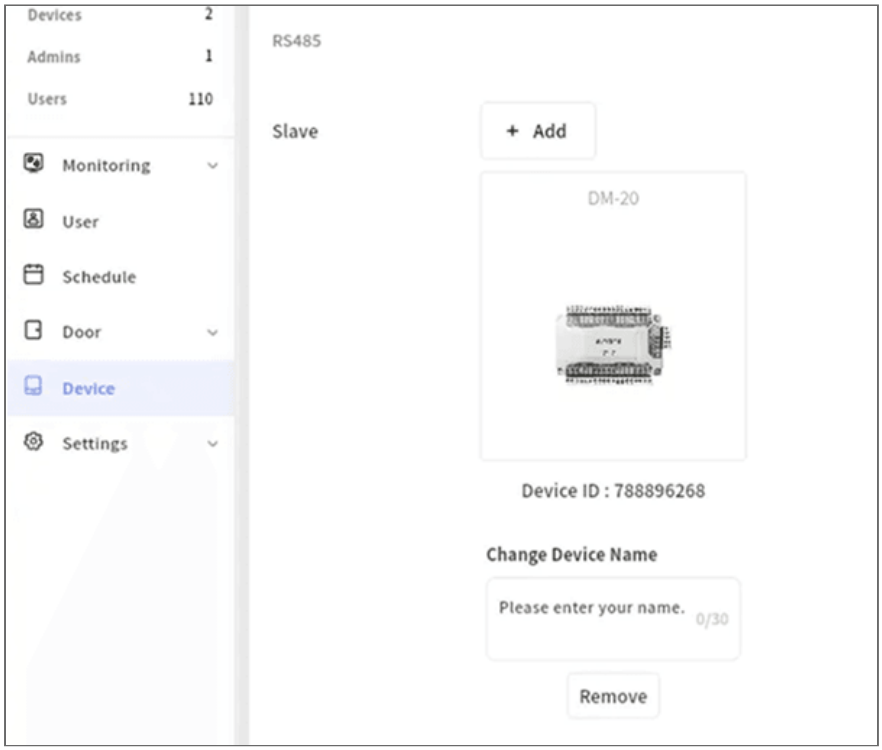
슬레이브 장치 릴레이 사용

SIO2, DM-20, DI-24와 같은 RS485 슬레이브 장치를 사용한다면, 마스터 장치에 연결되어 있어도 별도의 공간에 할당해야 합니다. 일반 장치와 동일한 방법으로 공간에 할당하세요. 장치를 공간에 할당하는 방법은 장치 추가하기를 참고하세요.

- 장치 목록에서 슬레이브 장치를 확인하세요.



- 마스터 장치를 선택하고 연결된 슬레이브 장치를 추가하세요. 이후 슬레이브 장치의 릴레이와 입력 포트를 사용할 수 있습니다.


Devices 2
Admins 1
Users 110
Monitoring
User
Schedule
Door
Device
Settings
RS485
Slave
+ Add
DM-20
Device ID : 788896268
Change Device Name
Please enter your name.
0/30
Remove

펌웨어 업그레이드하기

CLUe 장치의 펌웨어를 최신 버전으로 업그레이드하면 새로운 기능과 성능 개선, 보안 패치를 적용할 수 있습니다. 업그레이드는 CLUe 웹 포털에서 몇 번의 클릭만으로 진행되며, 완료까지 약 5~10분이 걸립니다.

업그레이드를 시작하기 전에 다음 사항을 확인하세요.

- 업그레이드 중에는 장치를 사용할 수 없으며, 재시작 시 잠금 장치 연결 방식에 따라 출입문이 순간적으로 열리거나 닫힐 수 있습니다.
- 업그레이드 중 장치 설정을 변경하면 완료 후에 반영됩니다.

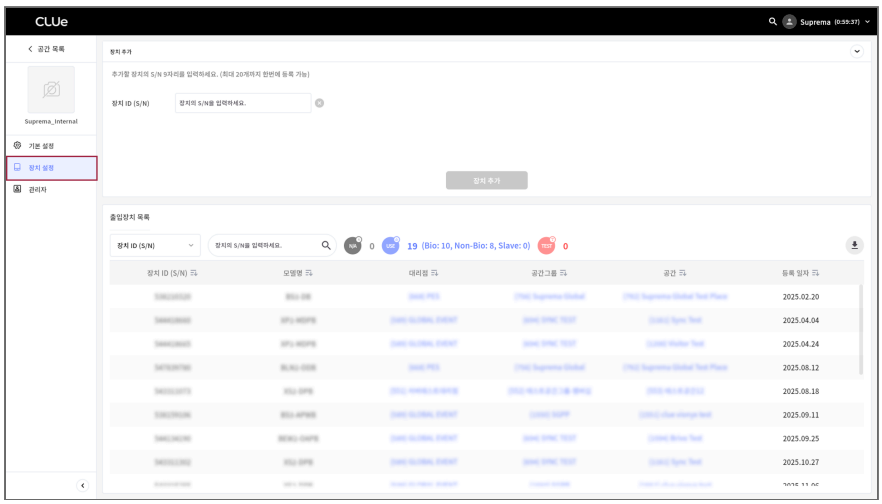
공간으로 이동

공간에 할당된 출입 장치를 업그레이드하려면 해당 공간으로 바로 이동하거나, 상위 브랜치 또는 대리점, 공간 그룹을 통해 이동할 수 있습니다.

1. CLUe 웹 포털에 로그인하세요.
2. 초기 화면에서 브랜치 또는 대리점, 공간 그룹을 선택하세요.
3. 화면 오른쪽 상단의 ⋮ → **상세 설정**을 클릭하세요.



4. 화면 왼쪽 사이드바에서 **장치 설정**을 클릭하세요.



5. **출입장치 목록**에서 펌웨어를 업그레이드할 장치의 **공간** 열을 클릭하세요.

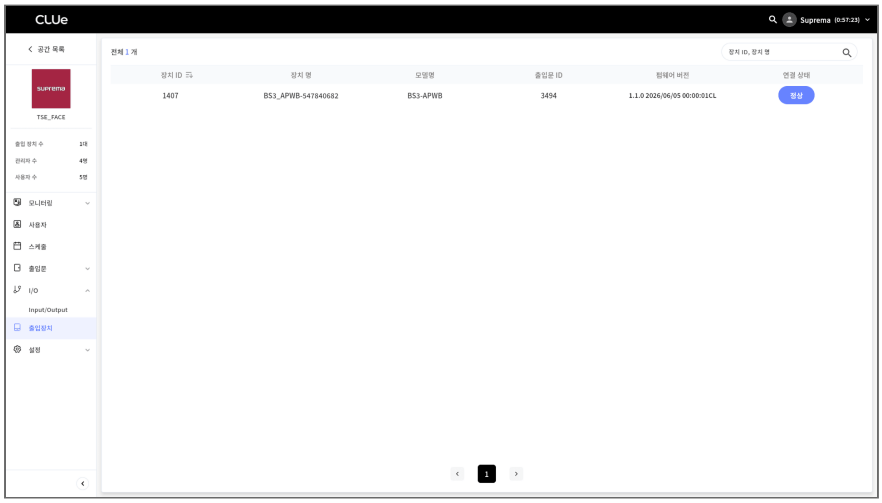


6. 버튼이 활성화되면 클릭하세요.

