CLUe

ADMINISTRATOR GUIDE

Version R_2026-09-28

English
EN 102.00

suprema
SECURITY & BIOMETRICS

CONTENTS

Getting Started with the CLUe Web Portal 5

Understand administrator levels 5

Add subitems 6

Invite Administrators 7

Service Settings 9

Integrate with a Customer API 12

Before you start 12

Customer API integration 12

Main workflow 14

Setting workflow 15

Summary of input rules 26

Troubleshooting 27

Change the Firmware 31

Switch to CLUe support mode 31

Troubleshooting 27

Add Device 34

Device enrollment (Branch manager) 34

Device assignment 35

Test place setting (Branch manager) 37

Self-Register Device 39

Supported devices and firmware versions 39

Admin preparation step 39

Onsite registration step 41

Notes 44

Add Doors 46

Access control setting 46

Use slave device relays 47

Upgrade Firmware 49

Go to a place 49

Firmware upgrade 50

Set Up Device Webhook 52

Supported devices 52

Key advantages 52

Webhook settings 52

Notes 44

View Audit Logs 57

View audit logs 57

View details 57

Set search period 58

Search 58

Using the Mobile App 60

Inviting CLUe mobile app admins 60

Download the CLUe app 61

Log in 62

Main features of the CLUe app 65

CLUe API Guide 67

What is an API key 67

Generate an API key 67

CLUe API basics 68

API rate limits 70

Integrate Dynamic QR Code 71

What is CLUe Dynamic QR Code 71

Before you start 12

Generate an API key 67

Service Settings 9

Next step 0

Next step 0

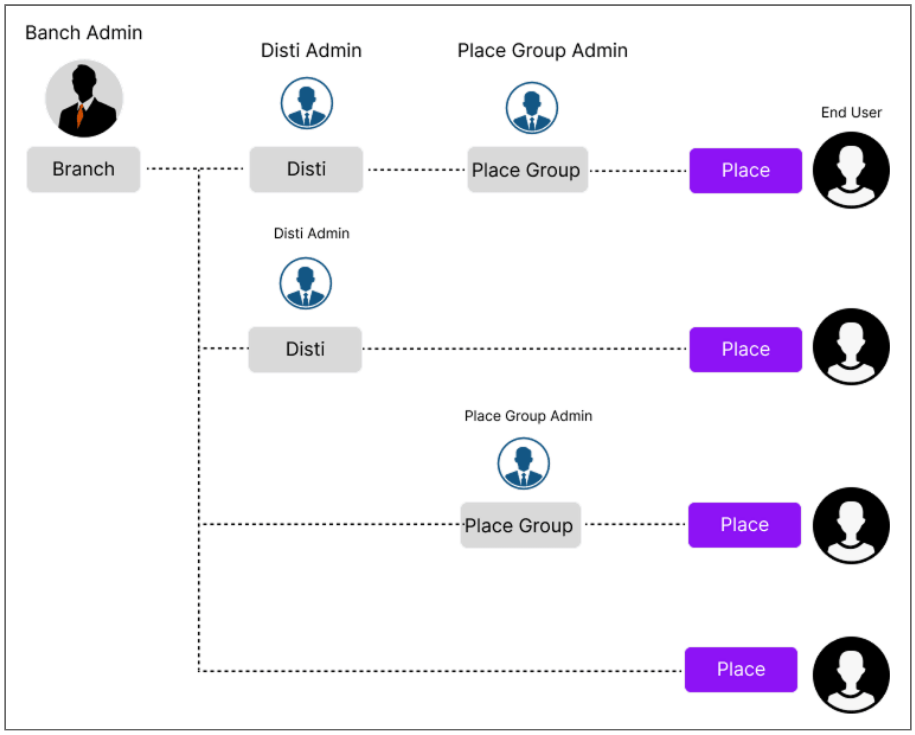
Next step 0

Getting Started with the CLUe Web Portal

If you are new to the CLUe web portal, start by understanding the administrator permission structure. This document explains how to add distributors, place groups, and places under a branch.

Understand administrator levels

CLUe is a multi-tenant system with a three-level hierarchy designed for distribution channel environments that operate customer services across multiple branches.



- **Branch Admin**: A Branch Admin can create **Distributor/Place group/Place** subitems.
- **Distributor Admin**: A Distributor Admin can create **Place group/Place** subitems.
- **Place Group Admin**: A Place Group Admin can create **Place** subitems.

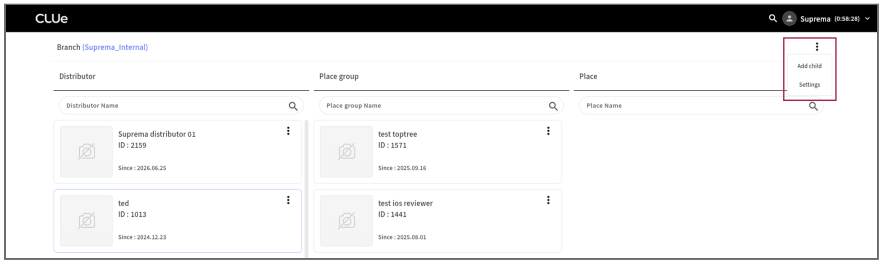
Invite customers by email. Invited customers can sign up through the link in the email and access the invited place group.

One branch can have multiple distributors, and one distributor can also have multiple place groups. At the Distributor Admin level, you can view only your own distributor and its subitems.

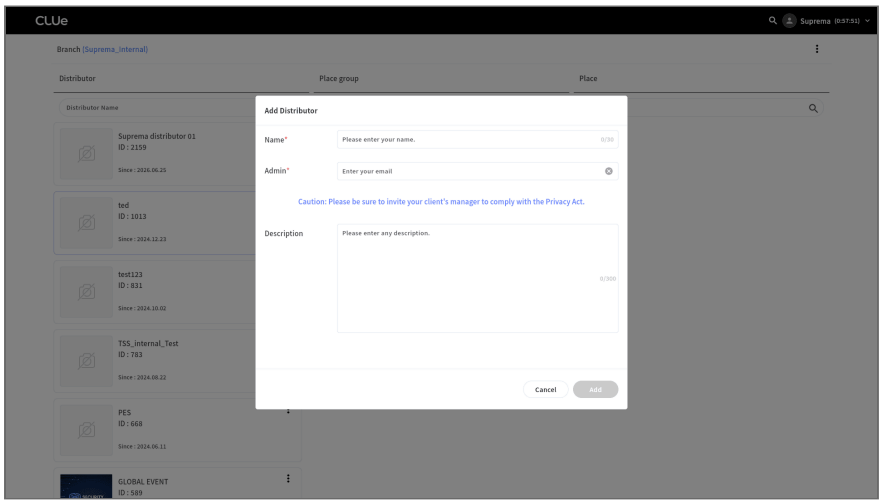
> **Which item does the customer or end user belong to?**
>
> In the hierarchy above, the **Place group** is the item assigned to the customer or service provider. A place group represents a customer unit that operates multiple places, so enter that customer's admin email when creating a place.

Add subitems

1. Log in to the CLUe web portal.
2. After logging in, you can view the list of invited branches. Select the branch you want.
3. When the list of subitems under the selected branch, such as distributors, place groups, and places, appears, click the ⋮ button in the top-right corner of the screen.
4. Click **Add child** from the popup menu.

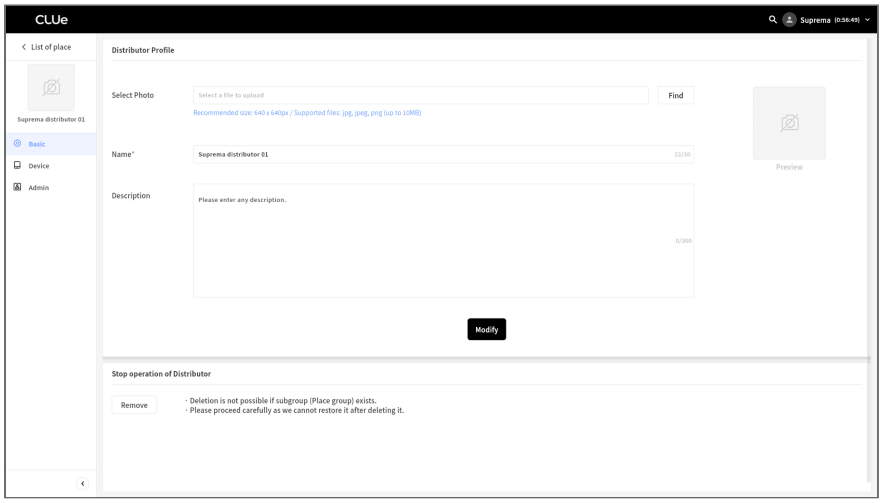


5. When the **Add Distributor** popup appears, enter each field.



> **Why enter the admin email?**
>
> By default, the super admin can access only menus unrelated to the customer's personal data, such as device or door settings. Access to customer personal data requires the customer's consent, so invite the customer admin first.
>
> If access to personal data is needed later, the customer can invite the super admin again. The invited super admin can access menus that include personal data, such as users, admins, and monitoring.

6. After you finish all entries, click the **Add** button at the bottom.
7. When the item is added, the system automatically moves to the **Basic** page, where you can change the name or photo.

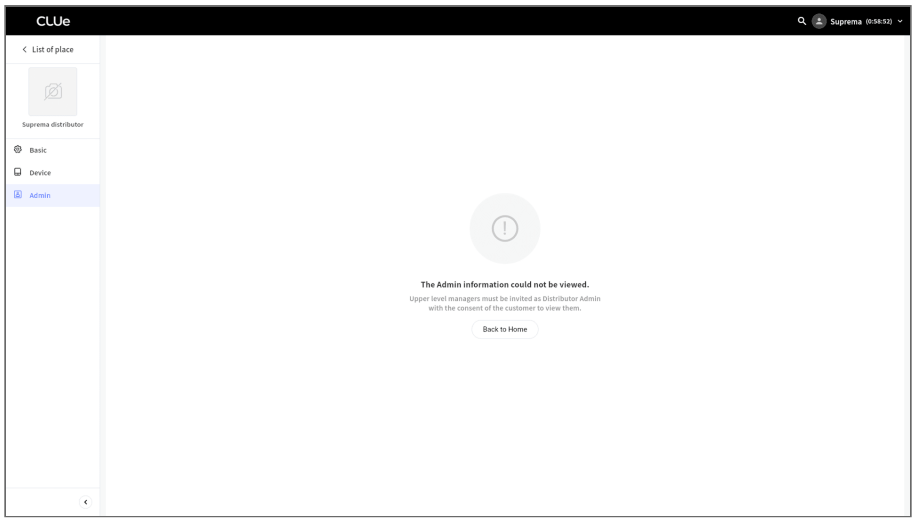


Info

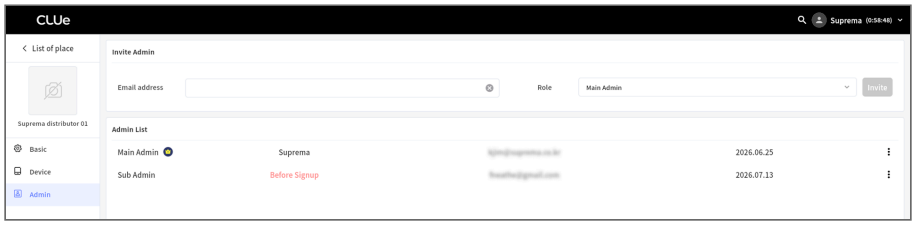
Likewise, click ⋮ → **Add child** in the distributor, place group, or place list to add a subitem.

Invite Administrators

The **Admin** menu appears, but you cannot view admin information without the customer's consent. View access is available only after the customer company, a distributor or place group admin, invites a higher-level admin.



In the **Admin** menu, enter an email address to easily invite an admin at the same level. After the invited user completes sign-up, they gain administrator permissions at the same level.



Info

Main Admin / **Sub Admin**: There is no functional difference. This ensures that at least one main admin remains. However, a sub admin cannot delete the main admin.

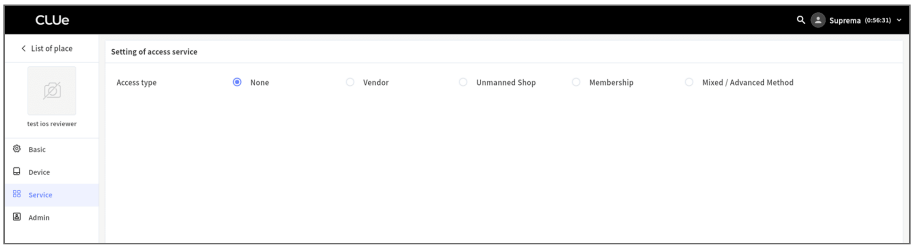
Service Settings

Set the access service method for each place group. The service type and credential set for a place group apply automatically to all child places, so you do not need to set them separately for each place.

CLUe supports two access service methods.

- **Vendor**: A method that requests access approval from a client through an external API.
- **Membership**: A method in which CLUe controls access independently without external integration.

Click **Service** in the left sidebar of Place group settings.



Vendor setting

The **Vendor** method calls an external client API before the door opens to decide whether to allow access. It supports QR codes and Facial Authentication.

QR case

When you scan a QR code, the CLUe server calls the client API and gets the access decision directly. Select one of the following two methods based on the QR code type you use.

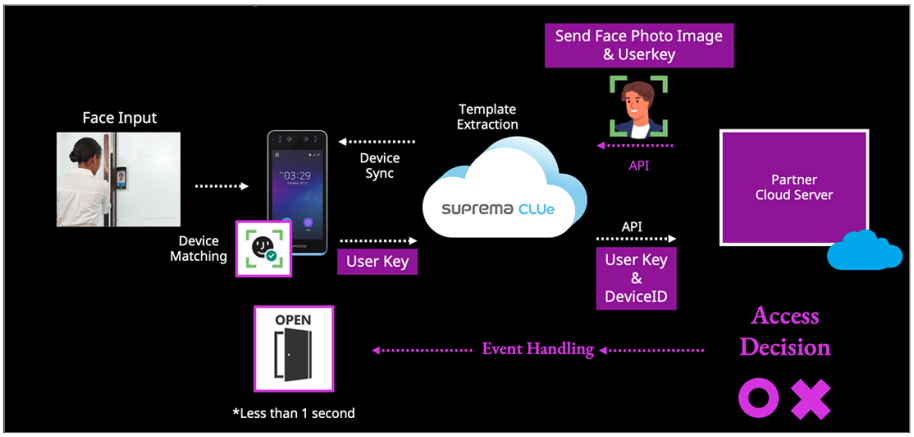
- **CLUe QR**: A dynamic QR code issued directly by CLUe.
- **Customer QR**: Select this when the customer generates and operates QR codes independently.