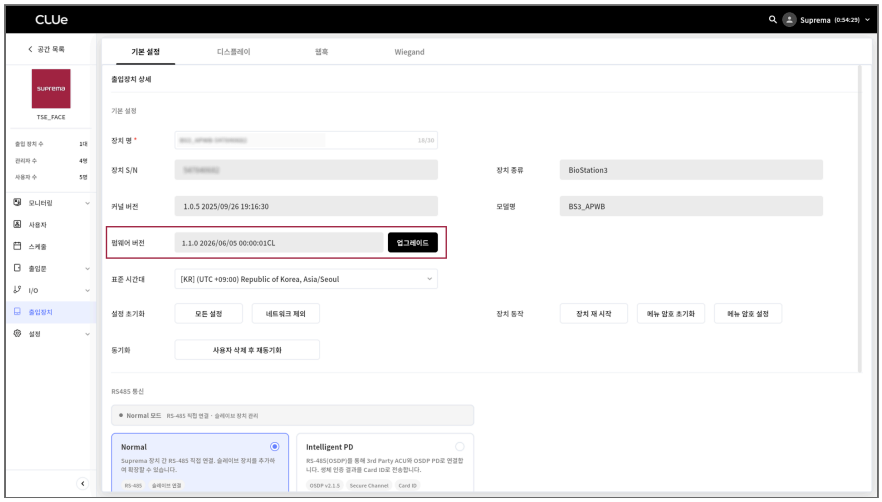
선택한 장치가 할당된 공간의 **출입장치** 화면으로 이동합니다.

펌웨어 업그레이드

1. 장치가 할당된 공간의 **출입장치** 목록에서 펌웨어를 업그레이드할 장치를 클릭하세요.

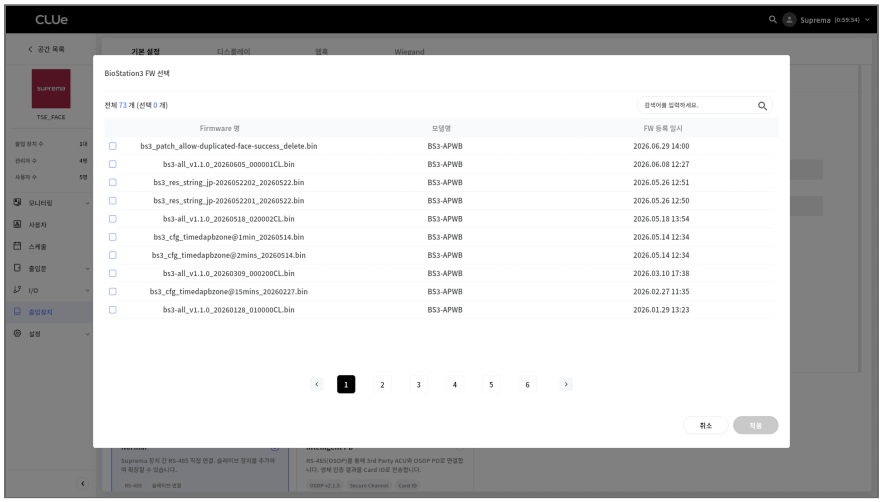


2. 선택한 장치의 **기본 설정** 화면이 나타나면 **펌웨어 버전** 항목에서 현재 펌웨어 버전을 확인하세요.



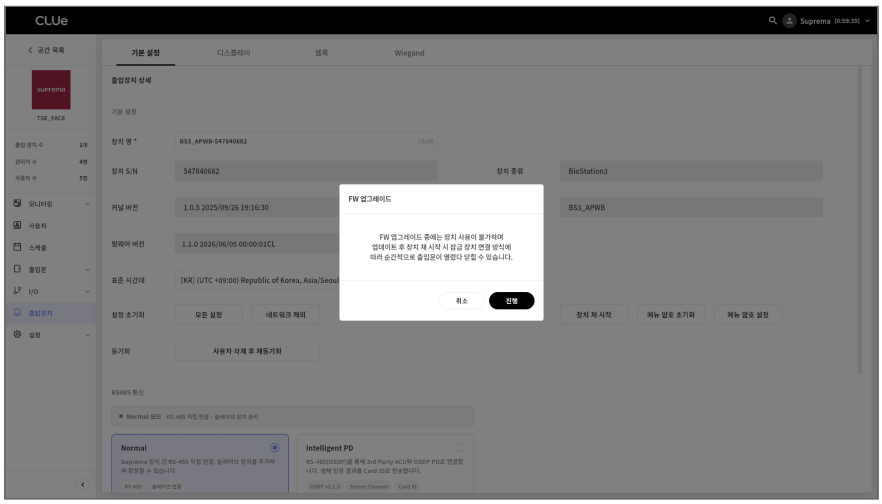
3. **업그레이드** 버튼을 클릭하세요.

4. 펌웨어 선택 창이 나타나면 업그레이드할 펌웨어의 체크박스를 클릭하세요.

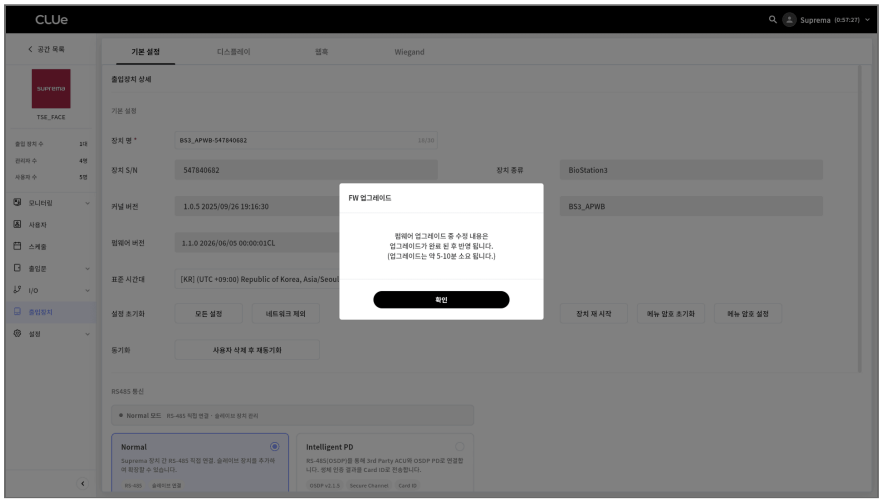


> 한 개의 펌웨어 버전만 선택할 수 있습니다.

5. 오른쪽 하단의 **적용** 버튼을 클릭하세요.
6. 업그레이드 확인 창이 나타나면 **진행** 버튼을 클릭하세요.



7. 메시지 창이 나타나면 내용을 확인 후 **확인** 버튼을 클릭하세요.



장치 웹훅(Webhook) 설정하기

CLUe 포털에서 웹훅(Webhook)을 설정하면, 지정한 이벤트가 발생했을 때 장치가 사용자가 지정한 엔드포인트(외부 서버)로 실시간 이벤트를 전송합니다. 이 기능으로 다음과 같은 사용 사례를 구현할 수 있습니다.

- **근태 기록 시스템**과의 연동
- **중복 얼굴 감지** 이벤트 수신

이 외에도 시스템과의 다양한 실시간 이벤트 기반 연동에 활용할 수 있습니다.

지원 장치

장치	모델	지원 펌웨어 버전
BioStation 3	BS3-DB, BS3-APWB	`bs3-all_v1.1.0_20250626` 이상

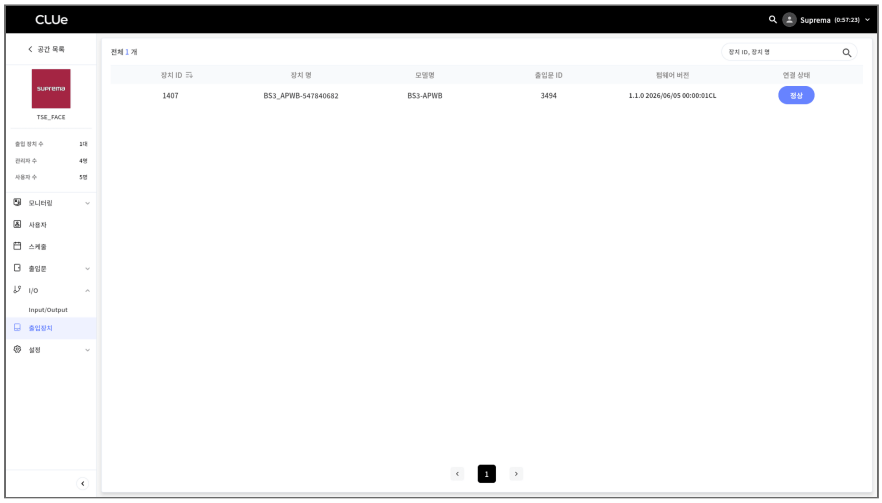
> **알아두기**
> 다음 CLUe 지원 장치도 웹훅을 지원할 예정입니다.
> - BioEntry W3, BioLite N2, X-Station 2, XPass 2

주요 장점

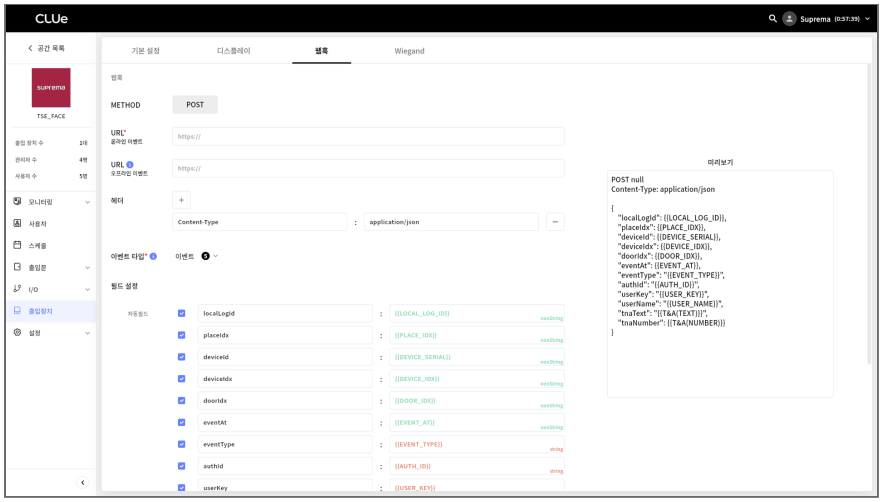
- 장치의 실시간 이벤트 알림을 외부 시스템으로 전송할 수 있습니다.
- 웹훅을 통해 외부 시스템과 손쉽게 연동할 수 있습니다.
- 인사 근태 연동, 보안 이벤트 모니터링 등의 사용 사례를 지원합니다.

웹훅 설정

1. CLUe 웹 포털에 로그인하세요.
2. 웹훅을 설정할 장치가 할당된 공간으로 이동하세요.
3. 화면 왼쪽 사이드바에서 **출입장치**를 클릭하세요.
4. 장치 목록에서 웹훅을 설정할 장치를 선택하세요.



5. 화면 상단의 **웹훅** 탭을 클릭하세요.



> **알아두기**
> **웹훅** 탭이 표시되지 않으면, 장치의 **CLUe 펌웨어 버전**을 확인한 후 지원하는 펌웨어 버전 이상으로 업데이트하세요.

1 메서드

웹훅은 **POST** 메서드를 기본 사용합니다.

2 엔드포인트(URL) 설정

- **온라인 이벤트**: 장치가 온라인 상태일 때 지정한 이벤트가 발생하면 실시간 웹훅 호출을 전송하는 엔드포인트입니다.
- **오프라인 이벤트**: 장치가 오프라인 상태였다가 다시 온라인 상태로 전환되면, 그동안 발생한 이벤트를 목록 형태로 전송하는 엔드포인트입니다.

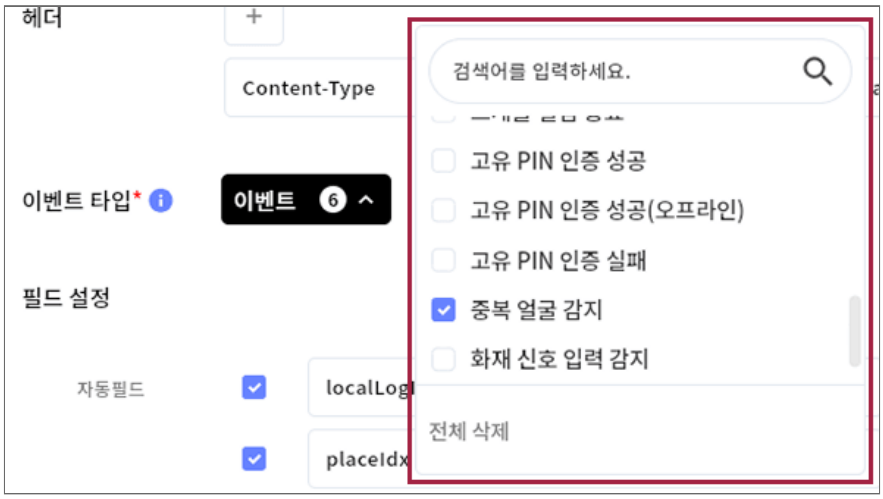
3 헤더 설정

웹훅 서버에 필요한 키 또는 인증 값을 요청 헤더에 설정하세요. 헤더를 추가하려면 ＋ 버튼을 클릭하세요.



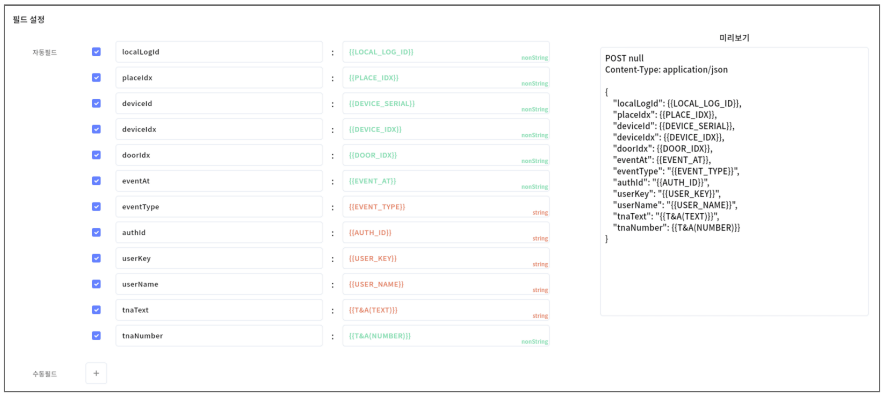
4 트리거 이벤트 지정

웹훅 호출을 트리거할 이벤트를 선택하세요. 기본으로 선택된 이벤트 외에도 **중복 얼굴 감지**와 같은 이벤트를 추가로 선택할 수 있습니다.



5 웹훅 필드 구성

장치에서 전송할 데이터를 정의하려면 **웹훅 필드**를 구성하세요.



- **자동 필드**: 장치가 전송할 수 있는 데이터 집합의 유형을 나타냅니다.
- **nonString**: Boolean, int와 같이 따옴표(`""`)로 감싸지 않는 데이터 유형을 의미합니다.

필요한 데이터 필드를 선택한 후 **미리보기** 패널에서 웹훅 페이로드를 미리 확인할 수 있습니다.

추가로 고정된 값을 포함해야 하면 **수동 필드**로 추가할 수 있습니다. 이 값은 웹훅 페이로드와 함께 고정 값으로 전송됩니다.

6 테스트 호출 실행

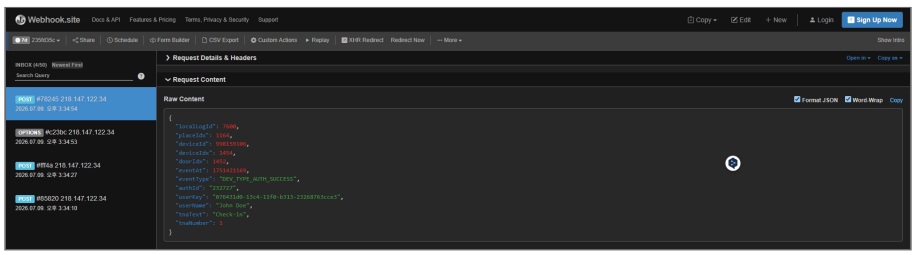
설정을 완료하면 **테스트 호출**을 실행할 수 있습니다.