The image above is an example screen and may differ from the actual screen.

Facial authentication case

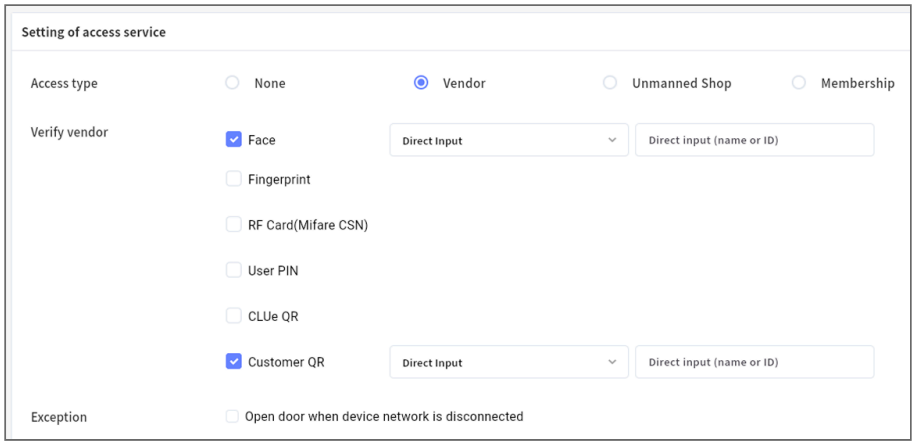
If you use Facial Authentication, register only the image. The CLUe server extracts the template and syncs it with the device. If face matching succeeds, CLUe decides whether to allow access through the client API, just like the QR method. See CLUe API documentation for how to enroll a face user.



The image above is an example screen and may differ from the actual screen.

Customer verification code setting

To use the **Vendor** method, enter the customer verification code together with where and how the CLUe server calls the customer or partner API.

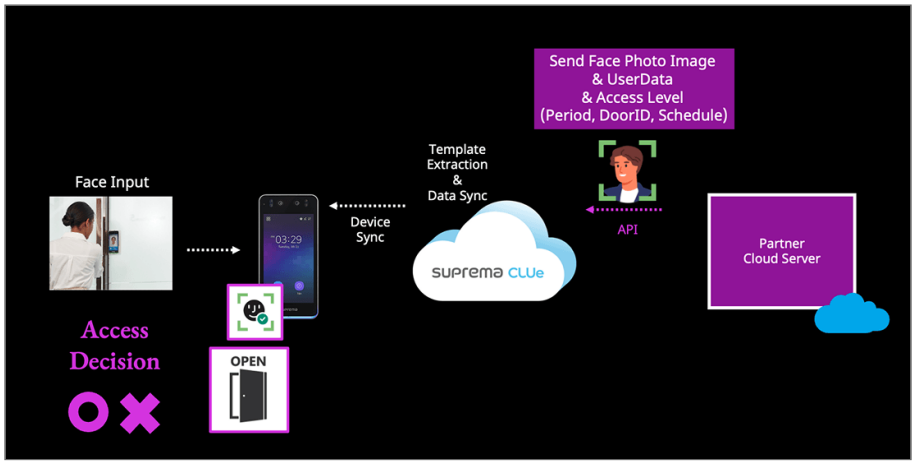


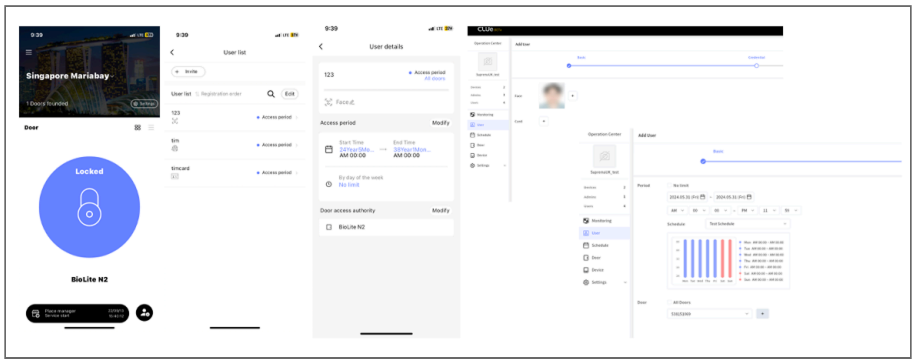
The Vendor code is a code format that the Suprema CLUe team pretests and develops to decide which client's API to call. After you enter this code, the system automatically calls the API for each authentication method in child places without additional settings, and controls access based on the specified response values.

> **How to get a customer verification code**
>
> The CLUe team manages it separately so other clients' codes do not get exposed. Customer verification code generation is handled separately after API specification review. Contact the CLUe team directly for details.

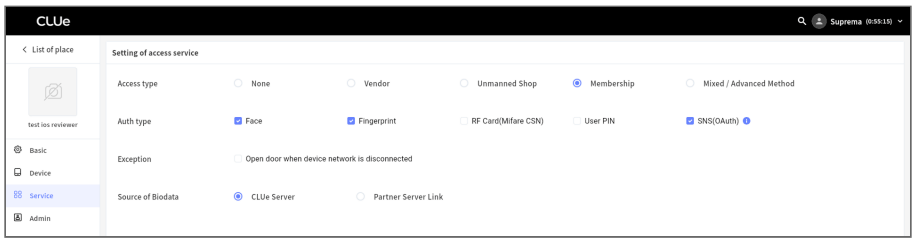
Membership setting

The **Membership** method lets the CLUe system decide access control independently, without intervention from an external client or third party. This also applies when you operate CLUe only through a web portal or mobile app.





With the **Membership** setting, you can select the credential that applies to child places.



Can I change the place setting differently from the place group?

Yes, you can configure the authentication method on the place settings page. However, you cannot change the access method from **Membership** to **Vendor**, or vice versa. So if clients in the same place group need different access methods, we recommend creating separate place groups for each use case.

Next step

See how to register a customer vendor API in a CLUe place group and connect it to a credential so the customer's access decision logic works with CLUe access control.

Integrate with a Customer API

Customer API integration is an access method where CLUe sends recognized credential data, such as a face, fingerprint, RF card, PIN, CLUe QR, or custom QR, to an external API operated by the customer. Access is then allowed or denied based on the response. This method lets you apply customer-specific policies, such as access permissions, attendance, and visitor management, directly to CLUe access control without extra development.

CLUe only identifies credentials and sends them to the customer API. The customer API response determines whether access is allowed.

Before you start

Audience

This document is for **place group administrators** and **place administrators**.

- **Place group administrator**: Register, edit, and delete customer APIs, map credential types to APIs, and apply settings to sub-places.
- **Place administrator**: Review settings inherited from the place group and apply place-specific overrides when needed.

> **Info**
> This document is for IT administrators familiar with **HTTPS**, **HTTP status codes**, **Webhooks** (HTTP POST), **JSON**, and **JSONPath**. Coordinate the customer API spec, including the URL, authentication header, and request/response JSON structure, with the customer contact in advance.

Prerequisites

- To access this menu, the target place group or place must invite you as an administrator.
- Prepare the customer's authentication Webhook URL in advance (**HTTPS required**, **HTTP POST received**) and the required authentication header values.

Key terms

Term	Description
Customer API integration	An access method that sends credential data to an external API operated by the customer for validation when a user presents a credential to the device.
Credential	Face / Fingerprint / RF card / User PIN / CLUe QR / Custom QR
Webhook URL	An HTTPS endpoint that the customer server opens to receive authentication requests from CLUe via **HTTP POST** with `Content-Type: application/json`.

Term	Description
Request Header	A Key/Value pair sent with the request for authentication and authorization. (Example: `Authorization` token)
Auto Fields	A value the system fills into the request body automatically. Select only the required fields.
Manual Fields	A fixed value that the administrator enters directly into the request body.
Judgment Criteria	A set of rules that interprets the customer response as access allowed or denied, including statusCode, success result Key/Value, and success/failure message keys. The screen shows this as the **Response Parsing** section.
Judgment Mode	An element that configures the judgment criteria. Select one of these options: HTTP response code only, response body field only, or a combination of both.

Customer API integration

Customer API integration is an access method that sends credential data recognized by the CLUe device to a customer-operated HTTPS API and decides whether to allow or deny access based on the response. This lets you directly apply customer-specific policies, such as access permissions, attendance, and visitor management, to CLUe access control.

- You can connect a different customer API for each credential type, such as face, fingerprint, RF card, PIN, CLUe QR, and custom QR.
- Before saving the registration, verify the integration with a test call.
- CLUe only identifies and sends credentials. The customer API response determines the actual allow or deny decision.

Supported credentials

- Face
- Fingerprint
- RF Card
- User PIN
- CLUe QR
- Custom QR

Roles of place groups and places

Level	roles	Responsibilities
Place group	Place group manager	Register, edit, and delete customer APIs, and connect APIs to credentials

Level	roles	Responsibilities
Place	Place administrator	Review inherited settings and apply place-specific overrides when needed

Application rules

- **Saved at the place group level**: The same settings apply immediately to all sub-places in the place group. Existing place-specific overrides are overwritten by the place group values.
- **Saved at the place level**: Applies only to that place. Does not affect other places or the parent place group.

Main workflow

Customer API integration has two main workflows. The **setting workflow** that administrators perform first, and the **access event workflow** that runs when a user actually tries to access.

Setting workflow overview

The steps that the administrator performs. Each step is described in detail starting in Chapter 4.

1. (Place group) Select the access method.
   - **Vendor** or **Mixed / Advanced Method**
   - The **Customer API Integration** entry becomes active in the left sidebar.
2. (Place group) Register the API in **Customer API Integration**.

   Basic info → Custom header → Auto field → Manual field → Run test → Configure response parsing → Save
3. (Place group) Connect the registered API to each credential.

   When you save, the same settings apply automatically to all sub-places.
4. (Optional) Set a place-specific override.

   Applies only to the selected place. By default, the place group settings remain in effect.

Access event workflow overview

This is the sequence that runs after setup when a user actually tries to access.

1. The user presents a credential to the device. (Face / Fingerprint / RF card / PIN / CLUe QR / Custom QR)
2. The device sends a verification request to the CLUe server.
3. The CLUe server sends a verification request to the customer server.

   Includes the registered Webhook URL, custom header, auto fields, and manual fields
4. The CLUe server decides access based on the customer response.

   The configured judgment criteria determine whether access is allowed or denied.
5. The system returns the result to the device.

If the response includes a message, it appears on the device screen.

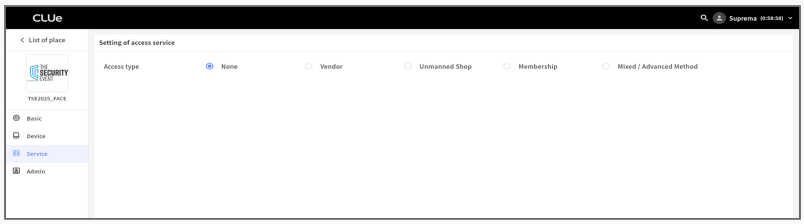
Setting workflow

Step 1 — Enable customer API integration

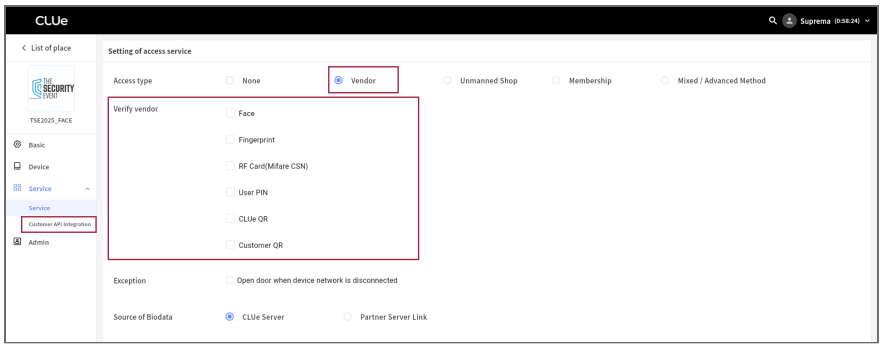
1. Log in to the CLUe web portal.
2. Select the place group.
3. Click ⋮ → **Settings** in the upper right of the screen.



4. Click **Service** in the left sidebar of the screen.

> Initially, **Access type** is set to **None**. In this state, no settings are active.
>
> 
>

5. Under **Access type**, select **Vendor**.
6. The **Verify vendor** section appears.



The **Verify vendor** section shows all six supported credentials. Then connect the customer API registered for each credential.

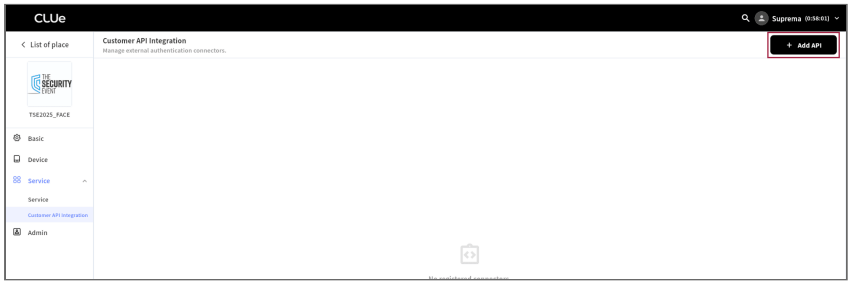
7. When **Customer API Integration** becomes active in the left sidebar, click it.

> **Info**
>
> - **Customer API Integration** becomes active when **Access type** is set to **Vendor** or **Mixed / Advanced Method**.
> - No save is required at this step. To register the API to connect, see Step 2 — Register customer API.