> **알아두기**
>
> 테스트 호출은 실제 장치가 아닌 브라우저에서 직접 설정된 엔드포인트로 전송되는 데이터의 구조와 형식을 확인할 수 있게 해줍니다.

참고 사항

서버가 아직 준비되지 않아도 인터넷에서 공개적으로 제공되는 웹훅 테스트 서비스를 사용해 웹훅 테스트를 진행할 수 있습니다. 예를 들어, Webhook.site를 사용해 웹훅 호출을 손쉽게 확인할 수 있습니다.

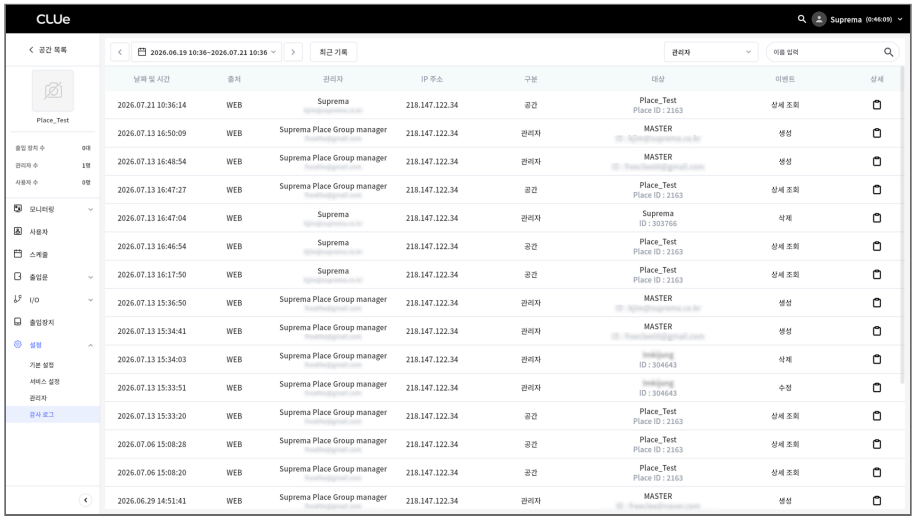


감사 로그 확인하기

감사 로그는 CLUe 포털의 공간에서 발생하는 모든 활동을 기록하고 추적하는 기능입니다. 관리자는 감사 로그를 통해 누가, 언제, 어떤 활동을 수행했는지 확인하고 보안 및 규정 준수 요구 사항을 충족할 수 있습니다.

감사 로그 조회

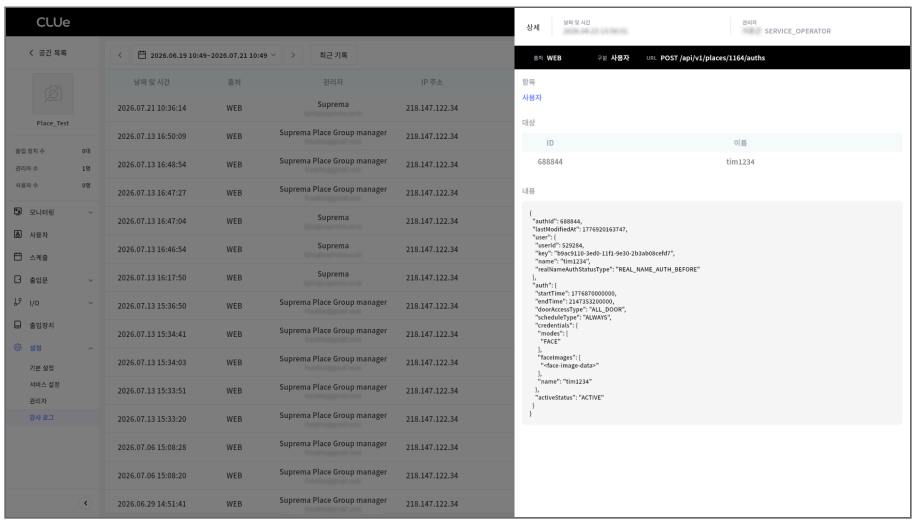
1. CLUe 웹 포털에 로그인하세요.
2. 감사 로그를 확인할 공간을 선택하세요.
3. 화면 왼쪽 사이드바에서 **설정** → **감사 로그**를 클릭하세요.



가장 최근의 감사 로그가 최신 순으로 목록에 표시됩니다. 각 로그 항목에는 활동을 수행한 **날짜 및 시간**, **출처**, **관리자**, **IP 주소**, **구분**, **대상**, **이벤트**를 확인할 수 있습니다.

상세 정보 확인

감사 로그 항목의 상세 정보를 확인하려면, 목록 가장 오른쪽의 **상세** 열에서 버튼을 클릭하세요. 화면 오른쪽에 **상세** 패널이 나타납니다.



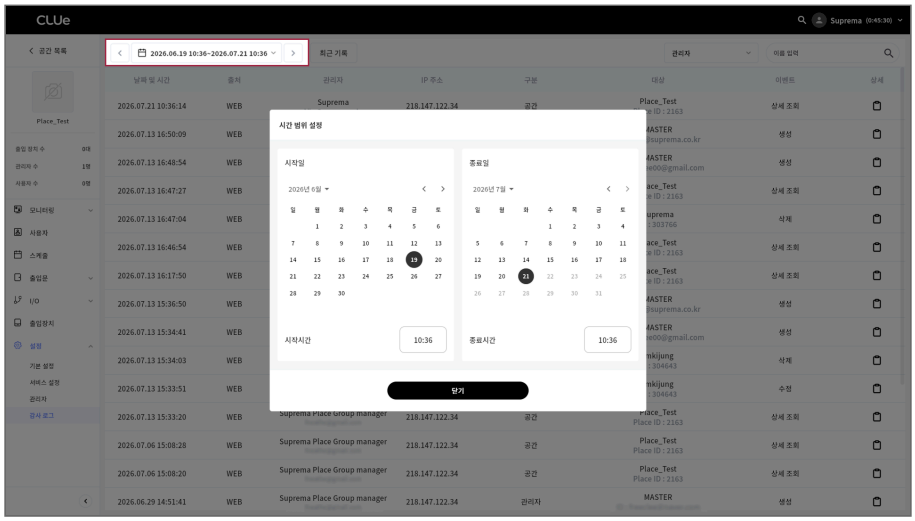
상세 패널에서는 날짜 및 시간, 관리자 계정과 함께 **출처**, **구분**, 관련 API를 확인할 수 있으며, 다음 정보도 함께 제공합니다.

- **항목**: 활동이 발생한 범주를 표시합니다.
- **대상**: 활동이 적용된 대상의 ID와 이름을 표시합니다.
- **내용**: API 요청 본문 데이터를 표시합니다. 요청 본문이 없으면 빈 값(`{}`)으로 표시됩니다.

조회 기간 설정

현재 설정된 조회 기간 단위로 조회 기간을 변경하려면 감사 로그 목록 왼쪽 상단의 < 또는 > 를 클릭하세요.

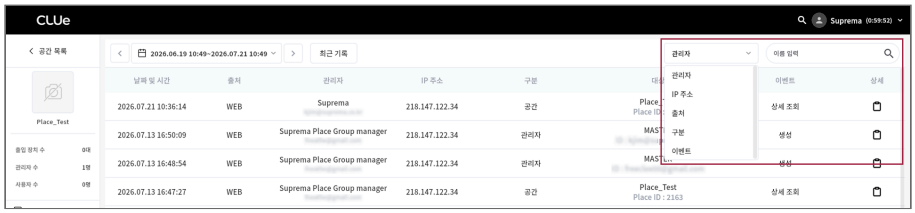
특정 기간 동안의 감사 로그를 조회하려면 날짜와 시간 영역(📅)을 클릭하세요. **시간 범위 설정** 창이 나타나면 시작 날짜와 시간, 종료 날짜와 시간을 설정하세요. 설정한 기간 동안의 감사로그를 조회할 수 있습니다.



> **알아두기**
> 설정한 조회 기간을 초기화하려면 **최근 기록** 버튼을 클릭하세요.

검색

감사 로그 목록의 각 컬럼 값을 기준으로 원하는 데이터를 검색하거나 필터링할 수 있습니다. 감사 로그 목록 상단 오른쪽의 검색 도구를 사용하세요.



- **관리자**: 관리자 이름을 입력해 검색할 수 있습니다. 대소문자 구분하여 검색합니다.
- **IP 주소**: IP 주소를 기준으로 검색할 수 있습니다. 정확한 아이피 주소를 입력해야 합니다.

  > *예: 192.168.1.1*

- **출처**: 사용자가 어떤 플랫폼에서 활동했는지 조건을 선택할 수 있습니다.

  > *웹(**WEB**), 모바일(**MOBILE**), API(**API_TOKEN**)*

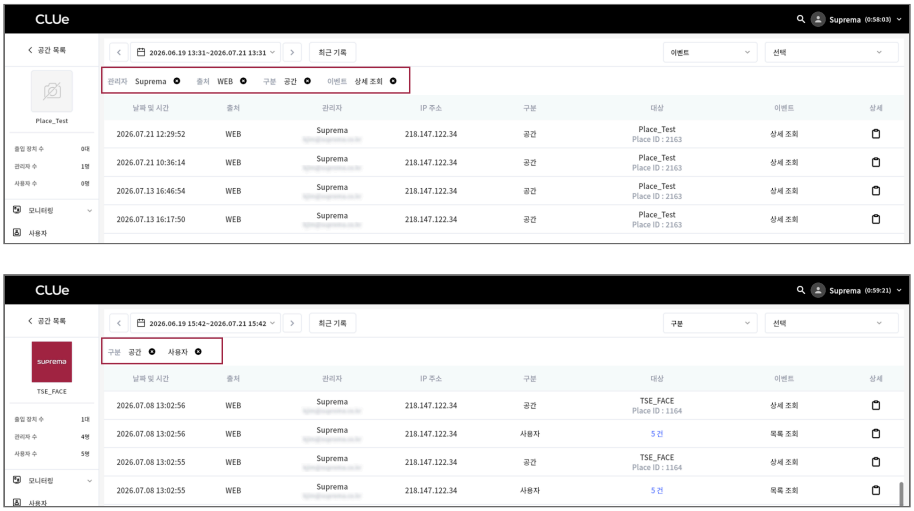
- **구분**: 사용자의 활동 범주를 선택할 수 있습니다.

  > ***장치, 출입문, 공간, 사용자, 공간 전략, 관리자, 개인정보열람***

- **이벤트**: 다음 이벤트 조건을 선택할 수 있습니다.

  > ***상세 조회, 목록 조회, 생성, 수정, 삭제, 명령***

여러 필터 항목을 함께 선택해 필터링할 수 있습니다. 서로 다른 항목을 선택하면 AND 조건으로, 같은 항목에 값을 여러 개 선택하면 OR 조건으로 필터링합니다. 필터링을 해제하려면 ✕ 버튼을 클릭하세요.



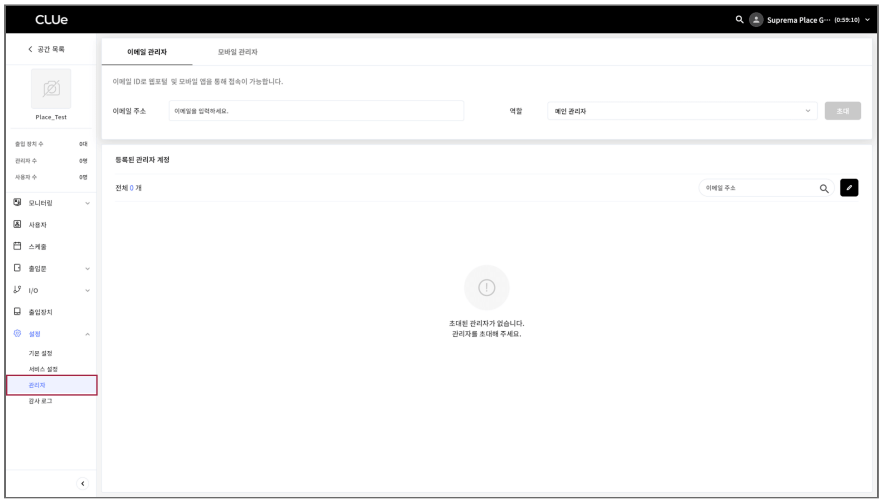
모바일 앱 사용하기

CLUe 모바일 앱을 사용하면 스마트폰으로 출입문을 원격 제어하고, 사용자를 관리하며, 공간 이벤트를 실시간으로 확인할 수 있습니다. 이 문서에서는 공간 관리자 초대 방법부터 앱 다운로드, 로그인, 주요 기능까지 안내합니다.

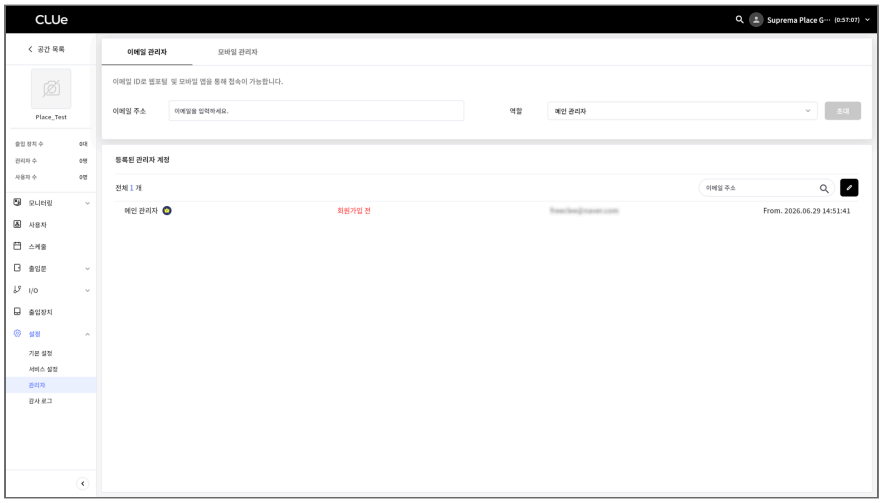
CLUe 모바일 앱 관리자 초대

공간 그룹 관리자가 공간 설정에서 이메일로 공간 관리자를 초대할 수 있습니다.

1. CLUe 웹 포털에 로그인하세요.
2. 모바일 앱 관리자를 초대할 공간을 선택하세요.
3. 화면 왼쪽 사이드바에서 **설정** → **관리자**를 클릭하세요.

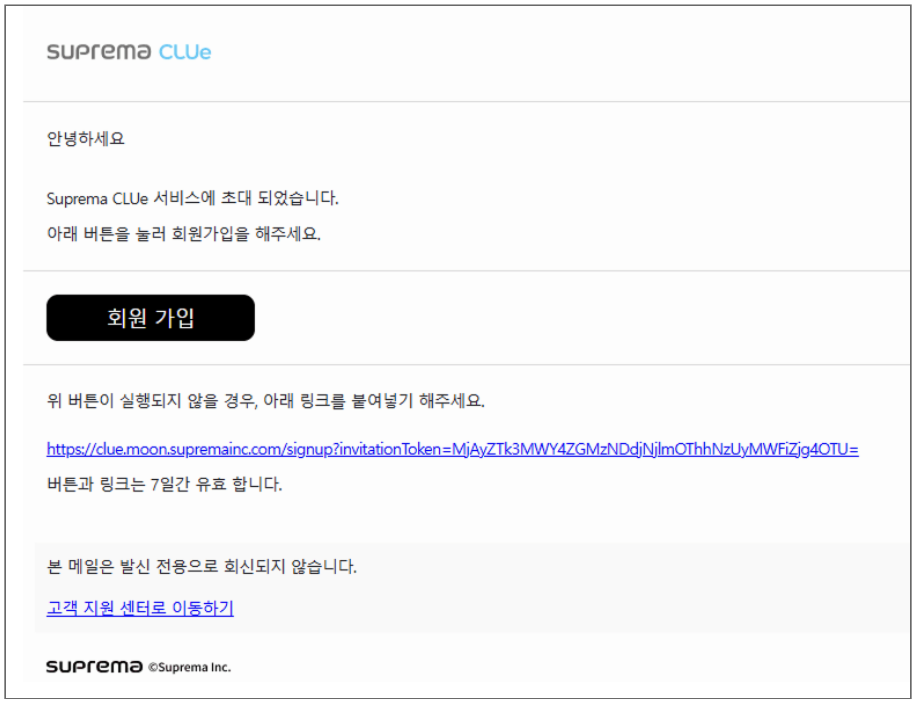


4. 이메일 주소를 입력하고 역할을 선택하세요.
5. **초대** 버튼을 클릭하세요.