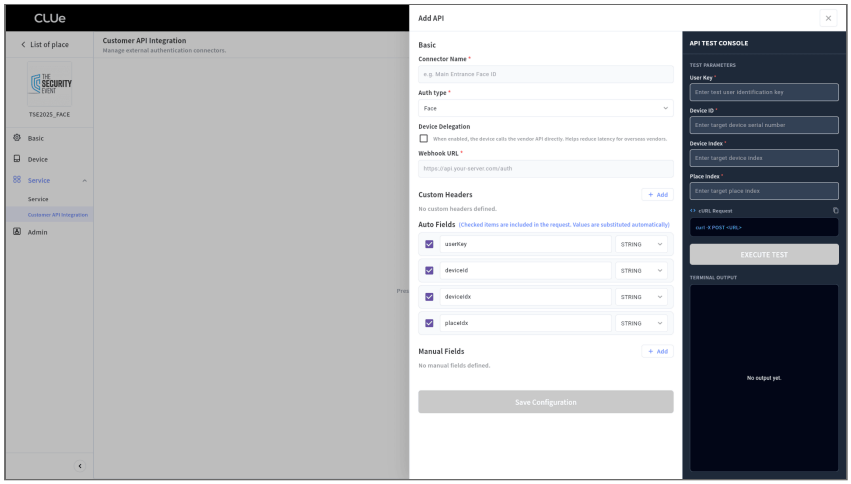
Step 2 — Register customer API

1 Add API

1. Click the **Add API** button at the top right of the screen.



2. When the **Add API** panel appears, enter the required information.



2 Enter basic information

Field	Description	Required	Input rule
Connector Name	Enter a name to identify this integration.	Yes	Up to 64 characters.
Auth type	Select the credential that will use this API.	Yes	Select one of the six types.

Field	Description	Required	Input rule
Webhook URL	Customer Webhook URL.	Yes	Must start with `https://` and can be up to 512 characters. `http://` URLs cannot be saved.

> **Info**
> **Auth type** cannot be changed after it is set once. To use it for a different credential type, register a new API.

3 Request spec

CLUe sends only **HTTP POST** requests with `Content-Type: application/json` to the registered URL. The customer API must accept requests in this format. Endpoints that allow only other methods, such as `GET` or `PUT`, are not supported.

4 Response spec

The customer API must include `Content-Type: application/json` in the response header and return the response body in JSON format. CLUe cannot parse non-JSON responses, such as HTML error pages, plain text, or XML. Test and live access verification both fail.

Example response body

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

In the example above, set the judgment criteria `Key` to `$.valid` and `Value` to `true` (`BOOLEAN`) to define the success condition, and set **Success Message JSONPath** to `$.message` to show the success message. Match the actual key names and structure to the customer API spec.

> **Registration limit**
>
> You can register up to **3** APIs per credential type. In other words, you can register up to 18 APIs per place group across the six types: face, fingerprint, RF card, PIN, CLUe QR, and custom QR. You cannot register more for a credential type that already has 3 APIs. Select the API that each credential actually uses in Step 3 — Assign APIs to each credential.

5 Add custom headers

Add custom headers if the customer API requires **Authentication** or **Authorization** headers.

> *Example:* `Authorization` *token, API key*



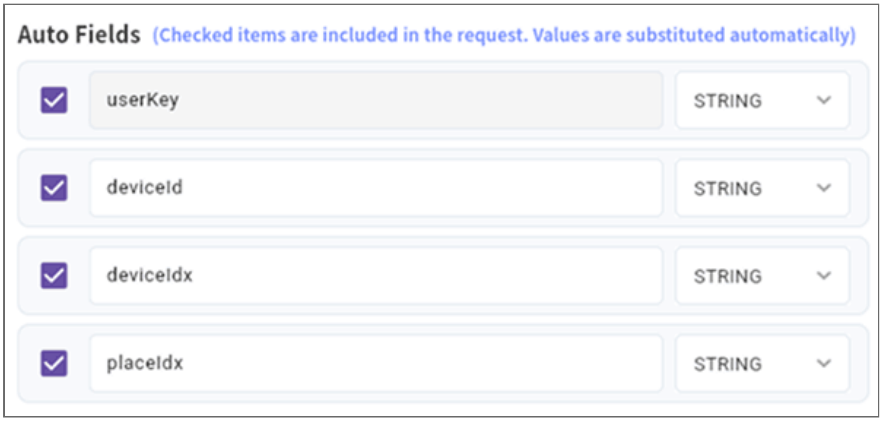
Field	Description
Header Name	Enter the header name, such as `Authorization`. Duplicate names are not allowed.
Header Value	Enter the header value.

- You can add up to **10** custom headers.
- Leave this section blank if the customer API is a public endpoint or does not require separate headers.
- To insert a row, click the **Add** button. To delete one, click the ✕ button.

> **Fixed headers cannot be configured**
>
> `Content-Type` and `Accept` cannot be added as custom headers. CLUe sends `Content-Type: application/json` and `Accept: application/json` as fixed values internally, so the administrator does not need to set them separately. If you try to add a header with this name, the system does not save it. The customer API should be designed with these two headers in mind.

6 Select auto fields

Auto Fields are values that the system **fills into the request body automatically**. Available auto fields vary by credential type. The location of each field value appears as a `{{...}}` **placeholder**, and the system replaces it with actual device or user values at request time.



The image above is an example screen and may differ from the actual screen.

Default key	Placeholder (value location)	Available for	Actual value
deviceId	{{DEVICE_SERIAL}}	All credential types	The serial number of the requested device
userKey	{{USER_KEY}}	Face / Fingerprint / CLUe QR	The user identifier managed by CLUe
rfCard	{{CARD_NUMBER}}	RF Card	Presented card number
uniquePin	{{UNIQUE_PIN}}	User PIN	Entered PIN value
qrCode	{{QR_CODE}}	Custom QR	QR payload

Field selection rules

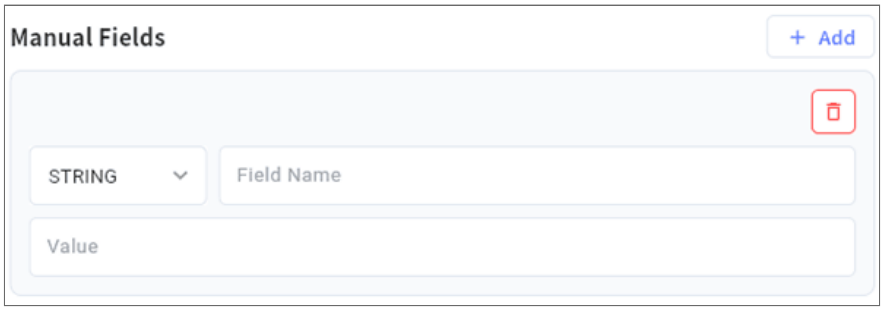
- Use the checkbox on the left of each field to **decide whether to include it in the request**.
- You do not need to select all of them. Select only the values the customer API actually needs for judgment. Reducing unnecessary data makes troubleshooting easier.
- You can edit the key field name. Change it to match the name required by the customer API, such as `userKey → employeeId`. The system fixes the placeholder location value, so you cannot change it.
- The data type for each field, such as `STRING`, appears to the right of the field.

Info

- You cannot add placeholders beyond these five. If the customer API requires additional values, see Add manual field to add fixed values, or coordinate with the customer so they derive them from the device serial number or user key.
- You can include up to **10** fields in the request body, combining auto fields and manual fields. The more auto fields you select, the fewer manual fields you can use.

7 Add manual field

Add manual fields when the customer API requires fixed values in the request.



Field	Description
Field Name	Field names must be unique and must differ from auto field names.
Field type	Select `STRING`, `NUMBER`, or `BOOLEAN`.
Value	Enter the value for this field. The system converts it to the appropriate JSON data type based on the selected type. Example: `NUMBER: 123`, `STRING: "123"`, `BOOLEAN: true/false`

- You can include up to **10** fields total, combining auto fields and manual fields.
- If no manual fields are added, the **No manual fields defined.** message appears.
- To insert a row, click the **Add** button. To delete one, click the button.

8 Run API test

After you finish basic info, custom headers, auto fields, and manual fields, run a test before configuring the judgment criteria. The actual response from the test is required to configure the judgment criteria (Configure response parsing).

Use **API TEST CONSOLE** on the right side of the **Add API** panel.

9 Test parameters

The input fields shown in the test console vary by credential type. **Device ID** (device serial number) is required for all types. Enter the remaining values in the same format the customer manages for that credential type.

Authentication method	Value to enter	Matching placeholder
All types	**Device ID** — 9 to 12 digits, device serial number	`{{DEVICE_SERIAL}}`
Face / Fingerprint / CLUe QR	**User Key** — 1 to 64 characters, the user identifier managed by CLUe	`{{USER_KEY}}`
RF Card	The **card number** managed by the customer	`{{CARD_NUMBER}}`
User PIN	The **user PIN** managed by the customer	`{{UNIQUE_PIN}}`
Custom QR	The **QR payload** managed by the customer	`{{QR_CODE}}`

Values entered in the test console replace the auto-field placeholders and are sent as the actual request body. For testing, enter values that actually exist in the customer database to verify both allow and deny responses. In a live environment, the values recognized by the device are filled in automatically.

10 Run test

1. Click the **EXECUTE TEST** button at the bottom of the console.
2. A progress indicator appears while the test runs.
3. When results arrive, the request and response details appear in the **TERMINAL OUTPUT** console area.

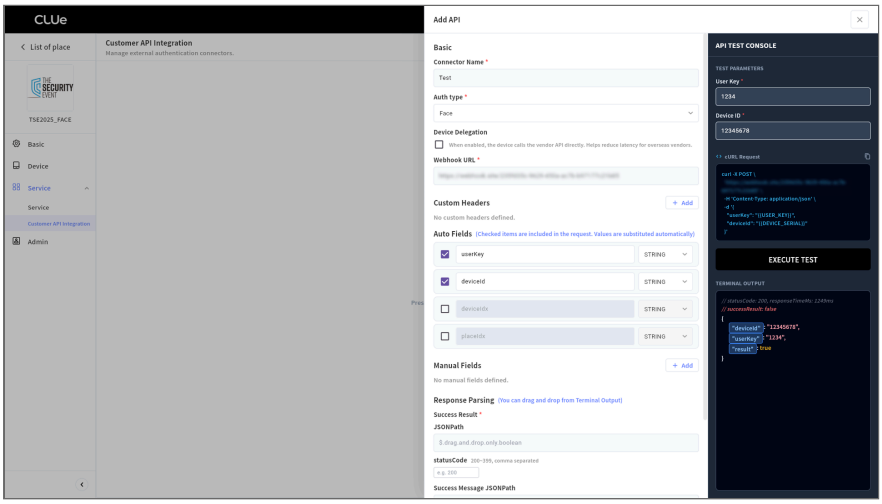
If you close the panel or move to the previous step while it runs, the test stops.

When the response arrives successfully, move to the next step and configure the judgment criteria based on the response. If URL, header, or field settings prevent a response, review the values and test again.

> **Required before saving**
>
> The **Save Configuration** button activates after at least one successful test. Here, success means receiving an HTTP response of any kind from the customer server, including 4xx and 5xx responses. If a network error prevents a response, you cannot save.

11 Test failure example — when the response body is not JSON

Even if the customer server returns a response, the test console shows an error and failure log if the body is not JSON or if the response header `Content-Type` is not `application/json`. The **Save Configuration** button does not activate.



The image above is an example screen and may differ from the actual screen.

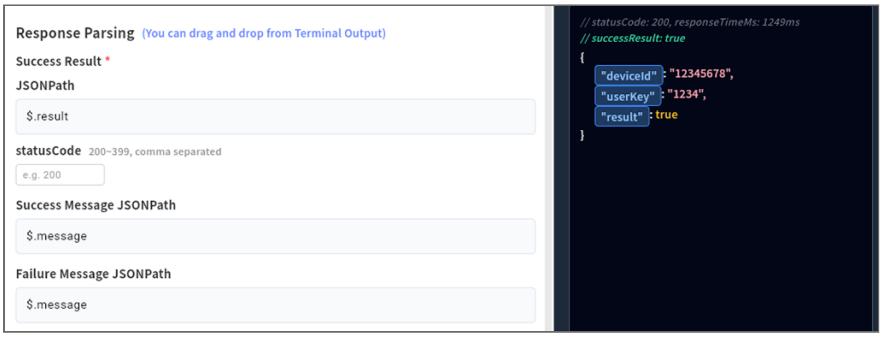
Using Response spec, check with the customer contact that the API meets both conditions below.

- The response header includes `Content-Type: application/json`
- The response body is valid JSON, not an HTML error page, plain text, or XML

12 Configure response parsing

Based on the response you receive, define which response counts as access allowed at this step. Responses that match the configured criteria are allowed. All others are denied.

The judgment mode is determined automatically based on the fields you enter. At least one of **statusCode** and **Success Result JSONPath** is required. If you leave both blank, you cannot save.



The image above is an example screen and may differ from the actual screen.

#	Mode	Input	Success criteria
1	Response code validation	**statusCode** only	Success occurs when the HTTP status code matches one of the values in the list.
2	Response body validation	**Success Result JSONPath** only	Success occurs when the body satisfies the `Key = Value` condition, regardless of the HTTP response code. If the condition matches, 4xx and 5xx responses are still allowed.
3	Combined validation	Both	Success occurs when the status code matches and the body condition also matches. If the status code does not match, the system does not evaluate the body.

statusCode (used in modes 1 and 3)

- You can specify only integers in the 100 to 399 range. You cannot set `4xx` or `5xx` codes as success.
- You can specify up to 3 values, and duplicate values are not allowed.
- If you set multiple values, success applies when any one of them matches, such as `200` or `201`.

Success Result JSONPath (used in modes 2 and 3)

- Enter the `Key`, `Value`, and data type (`BOOLEAN`, `STRING`, or `NUMBER`) that identify the success response.
- You can set only one success key condition.
- Responses that do not match this condition are denied.