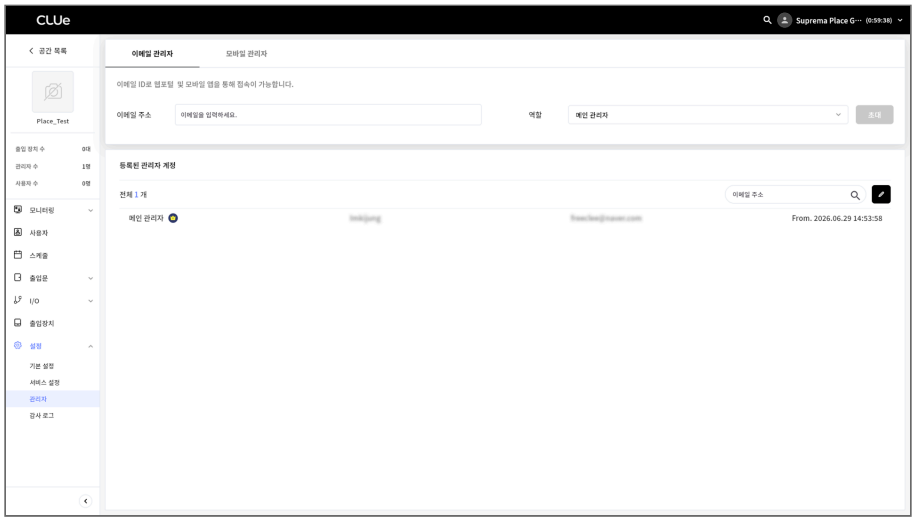


등록된 관리자 계정 목록에서 초대 상태를 확인할 수 있습니다.

초대가 완료되면 관리자에게 초대 이메일이 발송됩니다. 초대받은 관리자는 이메일에 포함된 링크를 통해 가입할 수 있습니다.



가입을 완료하면 관리자 목록에서 상태 변경을 확인할 수 있습니다.



CLUe 모바일 앱에서 직접 가입할 수 있나요?

CLUe 웹 포털에 접근할 수 없는 관리자는 CLUe 앱을 다운로드하여 모바일 앱으로 가입할 수 있습니다. 단, 실제 사용을 위해서는 반드시 공간에 초대되어 있어야 합니다.

CLUe 앱 다운로드

아래 링크 또는 QR 코드를 통해 CLUe 앱을 다운로드할 수 있습니다.

플랫폼	다운로드 링크	QR 코드
iOS	App Store	
안드로이드	Google Play	

알아두기
앱을 찾을 수 없다면 앱 스토어에서 "suprema clue"로 검색하세요.

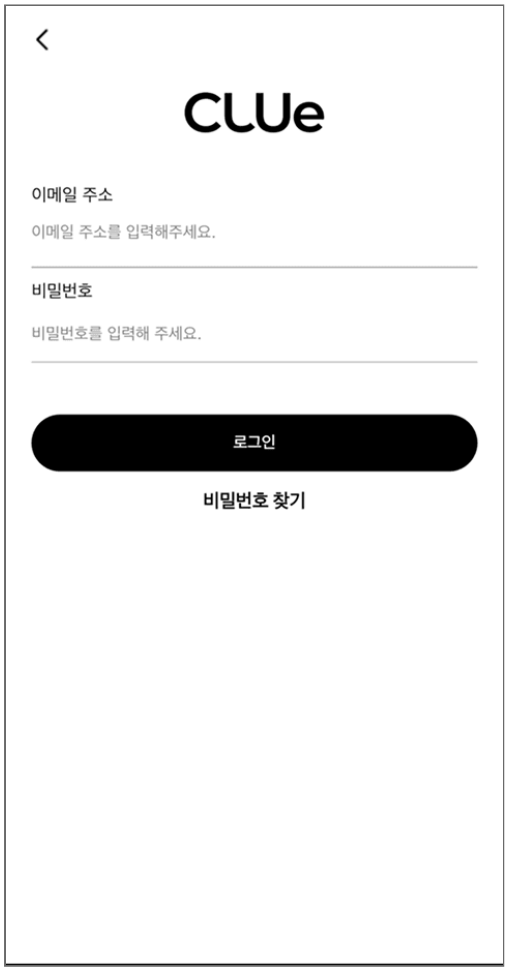
로그인

앱을 설치한 후 초대받은 이메일 주소로 로그인할 수 있습니다.

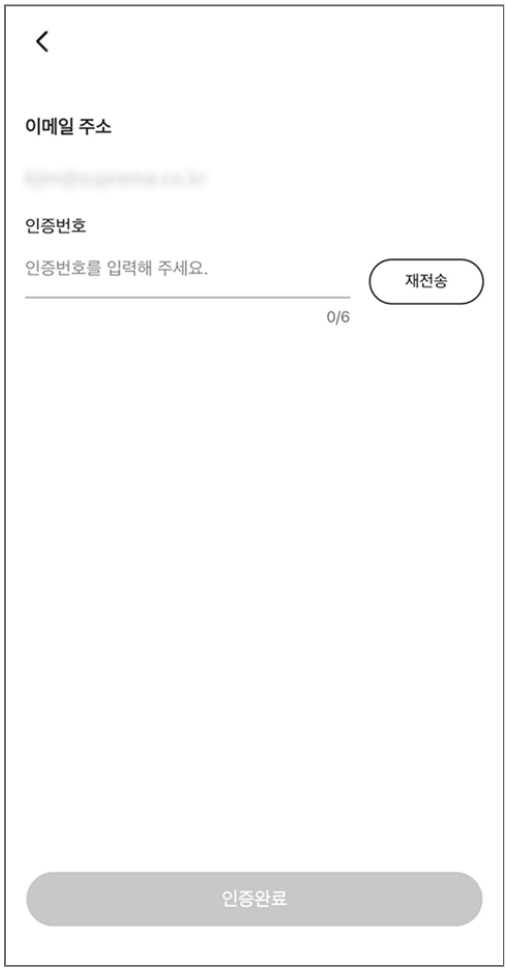
1. 모바일 기기에서 CLUe 앱을 실행하세요.
2. **이메일로 로그인**을 선택하세요.



3. 이메일 주소와 비밀번호를 입력하고 **로그인** 버튼을 탭하세요.

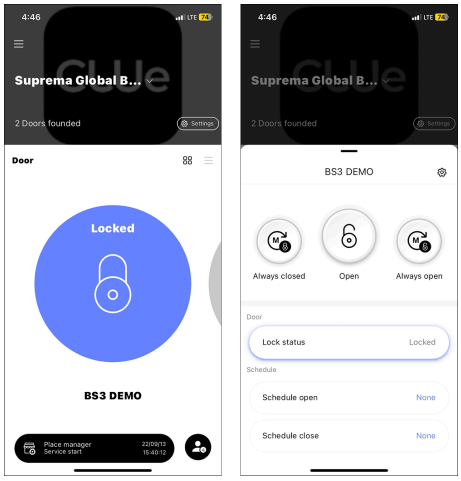


4. 이메일 주소로 발송된 인증 코드를 입력하고, **인증완료** 버튼을 탭하세요.



로그아웃할 때까지 로그인 상태가 유지됩니다.

CLUe 앱 주요 기능



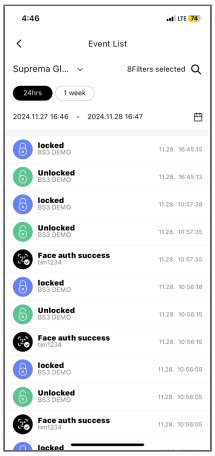
원격 출입문 제어

출입문의 현재 잠금 상태를 확인하고 원격으로 제어할 수 있습니다. 스케줄을 설정하여 지정된 시간에 자동으로 열리거나 닫히도록 구성할 수 있습니다.



사용자 관리

사용자를 초대하거나 관리할 수 있습니다. CLUe 모바일 앱과 슈프리마 장치를 사용하여 얼굴, 지문, RF 카드 등의 크리덴셜을 등록할 수 있습니다.



이벤트 모니터링

출입문의 잠금 및 잠금 해제, 인증 성공 및 실패 등 공간에서 발생한 이벤트를 실시간으로 확인할 수 있습니다. 24시간 또는 1주일 단위로 조회하거나 필터를 적용하여 원하는 이벤트를 빠르게 찾을 수 있습니다.

CLUe API 가이드

이 문서를 통해 슈프리마 CLUe API를 빠르고 간편하게 연동할 수 있습니다. API 키 발급 방법부터 요청/응답 형식, 오류 코드, 호출 제한까지 CLUe API 사용에 필요한 기본 정보를 안내합니다. CLUe API는 슈프리마 CLUe 웹 포털 설정과 함께 동작하므로, CLUe 웹 포털 계정이 없다면 먼저 계정을 요청하세요.

CLUe API 사용에 대한 자세한 내용을 확인하세요.

API 키란

CLUe API를 호출하려면 API 키가 필요합니다. 공간 그룹의 관리자 메뉴에서 발급받을 수 있습니다. CLUe API는 요청 헤더에 Bearer 토큰으로 API 키를 필수로 포함해야 합니다. API 키는 CLUe 웹 포털에서 발급하고 관리할 수 있습니다.

회원 가입을 하려면 상위 관리자 또는 같은 공간 그룹의 관리자로부터 초대를 받아야 합니다.

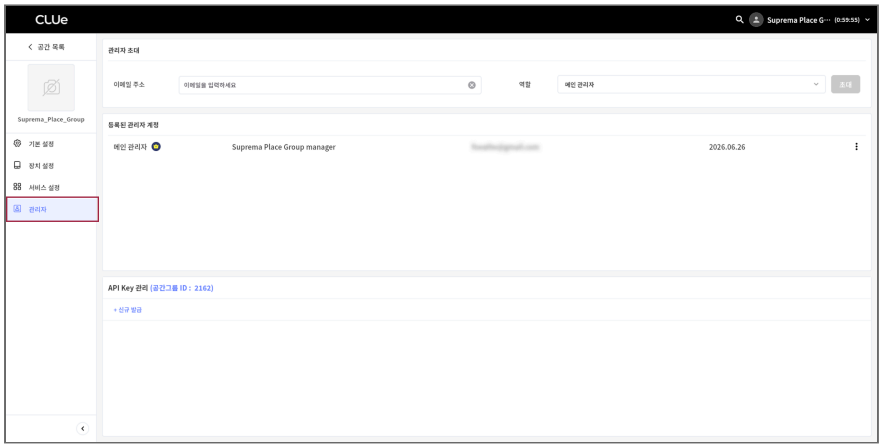
> **공간(Place)과 공간 그룹(Place Group)이란?**
>
> CLUe는 멀티 테넌트 시스템을 지원하므로, **공간**은 회사나 지점(branch)처럼 독립된 단위를 의미하며, **공간 그룹**은 여러 공간을 묶어 관리하는 상위 개념입니다.

API 키 발급

1. CLUe 웹 포털에 로그인하세요.
2. API 연동을 위한 공간 그룹을 선택하세요.
3. 화면 오른쪽 상단의 ⋮ → **상세 설정**을 클릭하세요.



4. 화면 왼쪽 사이드바에서 **관리자**를 클릭하세요.



5. **API Key 관리** 섹션에서 **+ 신규 발급**을 클릭하세요.
6. 원하는 유효 기간을 선택하세요.



> **직접 입력**을 선택하면 유효 기간을 최대 365,000일까지 설정할 수 있습니다.

7. 새 API 키를 발급하려면 **생성** 버튼을 클릭하세요.
8. 새 API 키가 생성되면 **복사** 버튼을 클릭해 CLUe API 호출 시 Bearer 토큰으로 사용하세요.



> **주의**
> API 키는 CLUe API에 대한 접근 권한을 그대로 부여하므로 외부에 노출되지 않도록 안전하게 보관하세요. 오남용으로 발생하는 문제에 대해 슈프리마는 책임지지 않습니다.

CLUe API 기본

Base URL

모든 API 요청을 보내는 기본 URL은 `https://api.moon.supremainc.com/v1` 입니다. 모든 API 요청은 HTTPS를 통해 전송해야 합니다.

CLUe API는 가능한 한 RESTful 원칙을 따르며, 페이지 및 데이터베이스 리소스에 대한 대부분의 작업을 `GET`, `POST`, `PATCH`, `DELETE` 요청으로 수행합니다. 요청 본문과 응답 본문은 모두 JSON 형식으로 인코딩됩니다.

API 성공 응답

응답에 성공하면 다음 상태가 반환됩니다.

HTTP 상태 코드: `200`

필드	설명	선택 여부
code	API 응답 코드	
status	API 응답 상태	
message	API 응답 메시지	true
data	API 응답 데이터	true

API 실패 응답

응답에 실패하면 다음 상태 중 하나가 반환됩니다.

HTTP 상태 코드: 400 / 500

필드	설명	선택 여부
errors	API 실패 응답	
errors.code	실패 오류 코드	
errors.message	실패 참조 메시지	
errors.details	실패 상세 정보	true

일반 오류 코드

코드	설명
e1000	내부 서버 오류
e1001	권한 거부
e1002	지원하지 않음
e1003	잘못된 형식
e1004	JSON 파싱 오류
e1005	잘못된 메서드 인자
e1006	잘못된 요청
e1007	존재하지 않는 리소스

코드	설명
e1008	메서드 인자 타입 불일치
e1009	요청 헤더 누락

API 호출 제한

주의

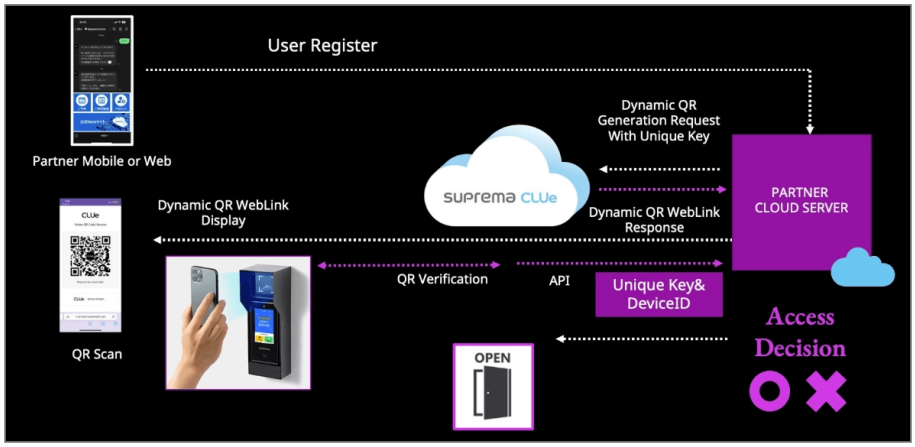
CLUe는 API별로 5분당 300회의 호출 제한을 두고 있으며, 이 제한은 호출 소스 단위로 적용됩니다. 다만 얼굴 이미지를 추가하는 API는 템플릿 추출 및 생성과 같이 처리 시간이 필요한 작업이 포함되므로, 호출 사이에 약간의 대기 시간을 두는 것을 권장합니다.