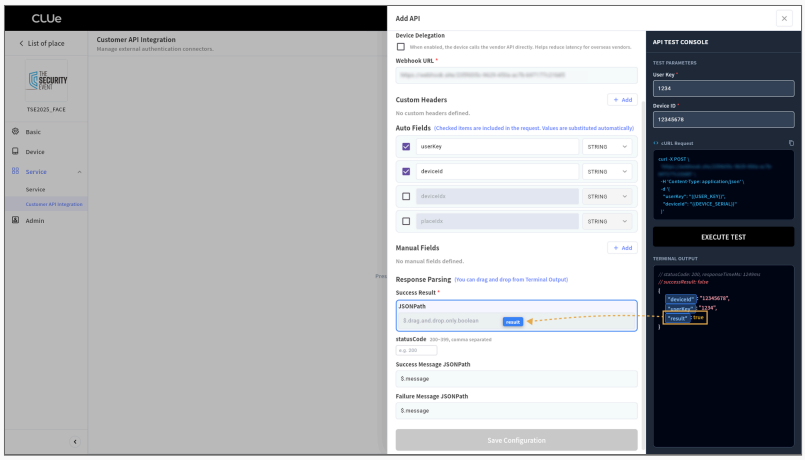
Success Message JSONPath / **Failure Message JSONPath** (Optional)

- Specify the key to extract the string shown on the device for success and failure. `$.message` is commonly used.
- You can save even if you do not specify it. If left blank, the system judges only allow or deny and does not show a message on the device.
- You can set different keys for success and failure.
- The value for the specified key must be a string, and it should not be too long for the device screen.

Tip

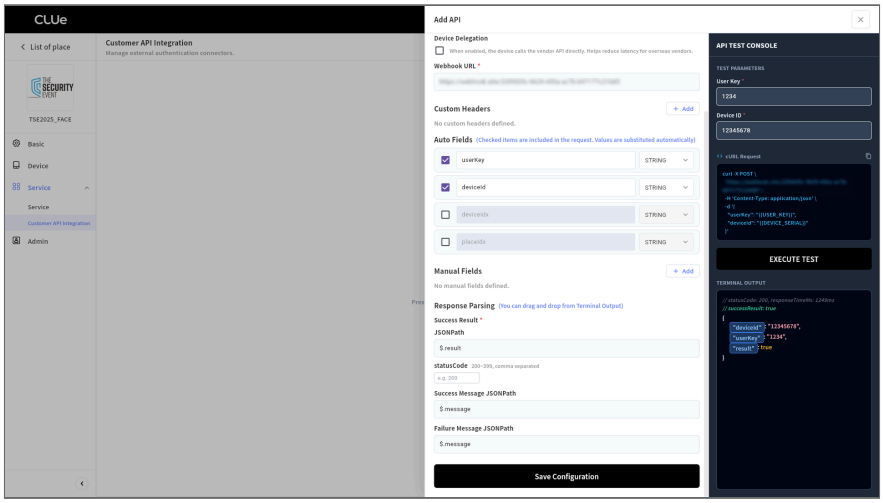
If direct JSONPath input is difficult

Drag and drop fields from the response area into the **Success Result JSONPath**, **Success Message JSONPath**, and **Failure Message JSONPath** inputs. The JSON path fills in automatically. You do not need to write the JSONPath manually.



13 Save

The **Save Configuration** button at the bottom of the **Add API** panel activates when all required fields and judgment criteria are entered correctly, and the API test succeeds at least once.

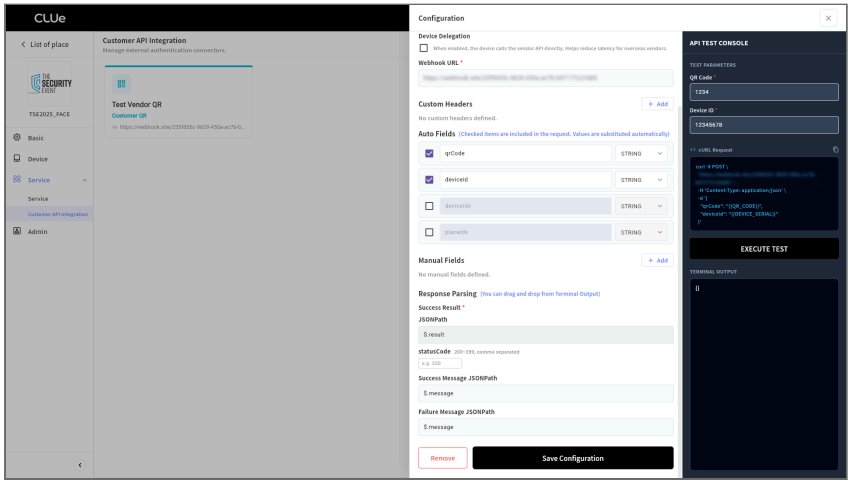


- If any required field is missing, the URL format is invalid, a manual field value cannot convert to the specified type, judgment criteria are missing, or the test has not succeeded, including network errors, the **Save Configuration** button remains disabled.
- To complete the registration, click the **Save Configuration** button.

When you save the API, the panel closes and the newly registered API appears in the list as a card. The card shows information such as the name, credential type, and registered URL.

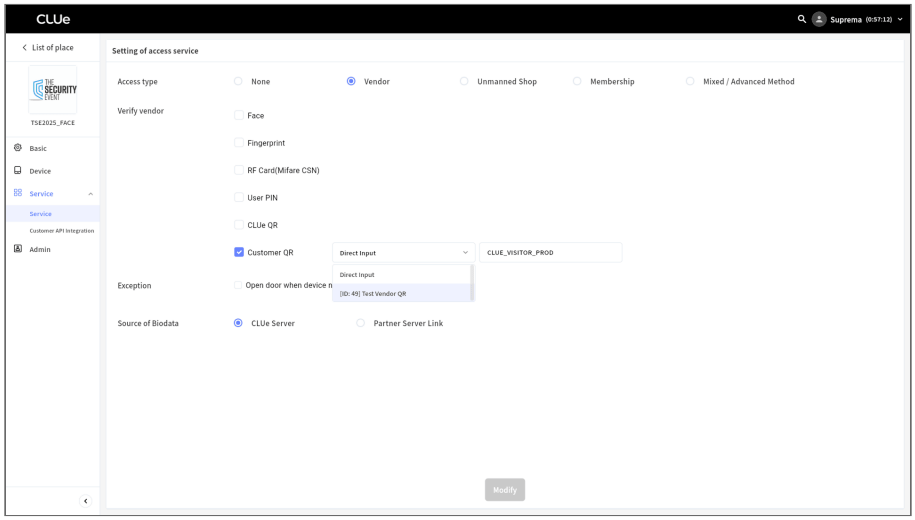


- To edit an API, click the card. The edit panel opens. You can edit **Connector Name**, **Webhook URL**, **Auto Fields**, **Manual Fields**, and **Response Parsing**. **Auth type** cannot be changed.
- **Remove**: Delete the registered API. If this API was connected to a credential, that connection is removed automatically, and the change applies to the device immediately. A disconnected credential then works with device authentication only, without customer verification. If you worry about an operational gap, register and connect a replacement API before deletion.



Step 3 — Assign APIs to each credential

On the left sidebar, click **Service** → **Service**. In the **Verify vendor** section, specify the API for each credential.

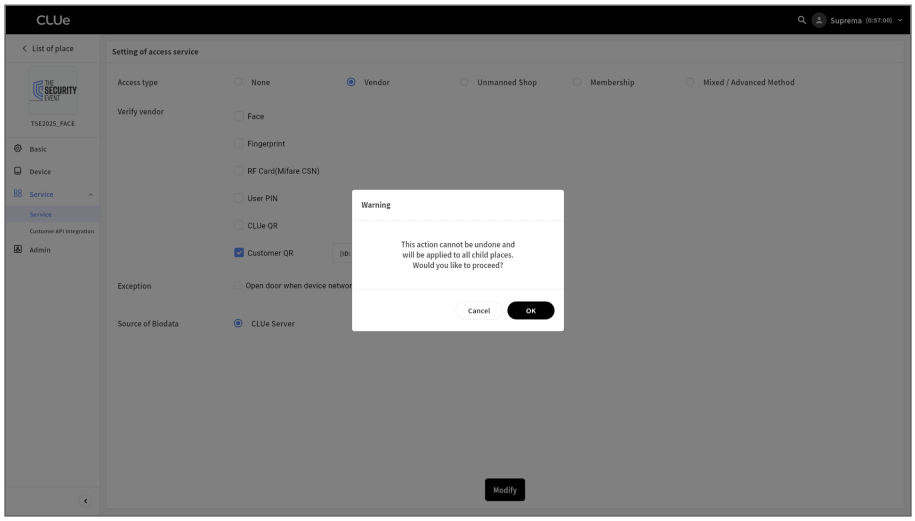


- Click the dropdown next to each credential to show the list of registered APIs. Only APIs that match the selected credential and **Auth type** appear.
- For each face, fingerprint, RF card, PIN, CLUe QR, and custom QR credential, select the API to use. You can assign a different API to each credential.

- A credential without an assigned API works with device authentication only. No verification request is sent to the customer API for that credential. Leave unassigned only the credentials that do not need customer verification.

Save and apply rules

After you assign the API registered to the credential and click the **Modify** button, a confirmation dialog asks whether to apply the change to sub-places.



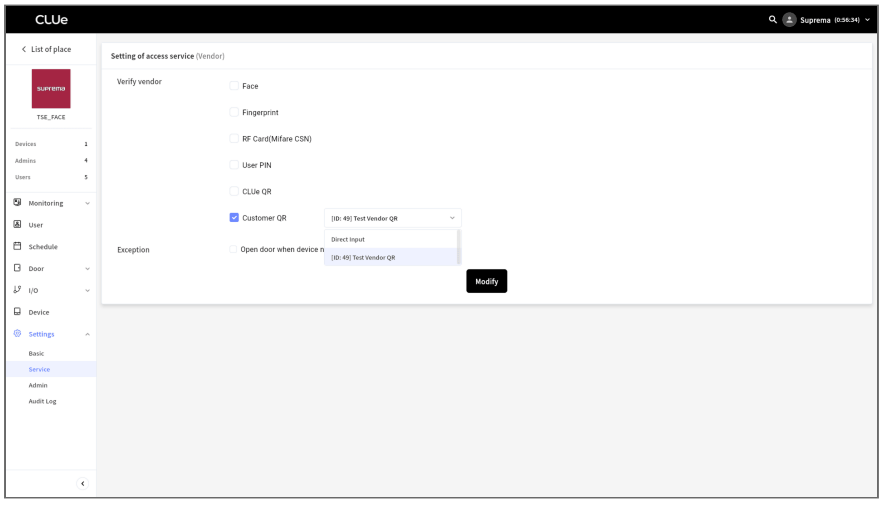
- **OK**: The same settings apply immediately to all sub-places in the current place group. Existing place-specific overrides are overwritten by the place group values.
- **Cancel**: Do not save the changes.

In most cases, place group-level settings are enough to keep all sub-places consistent. If you need a different API for a specific place, see Step 4 — Set a place-specific override (optional).

Step 4 — Set a place-specific override (optional)

This section explains how to assign a different API only to a specific place, instead of the settings inherited from the place group. Settings applied only to a specific place do not affect other places or the parent place group.

1. Move to a specific place under the place group.
2. On the left sidebar, click **Settings** → **Service**.



3. In each credential dropdown in the **Verify vendor** section, select the different API to use only for this place.

4. Click the **Modify** button to save the changes.

The changes save only to the current place. They do not apply to other places.

> **Info**
> Only place administrators invited as administrators for that place can access **Settings** → **Service**.

> **Caution**
> If you change the credential-to-API assignment in the parent place group after assigning an API to a specific place and save, the place-specific override is overwritten by the place group values. If you need to keep place-specific settings after a place group change, assign them again in that place's **Settings** → **Service** after updating the place group.

Summary of input rules

Field	Required	Rules
Connector Name	Yes	Up to 64 characters
Auth type	Yes	Cannot change after saving
Webhook URL	Yes	`https://` required / up to 512 characters / CLUe sends only **HTTP POST**/ `application/json` requests to this URL
Number of **Auth type** APIs	-	Up to **3** APIs per credential type can be registered
Custom Headers	Optional	Up to 10 Key/Value pairs / duplicate names not allowed (case-insensitive)
Auto Fields	Optional	Include only checked fields in the request / key names can be edited / the system fills in the values automatically
Manual Fields	Optional	Up to **10** fields total with auto fields / duplicate names not allowed / values convert to JSON data based on the selected type (`STRING` / `NUMBER` / `BOOLEAN`)
User Key (Test)	Depends on **Auth type**	1 to 64 characters
Device ID (Test)	Yes	Only 9 to 12 digits
Response Parsing	-	At least one of **statusCode** or **Success Result JSONPath** is **required**. If both are entered, combined validation activates.
statusCode	-	Integers in the 100 to 399 range / up to 3 / duplicates not allowed

Field	Required	Rules
Success Result JSONPath	-	1 field: `Key` + `Value` + data type (`BOOLEAN` / `STRING` / `NUMBER`)
Success Message JSONPath / **Failure Message JSONPath**	Optional	If specified, the key to extract from the response body. The value must be a string, and it must fit the device screen. If not specified, no message appears on the device.
Save conditions	-	Can save only after a successful test

Troubleshooting

Access issues (step-by-step troubleshooting)

See Setting workflow overview to narrow down the issue area.

Steps	Symptom	Check items
1	A specific credential is not recognized	Make sure the credential is enrolled on the device and active.
2	Device-server communication failed	Check the network connection and the device enrollment status.
3	The request does not reach the customer server	Check the registered URL (HTTPS), custom headers, and firewall rules.
4	The customer responds, but all attempts are denied	Check the judgment criteria, including the judgment mode, success key/value, and HTTP status code.
5	Allow/deny works correctly, but no message appears	Check **Success Message JSONPath**/**Failure Message JSONPath** and the message string in the response body.

Save Configuration button disabled

If you cannot click the **Save Configuration** button, check the following in order.

- **Required fields**: Make sure none of **Connector Name**, **Auth type**, or **Webhook URL** is blank.
- **Webhook URL**: Make sure it starts with `https://` and does not exceed the 512-character limit.
- **Manual Fields**: Make sure the value can convert to the selected type (`STRING` / `NUMBER` / `BOOLEAN`).

  > *Example: when you enter a non-numeric character in `NUMBER`*

- **Response Parsing**: Make sure you entered at least one of **statusCode** or **Success Result JSONPath**.
  - If you use **Success Result JSONPath**, make sure you entered the `Key` , `Value` , and data type.
  - **Success Message JSONPath**/**Failure Message JSONPath** are optional and do not affect saving.

- **API test**: Make sure at least one test succeeded. You cannot save without a successful test.

Test failure

Test failures fall into three types.

- (A) Blocked during input validation
- (B) Request sent, but the test failed
- (C) Response received, but the result is not as expected

(A) Blocked during input validation

The request itself does not send because the input does not meet the rules.

Symptom	Check items
Webhook URL format error	Make sure **Webhook URL** starts with `https://` and does not exceed 512 characters.
Judgment criteria key format error	Make sure **Success Result JSONPath**, **Success Message JSONPath**, and **Failure Message JSONPath** use JSONPath format starting with `$.`, up to 128 characters.
No judgment criteria specified	Make sure you entered at least one of **statusCode** or **Success Result JSONPath**.
Success status code range/count error	Make sure each value is in the 100 to 399 range, three or fewer values are set, and there are no duplicates.
Duplicate field key	Make sure the keys in **Auto Fields** and **Manual Fields** are unique and do not overlap.
Duplicate request header key	Make sure the request header keys are unique and do not overlap, case-insensitive.
Restricted header name used	Make sure you did not add `Content-Type` or `Accept` as custom headers. The system uses them as fixed values, case-insensitive.
Too many fields or headers	Make sure you have no more than 10 **Auto Fields** and **Manual Fields** fields, and no more than 10 custom headers.
Too many **Auth type** registrations	Make sure this credential type already has 3 registered APIs.
User Key format error	Make sure the **User Key** in the test console meets the allowed character set (letters, numbers, `-`, `_`, `@`, `.`) and the 1 to 64 character length.
Device ID format error	Make sure the **Device ID** in the test console is 9 to 12 digits.

(B) Request sent, but the test failed

The test result shows `success = false`, and you cannot save in this state.

Symptom	Check items
Connection failure / network error (no response from the customer server)	Check external access to the customer server, HTTPS certificate validity, firewall and port settings, and custom headers, such as expired tokens or typos.
Timeout (no response)	Customer server response delay, network status. The test fails if no response arrives within a few seconds.
Response received, but the body is not JSON	Check whether the customer returns a JSON response and whether the response `Content-Type` is set to `application/json`. This includes HTML error pages and blank text.

(C) Response received, but the result is not as expected

With `success = true`, the actual HTTP status code appears in **statusCode**, and the customer's raw response appears in **TERMINAL OUTPUT**. You can save, and you must configure response parsing based on the response at this step.

Symptom	Check items
Status code received, but all access is denied	**Modes 1 and 3**: Check the list of status codes that count as success. **Mode 2**: Check the key/value condition in the body. The status code is ignored.
Body field condition does not match	Check the `Key`, `Value`, and data type (`BOOLEAN` / `STRING` / `NUMBER`) entered in **Success Result JSONPath**. Check whether the response is `"true"` (STRING) or `true` (BOOLEAN). The type must match.
Manual Fields shows in an invalid format in the request body	Check again whether the **Manual Fields** type (`STRING` / `NUMBER` / `BOOLEAN`) matches the actual input value.

> **Info**
>
> - The test API shows the response body as is without parsing it, so use the actual response JSON shown in **TERMINAL OUTPUT** to match the JSONPath, key, and value settings.
> - See Access issues (step-by-step troubleshooting) to identify the failure cause on the device side.

Duplicate name issue

The key names in **Auto Fields** and **Manual Fields** cannot overlap. Request header keys also cannot overlap. If you changed an **Auto Fields** key name, make sure it does not conflict with **Manual Fields**.

No message appears on the device

- Make sure the response body actually contains the field specified by **Success Message JSONPath** or **Failure Message JSONPath**.
- Make sure the value for that key is a **string**. Numbers, objects, and arrays do not appear.

- Make sure the configured **Success Message JSONPath** / **Failure Message JSONPath** name matches the actual response key exactly.

Change the Firmware

The following devices support CLUe: With one firmware update, switch from the existing BioStar support mode to CLUe support mode.

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

> **Caution**
> Before updating the firmware, make sure the device has no user data left on it. If user data remains, it may conflict with user information synchronized from the CLUe system.

Switch to CLUe support mode

> **Info**
> To pre-enroll the device before the firmware update, provide the device serial number (SN) and model name (for example, BS3-DB) to Suprema Global Technical Support Team. The pre-enrollment process will proceed.

1 Prepare a CLUe support firmware version

Obtain it through your local Suprema branch or the CLUe team. The versions available for the device are as follows.

- *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*

> **Info**
> The suffix `AU` means "Auto Update to CLUe FW".

2 Check the internet connection

Before updating the firmware, make sure the device can connect to the internet and the CLUe server.

After the CLUe firmware update, the device automatically gets the certificate from the CLUe server, applies it, and then tries to connect, so an internet connection is required. The device also gets an IP address through DHCP by default, so make sure it can receive a dynamic IP address.

- The default network setting is DHCP.
- Use the 8.8.8.8 DNS server.

3 Proceed with the firmware update

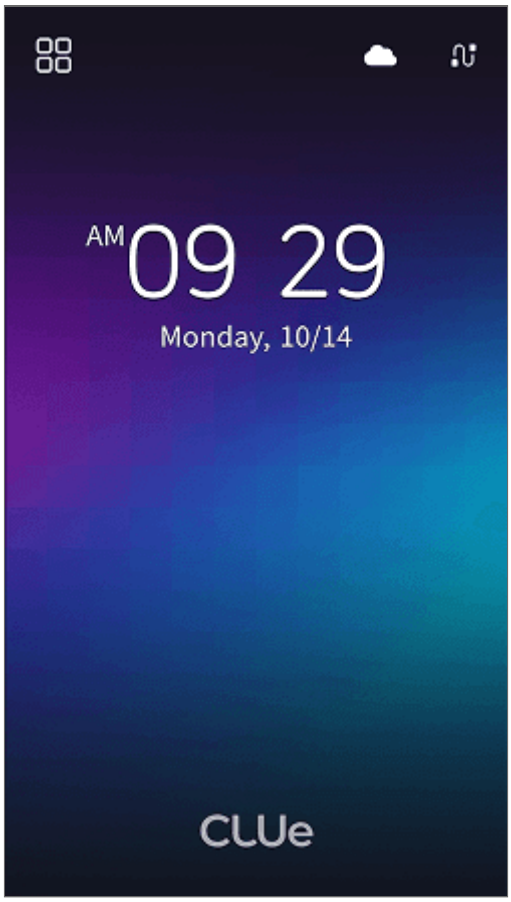
During the update process, the device reboots at least 2 to 3 times.

The main firmware update may take some time, and the certificate and setting firmware load process completes relatively quickly. The entire process takes about 3~5 minutes, so keep the device powered on and connected to the internet until the update completes.

> **Info**
> You can also update the firmware using BioStar 2 or USB.

4 Confirm the update is complete

When all updates finish, the CLUe icon appears on the device main screen.



For devices without a display, enter the serial number in the CLUe portal to check the device enrollment status.

5 Register Device

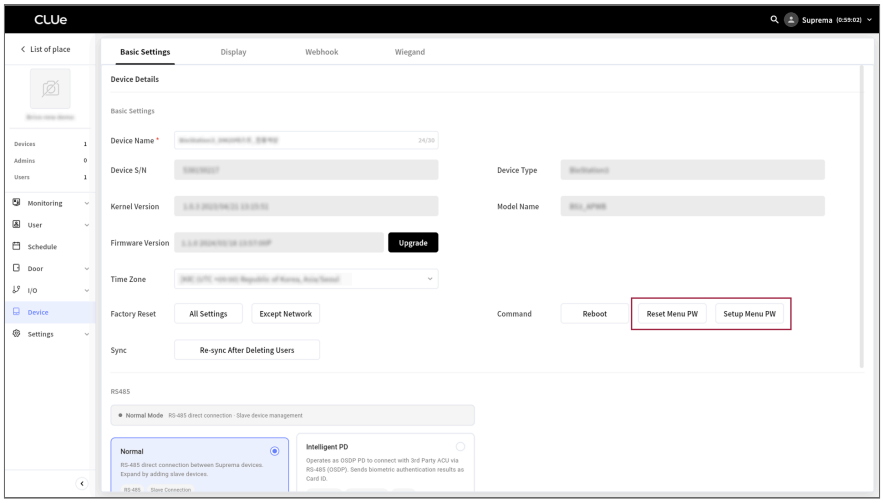
Ask the Suprema contact to assign the device to your account through the portal.

Then assign the device to the specified Place and use it with the door setting. For secure device management, the CLUe system requires each Branch manager to assign devices to the corresponding Place group.

6 Set the device menu password

After the firmware update, devices with an LCD display prompt you to set a menu password. Follow the on-screen instructions to set the password. You can also set the password through the CLUe portal.

Unlike BioStar devices, CLUe devices are often used without user data. Therefore, set a menu password to prevent unauthorized changes to menu settings.



Troubleshooting

If the cloud icon does not appear on the device screen, check the following:

- First, check the internet connection. The device connects directly to the cloud server, so it must stay connected to the internet. CLUe firmware also uses standard HTTPS port 443 for outbound communication.
- If the cloud icon still does not appear, run a **Ping test** on the device to check the internet connection.

Device	Path
BioStation 3	Menu (⊞) → **SETTINGS** → **NETWORK** → **Ethernet** → **Ping Test**
BioLite N2	**ESC** → **NETWORK** → **TCP/IP** → **Ping Test**
X-Station 2	Menu (⊞) → **NETWORK** → **Ethernet** → **Ping Test**

  - If the **Ping test successful** pop-up appears, the internet connection is working properly.
  - If the **Unknown** or **Fail** pop-up appears, check whether the network blocks the DNS in use.

Add Device

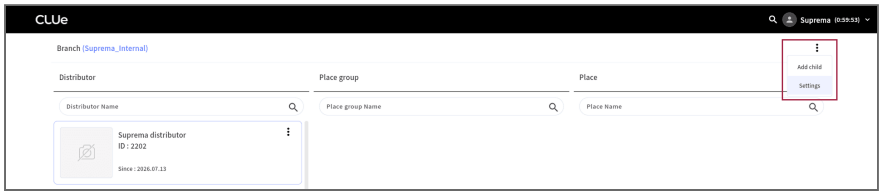
To use a CLUe device, complete enrollment and assignment in the web portal. Only the Branch manager can enroll devices, and the Distributor manager or Place group manager assigns enrolled devices to their assigned place.

Customers who purchased a new device should check that the CLUe firmware and certificate are applied, then request device enrollment from the Suprema branch.

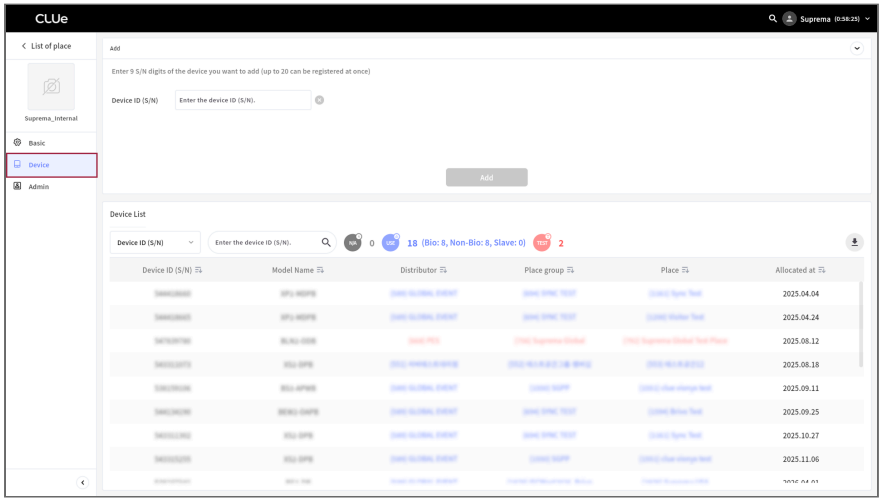
Device enrollment (Branch manager)

Only the Branch manager can enroll devices. Check the device serial number before enrolling the device. Find the serial number on the sticker attached to the back of the device.

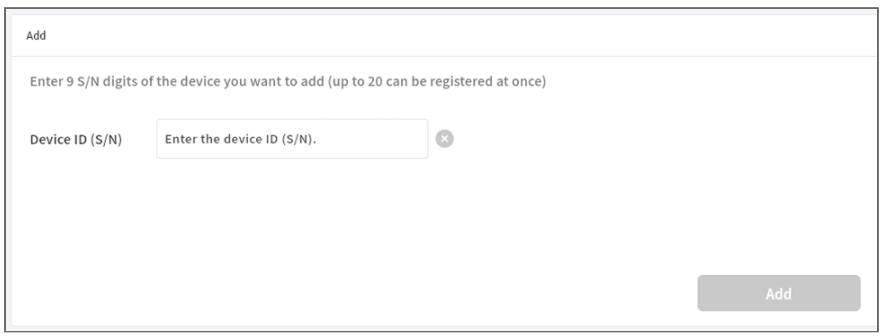
1. Log in to the CLUe web portal.
2. On the initial screen, select the Branch to enroll the device.
3. In the upper-right corner of the screen, click ⋮ → **Settings**.



4. Click **Device** in the left sidebar.



5. In the **Add** section, enter the device serial number in the **Device ID (S/N)** input field, then click **Add**.



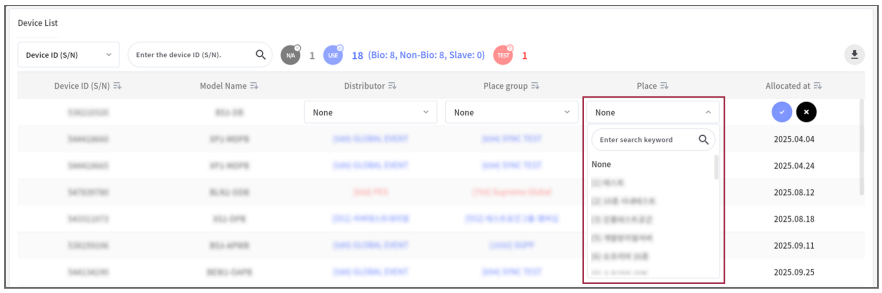
6. The added device appears in **Device List**.