Dynamic QR 코드 연동하기

CLUe Dynamic QR 코드는 생성부터 검증까지 전 과정을 지원하는 통합 QR 솔루션입니다. 이 문서는 CLUe Dynamic QR 코드를 자체 시스템에 연동하려는 개발자를 대상으로, API 키 발급부터 서비스 설정까지의 절차를 안내합니다.

CLUe Dynamic QR 코드란

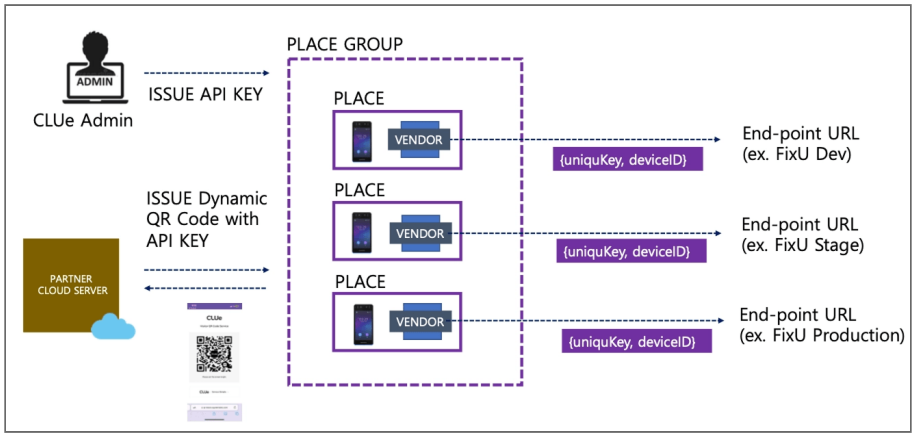
CLUe Dynamic QR 코드는 생성부터 검증까지 전 과정을 지원하는 통합 솔루션으로, 고객사가 QR 코드 기능을 처음부터 직접 개발하지 않고도 자체 시스템에 손쉽게 연동할 수 있도록 설계되었습니다.



> **알아두기**
> CLUe Dynamic QR 코드는 **고객사 확인(Vendor)** 서비스 방식과 함께 사용할 수 있습니다. **고객사 확인** 설정에 대한 자세한 내용은 서비스 설정하기를 참고하세요.

시작하기 전에

CLUe Dynamic QR 코드는 연동을 목적으로 하므로, 공간 그룹(Place Group) API 키가 필요하며 테스트를 위한 벤더 코드도 적용해야 합니다.



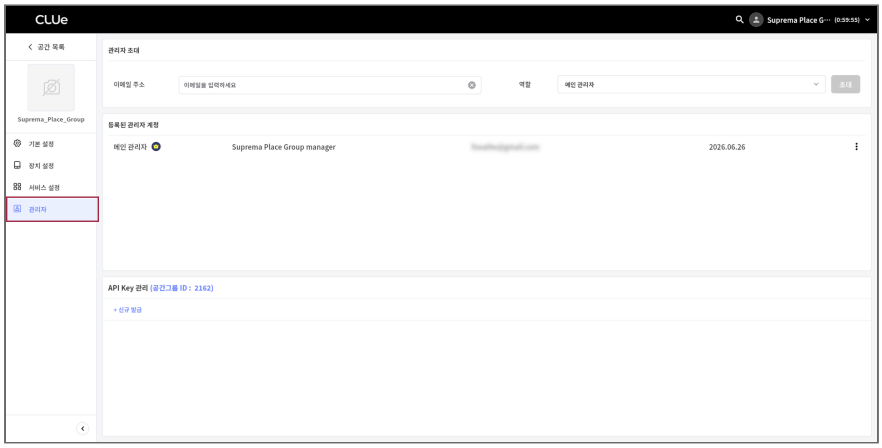
API 키 발급

1. CLUe 웹 포털에 로그인하세요.

2. API 연동을 위한 공간 그룹을 선택하세요.
3. 화면 오른쪽 상단의 ⋮ → **상세 설정**을 클릭하세요.



4. 화면 왼쪽 사이드바에서 **관리자**를 클릭하세요.



5. **API Key 관리** 섹션에서 **+ 신규 발급**을 클릭하세요.
6. 원하는 유효 기간을 선택하세요.



> **직접 입력**을 선택하면 유효 기간을 최대 365,000일까지 설정할 수 있습니다.

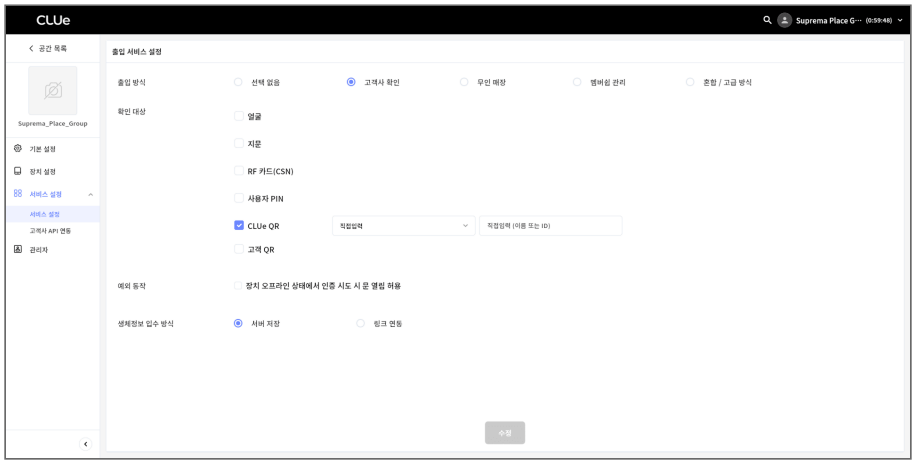
7. 새 API 키를 발급하려면 **생성** 버튼을 클릭하세요.
8. 새 API 키가 생성되면 **복사** 버튼을 클릭해 CLUe API 호출 시 Bearer 토큰으로 사용하세요.



> **주의**
> API 키는 CLUe API에 대한 접근 권한을 그대로 부여하므로 외부에 노출되지 않도록 안전하게 보관하세요. 오남용으로 발생하는 문제에 대해 슈프리마는 책임지지 않습니다.

서비스 설정

공간 그룹의 **서비스 설정**에서 **출입 방식**을 **고객사 확인**으로 설정하고, **CLUe QR**을 선택하세요.



고객사 확인 코드는 QR 연동 절차에 따라 슈프리마 CLUe 팀으로부터 발급받아 설정해야 합니다.

> **고객사 확인 코드 없이 테스트할 수 있나요?**
>
> 가능합니다. 다만 이때는 시스템에 **테스트용 고객사 확인 코드**를 설정해야 합니다. 슈프리마 담당자에게 문의해 지원을 요청하세요. 테스트용 고객사 확인 코드는 접근 권한이나 유효 기간을 검증하지 않고 접근을 허용합니다.

다음 단계

Dynamic CLUe QR API 사용에 대한 자세한 내용을 확인하세요.

(주) 슈프리마
13554 경기도 성남시 분당구 정자일로 248 파크뷰타워 17층
영업 문의 1522 4507(1번)　korea@suprema.co.kr | 고객지원 1522 4507(2번)　cs@suprema.co.kr

© 2026 Suprema Inc. 이 문서에 표기된 슈프리마, 제품명, 번호는 슈프리마의 등록 상표입니다. 모든 회사명과 제품명은 해당 회사의 상표이거나 등록 상표입니다. 제품 외관, 제조 상태 및 사양은 사전 통지 없이 변경될 수 있습니다.