7. To enable edit mode, click the **None** field and select .



8. Select the Distributor, Place group, or Place to assign the device.



9. Click to apply the selected option.

A success message for device assignment appears at the top of the screen. When you click each field, the button activates, and you can move to the corresponding Distributor, Place group, or Place. Click the button to move to the location, then set the device and door.

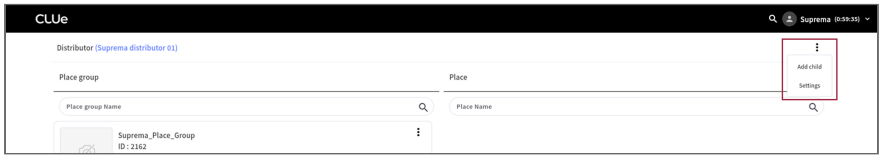


Device assignment

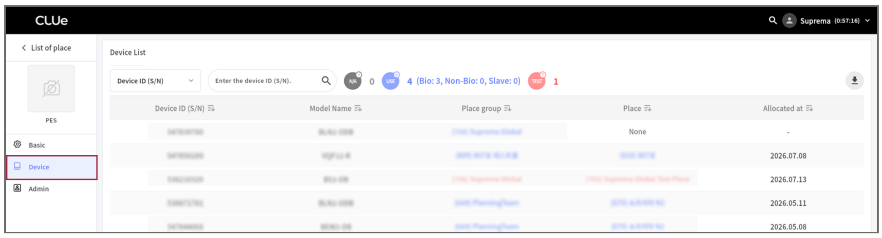
Distributor manager

The Distributor manager can assign devices assigned to them to a lower Place group or an individual Place. If the device that needs enrollment does not appear in the list, contact the relevant Suprema branch or headquarters.

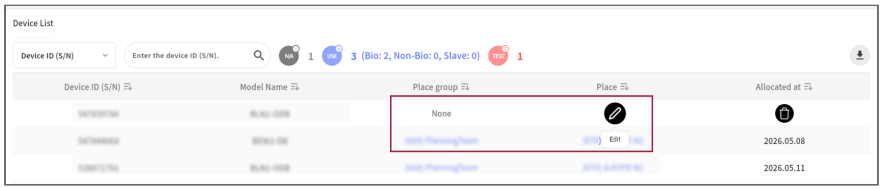
1. Log in to the CLUe web portal.
2. On the initial screen, select the Distributor to assign the device.
3. In the upper-right corner of the screen, click ⋮ → **Settings**.



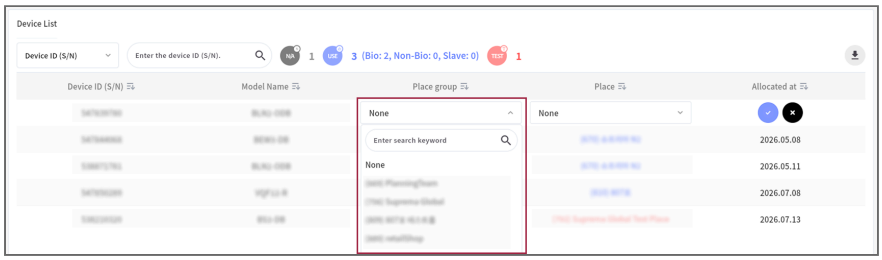
4. Click **Device** in the left sidebar.



5. To enable edit mode, click the **None** field and select .

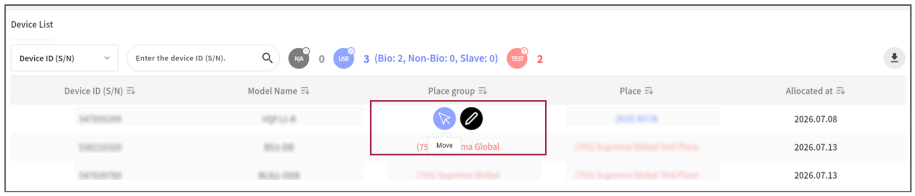


6. Select the Place group or Place to assign the device.



7. Click to apply the selected option.

A success message for device assignment appears at the top of the screen. When you click each field, the button activates, and you can move to the corresponding Place group or Place. After assignment, move to the Place and add a door.



Info

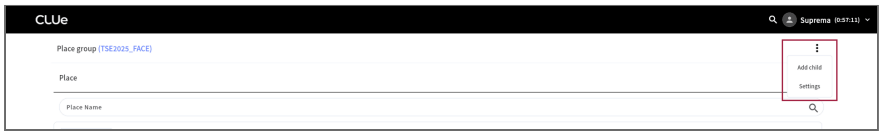
- By default, the Distributor manager cannot view the Users and Monitoring tabs under the privacy policy. If access is required, request an invitation from the Place group, Place manager.
- When you delete a device, it returns automatically to the Branch-level device list and becomes unassigned. If you deleted a device by mistake, ask the Branch manager to reassign it.

Place group manager

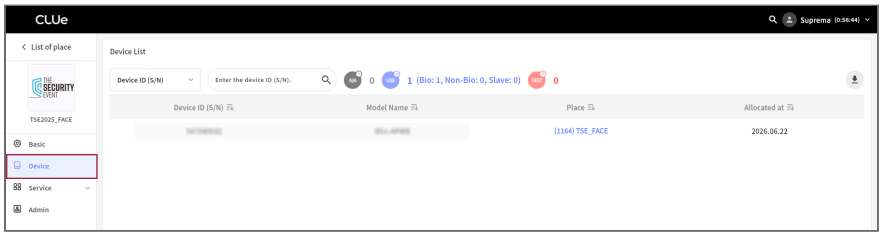
The Place group manager can assign devices assigned to them to a lower Place.

1. Log in to the CLUe web portal.
2. On the initial screen, select the Place group to assign the device.

3. In the upper-right corner of the screen, click ⋮ → **Settings**.



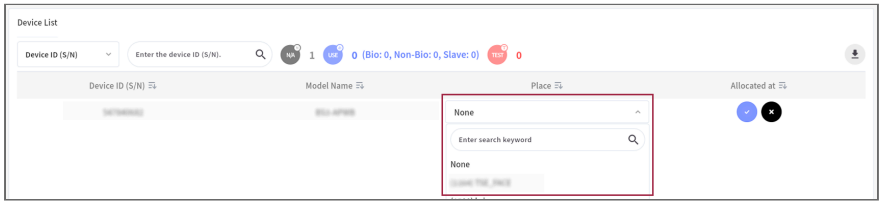
4. Click **Device** in the left sidebar.



5. To enable edit mode, click the **None** field and select .



6. Select the Place to assign the device.



7. Click to apply the selected option.

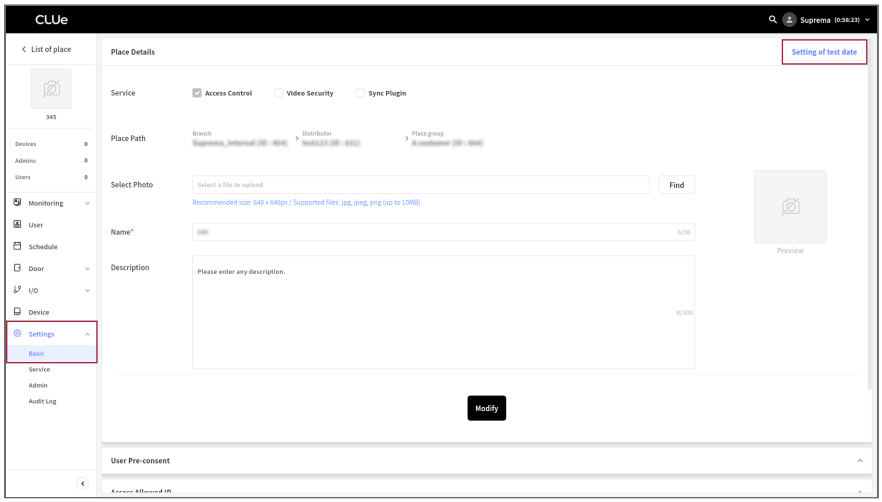
A success message for device assignment appears at the top of the screen. After device assignment, move to the corresponding Place and add a door.



Test place setting (Branch manager)

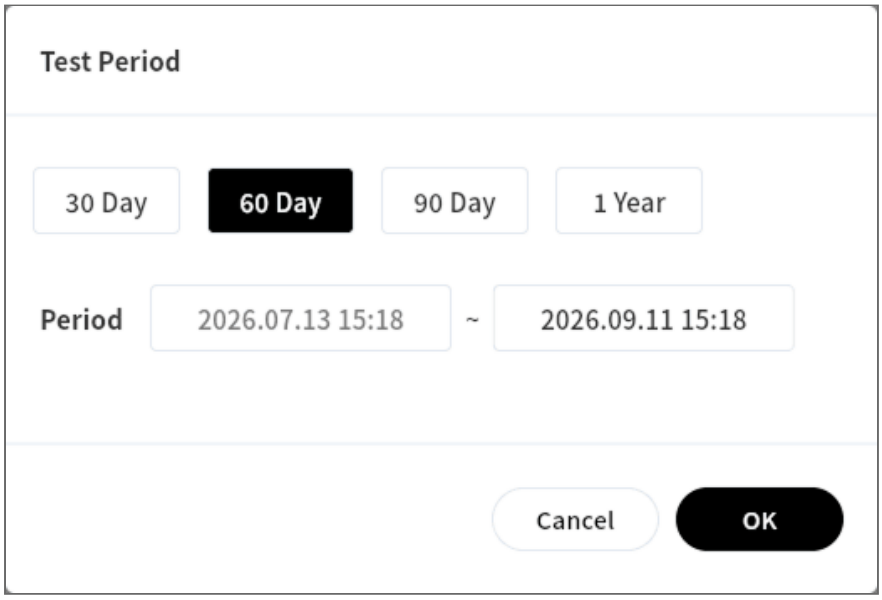
Because subscriptions are based on the number of devices, separate test devices and exclude them from the total. To do this, users with the Branch manager role can designate certain places as "test places" in Place settings.

1. Log in to the CLUe web portal.
2. Select the Place to designate as a test place.
3. On the left sidebar, click **Settings** → **Basic**.



4. Click **Setting of test date** in the upper-right corner of the screen.

5. When the **Test Period** popup appears, set the test period.



   To use it without a time limit, set the end date to **9999.12.31 23:59**.

6. To finish, click **OK**.

All devices in the Place appear in red in the device list, so they are identified as test devices. You can also check the total quantity information.



Next step

Learn how to upgrade the device firmware.

Self-Register Device

Even when installers cannot log in to the CLUe portal onsite, they can register a device to a Place using only the information the admin prepared in advance. This feature is called Device Self-Registration, and it consists of an admin preparation step performed in advance and an onsite registration step performed by the installer.

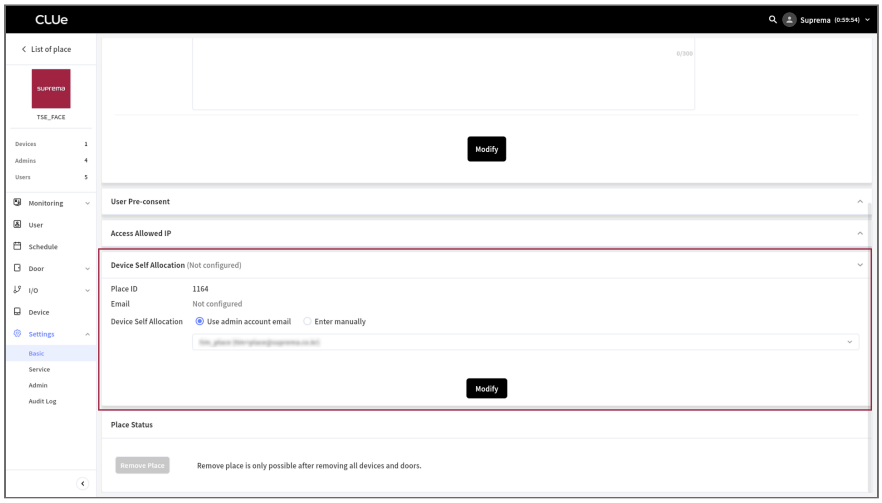
Supported devices and firmware versions

Device model	Supported firmware version
X-Station 2	2026.06.01 or later
BioStation 3	2026.05.26 or later
BioLite N2	2026.06.01 or later
XPass 2	2026.06.01 or later
BioEntry W3	Not supported
BioEntry W2	Not supported

Admin preparation step

Before starting onsite registration, the Place admin must check the Place ID in the CLUe portal and set the device allocation email address. If you do not set it, you cannot receive the allocation code onsite. Only admins invited with Place admin or higher permissions can access it.

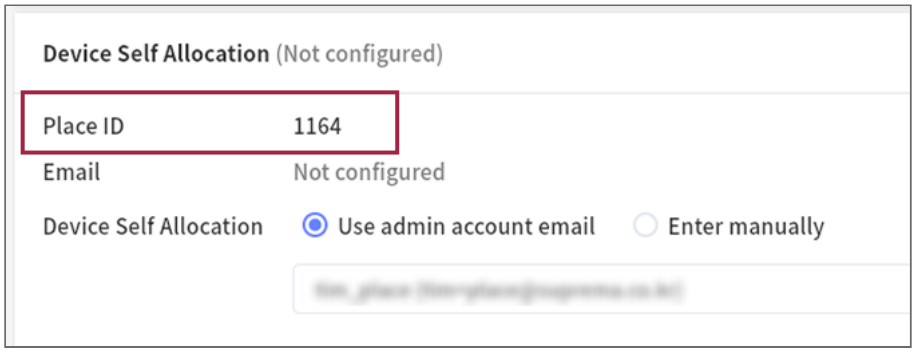
1. Log in to the CLUe web portal.
2. Go to the Place where you will allocate the device.
3. On the left sidebar, click **Settings** → **Basic**.
4. Click the **Device Self Allocation** section.



The **Place ID** (read-only) field and the **Device Self Allocation** email address field appear.

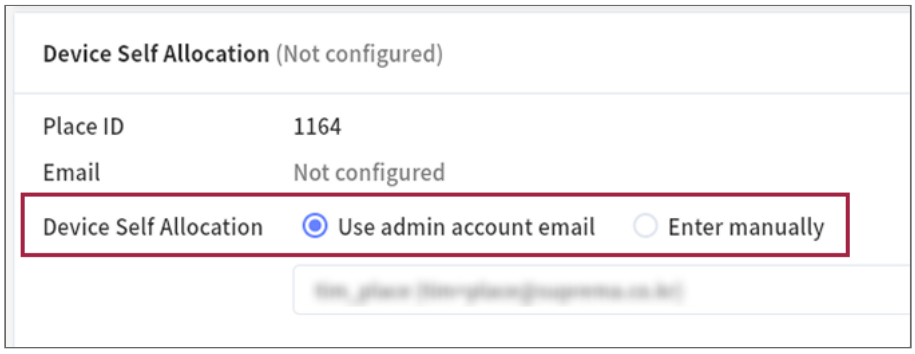
Check the place ID

Place ID is read-only. Share this number with the onsite installer. The installer can enter the Place ID on the device to complete registration. Entering the wrong Place ID is the most common cause of registration failure, so share it accurately.



Set the device allocation email address

Set the device allocation email address using one of two methods.



- **Use admin account email**: Automatically fills in the email address of the admin account currently signed in.
- **Enter manually**: Enter any email address manually. Enter it in the usual email address format, up to 254 characters.

In both methods, the entered email address is stored on the server as entered. The system does not distinguish whether the recipient is an admin, onsite installer, or third party. You can set only one allocation email for each Place. When you create a new Place, the allocation email starts unset, so set the email first to use the self-registration feature.

What happens if you do not set an email address?

If an installer executes **Send Allocation Code** in a Place without a set allocation email, the error "The admin must set the allocation email address first." appears.

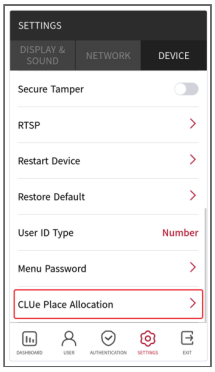
Onsite registration step

The registration process for devices with LCDs (LCD device self-registration) and devices without LCDs (Device self-registration without LCD (web server)) follows the same principle, but the screens differ. First, this guide explains the concepts that apply to both.

Steps	Trigger and Action	Result
Send allocation code	Enter the Place ID, then execute **Send Allocation Code**.	The server generates a 6-digit allocation code and sends it to the Place's allocation email address.
Enter allocation code	Enter the code you received by email within the specified time.	If the code matches, the device registers to that Place.

LCD device self-registration

The screens below are examples. Actual screen layouts and button names may differ by device model and firmware version. Proceed based on the guidance shown on the screen.

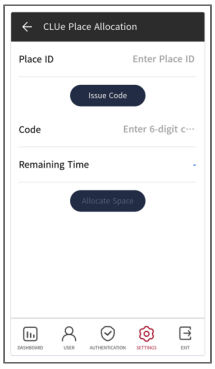


1 Go to Place registration

In the device settings menu, select **DEVICE** → **CLUe Place Allocation**. The Place registration screen appears.

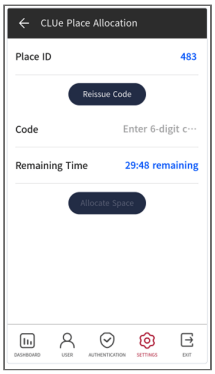
Info

- Menu names and locations may differ by device model and firmware version.
- If the device already belongs to a specific Place, Place group, Distributor, or Branch, you cannot enter the registration screen, and a message appears stating that it is already registered.



2 Enter the Place ID

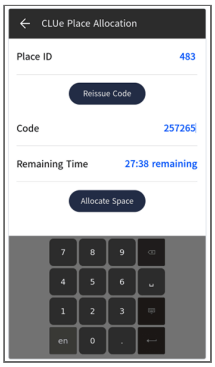
Enter the Place ID you received from the admin using the numeric keypad. If you enter an ID that does not exist, or a Branch, Distributor, or Place group ID instead of a Place ID, an error message appears. Check the Place ID again, then enter it.



3 Send allocation code

Enter the Place ID, then execute **Issue Code**. The server generates a 6-digit allocation code and sends it to the allocation email address for that Place. The device switches to the allocation code entry screen.

> **Info**
>
> If no allocation email is set, an error message appears. In this case, ask the admin to set the allocation email address.



4 Enter the allocation code

Enter the 6-digit code you received by email within 30 minutes. If the code expires or does not match, an error message appears.

> **Info**
>
> - To enter the code again or request a new one, tap the **Reissue Code** button.
> - If you enter the code incorrectly five times in a row, the issued code is discarded. Return to the previous step and request a new code.

5 Registration complete

Tap the **Allocate Space** button. If the code matches, the device registers to that Place, and a registration complete message appears. After that, the device switches to the normal access operation screen.

A registered device cannot change Places onsite. If you need to change it, do it in the CLUe portal.

Device self-registration without LCD (web server)

Devices without LCDs cannot register a Place on the device body. Use a web browser on a PC or mobile device connected to the same network as the device to access the device's web server and complete registration.

Access the device web server

Enter the following address in the web browser address bar on a device connected to the same network as the target device.

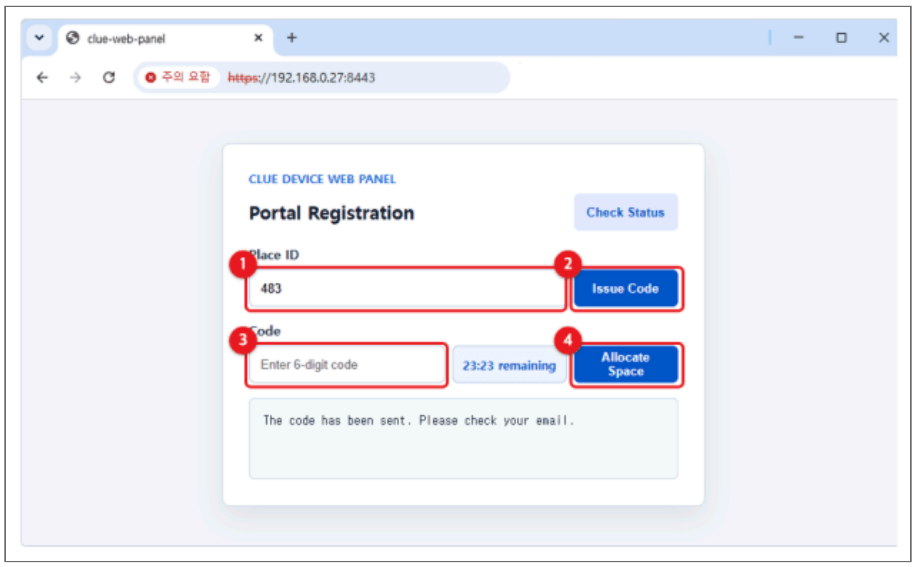
> *https://* *{device_IP_address}* *:* *{port}* *— for example, https://192.168.0.27:8443*

- Refer to the installation guide for each device to check the device's IP address and port.
- If you use a self-signed certificate, the browser may show a security warning: "Not Secure." Continue to open the registration screen.

If the device is not yet registered to any Place, the Place registration screen (**CLUe Device Web Panel**) appears. If the device belongs to a specific Place, a message appears stating that it is already registered, and you cannot access the registration screen.

Register on the web

Follow the instructions below to complete Device Self-Registration.



1 Enter the Place ID

Enter the Place ID you received from the admin in the **Place ID** input field. If you enter an ID that does not exist or is not a leaf Place, an error message appears. Check the Place ID again, then enter it.

2 Send allocation code

Enter the Place ID, then click the **Issue Code** button. The server generates a 6-digit allocation code and sends it to the allocation email address for that Place.

> **Info**
> If no allocation email is set, an error message appears. In this case, ask the admin to set the allocation email address.

3 Enter allocation code

Enter the 6-digit code you received by email within 30 minutes. If the code expires or does not match, an error message

appears.

> **Info**
>
> - To check the current registration status, click the **Check Status** button.
> - To receive the code again, click the **Reissue Code** button. However, the same device must wait 60 seconds after the previous code send before sending again.
> - If you enter the code incorrectly five times in a row, the issued code is discarded. Return to the previous step and request a new code.

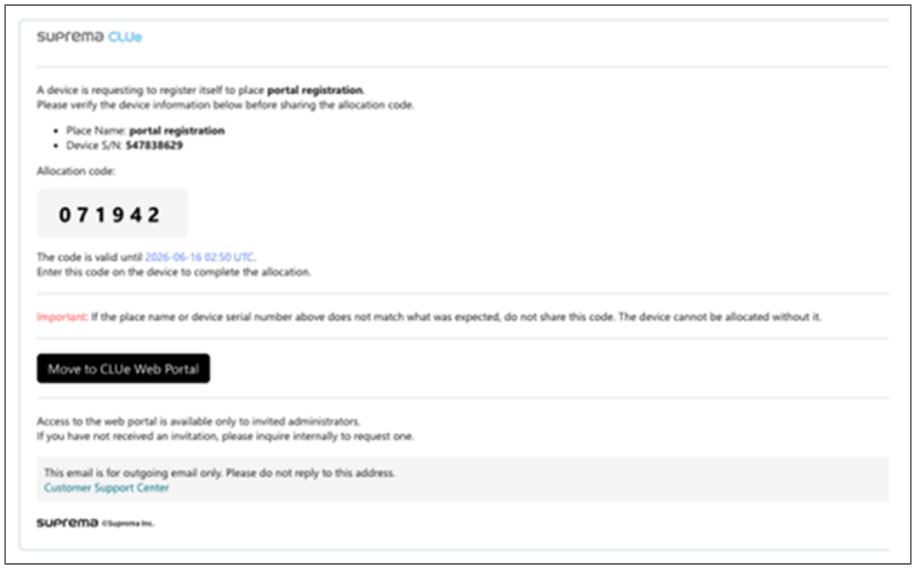
4 Registration complete

Click the **Allocate Space** button. If the code matches, the device registers to that Place, and a completion message appears. After registration completes, the web server runs for about 3 more minutes, then shuts down automatically. After that, attempts to access the same address no longer connect. This is normal behavior to prevent unnecessary resource use and enhance security. To change the Place after registration, do it in the CLUe portal.

Notes

Check allocation code email

When you execute **Send Allocation Code** (**Issue Code**), the system sends an allocation code email to the allocation email address set for the Place. Before entering the allocation code, the recipient must check the email body to confirm that the target for registration is correct.



The email subject includes the device serial number (deviceSn). In the inbox list, the subject alone identifies which device the code belongs to. When installing several devices at once, use the serial number in the subject to distinguish each device's email.

Already registered device (re-registration not allowed)

A device that already belongs to a specific Place, Place group, Distributor, or Branch cannot be registered again onsite. If you enter the registration menu (**CLUe Place Allocation**) on an LCD device or access the web server for a device without an LCD, the following message appears and access to the registration screen is blocked.

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

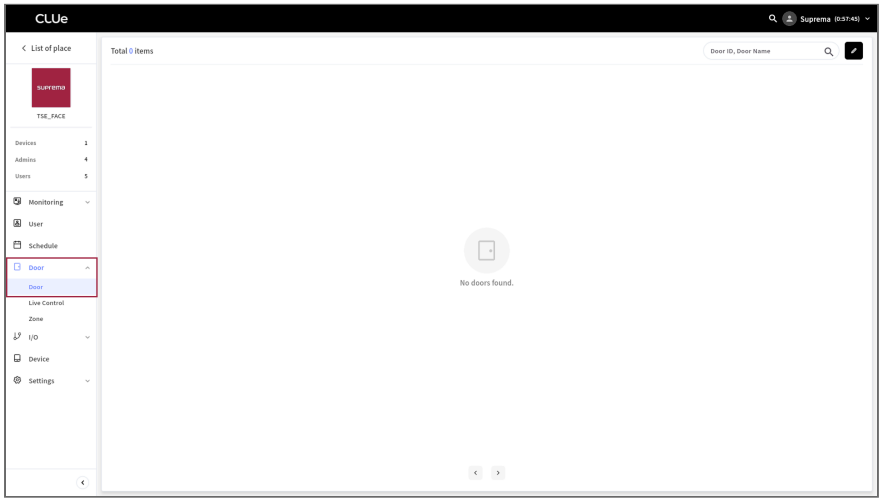
You can change or unassign a Place only in the CLUe portal, not onsite. In rare cases, the device itself may appear to belong to no specific Place, but the server already has it registered, such as when it was pre-registered in the portal. In that case, executing **Send Allocation Code** also shows the same already-registered error message. In this case too, change it in the portal.

Add Doors

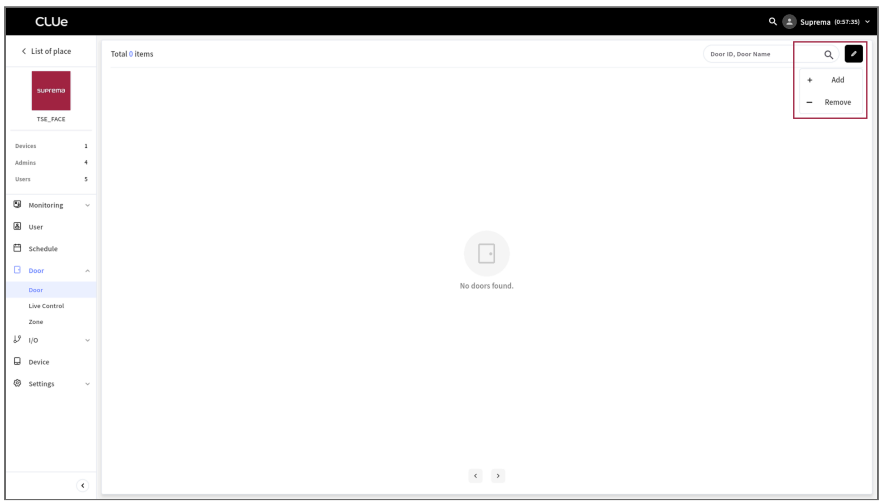
Door settings are required in CLUe. If you do not configure doors, communication with the server, including user synchronization, will not work properly. Complete this step before you start the service.

Access control setting

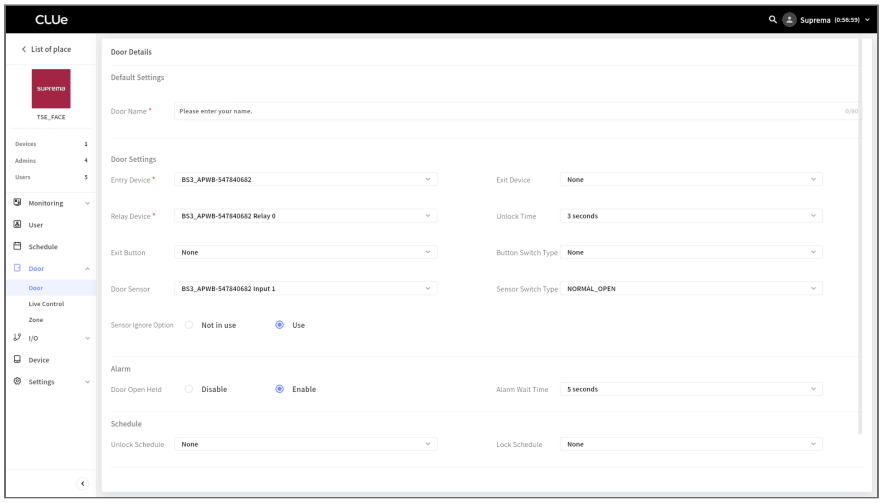
1. Log in to the CLUe web portal.
2. Select the Place where you want to add a door.
3. On the left sidebar, click **Door** → **Door**.



4. At the top right of the screen, click ✎ → **Add**.



5. Enter the door name, and select any other required settings, such as the entry device, relay, and exit button.



6. After you complete the door settings, click the **Add** button.

> **Info**
>
> **Sensor Ignore Option**
>
> - **Use**: The door relay changes state after the lock time passes, regardless of the door sensor status.
> - **Not in use**: The door relay does not return to its original state, even if the door sensor detects an open state. Select this option if you configure an automatic door.

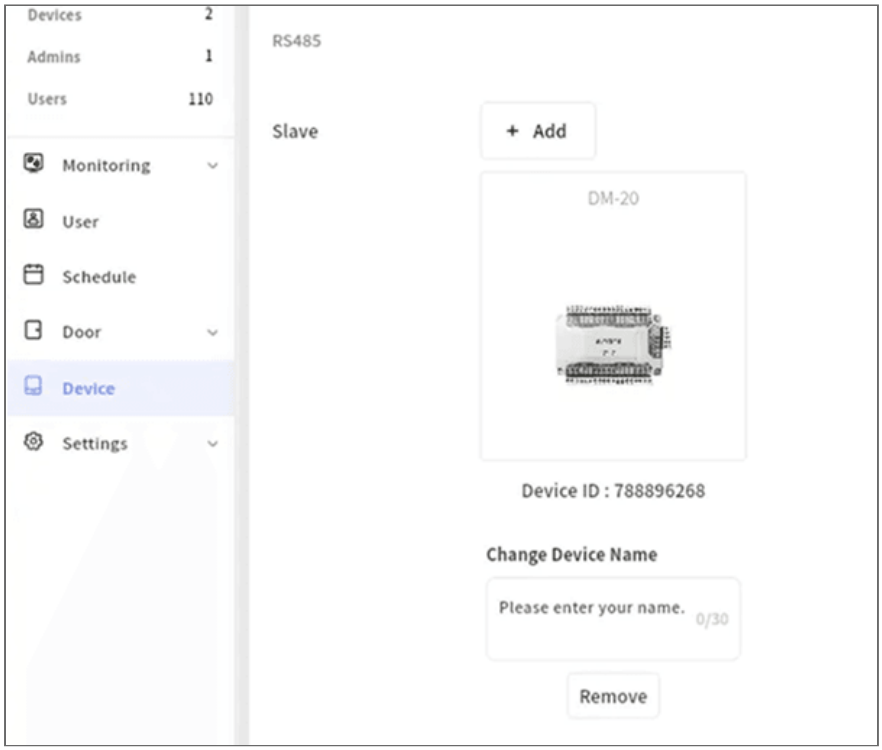
Use slave device relays

If you use an RS485 slave device, such as SIO2, DM-20, or DI-24, assign it to a separate Place, even if it connects to the master device. Assign it to a Place the same way you assign a standard device. For information on how to assign a device to a Place, see Add Device.

- Check the slave devices in the device list.



- Select the master device, and add the connected slave devices. Then, you can use the relay and input ports on the slave devices.


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

Upgrade Firmware

Upgrading the firmware on a CLUe device lets you apply new features, performance improvements, and security patches. The upgrade takes only a few clicks in the CLUe web portal and takes about 5 to 10 minutes to complete.

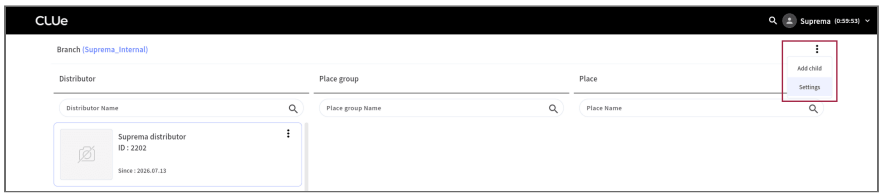
Before starting the upgrade, check the following:

- You cannot use the device during the upgrade, and when it restarts, the door may briefly open or close depending on the lock connection method.
- If you change device settings during the upgrade, the changes apply after completion.

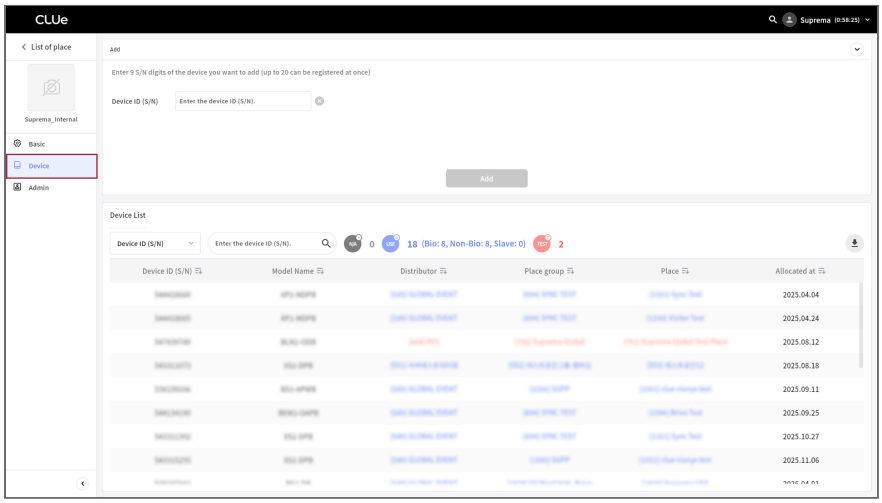
Go to a place

To upgrade an access device assigned to a place, go directly to that place, or navigate through the upper Branch, Distributor, or Place group.

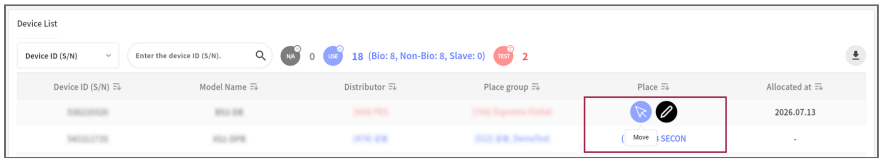
1. Log in to the CLUe web portal.
2. On the initial screen, select a Branch, Distributor, or Place group.
3. Click ⋮ → **Settings** in the upper right of the screen.



4. Click **Device** in the left sidebar.



5. In **Device List**, click the **Place** column for the device whose firmware you want to upgrade.

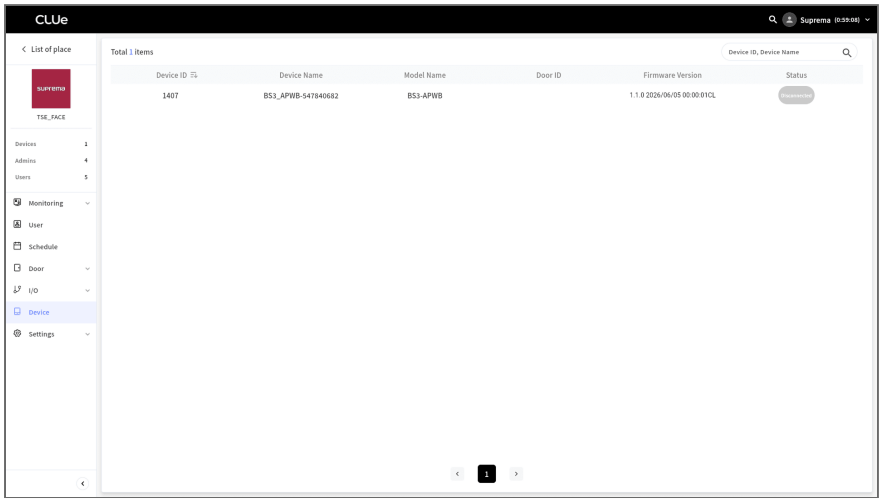


6. When the button becomes active, click it.

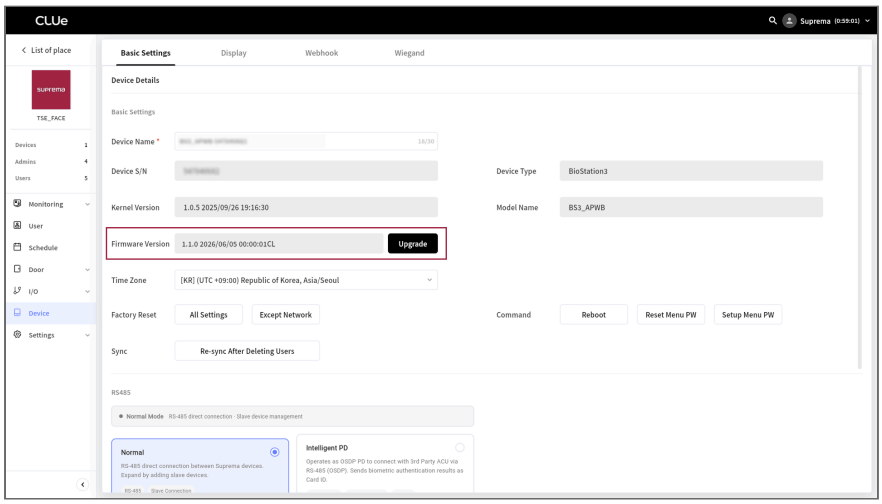
The selected device moves to the **Device** screen for the assigned place.

Firmware upgrade

1. In the **Device** list for the assigned place, click the device you want to upgrade.

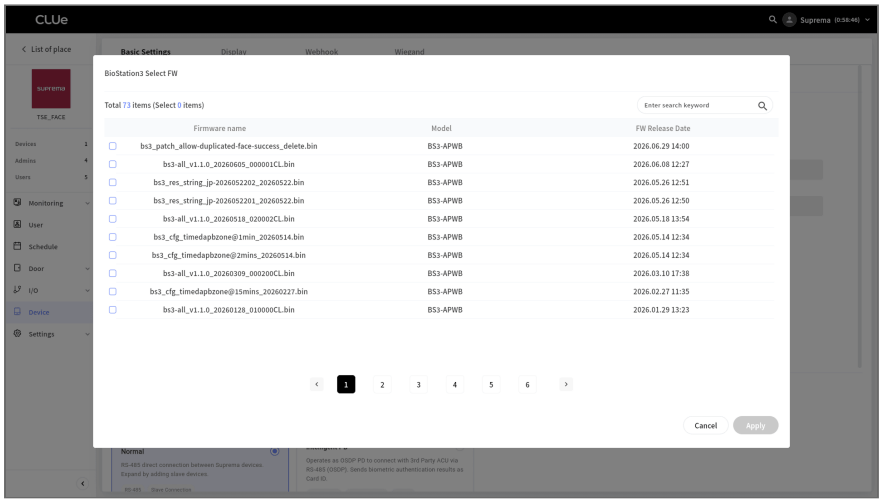


2. When the selected device's **Basic Settings** screen appears, check the current firmware version in **Firmware Version**.



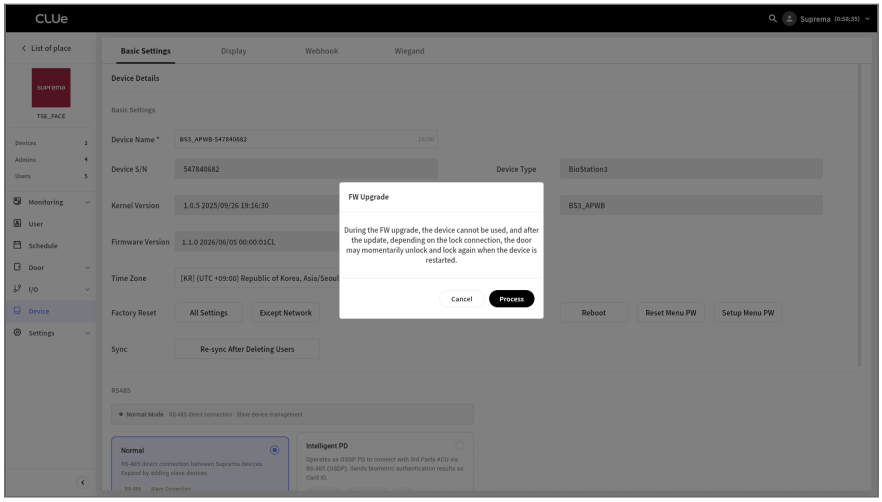
3. Click the **Upgrade** button.

4. When the firmware selection window appears, click the checkbox for the firmware you want to upgrade.

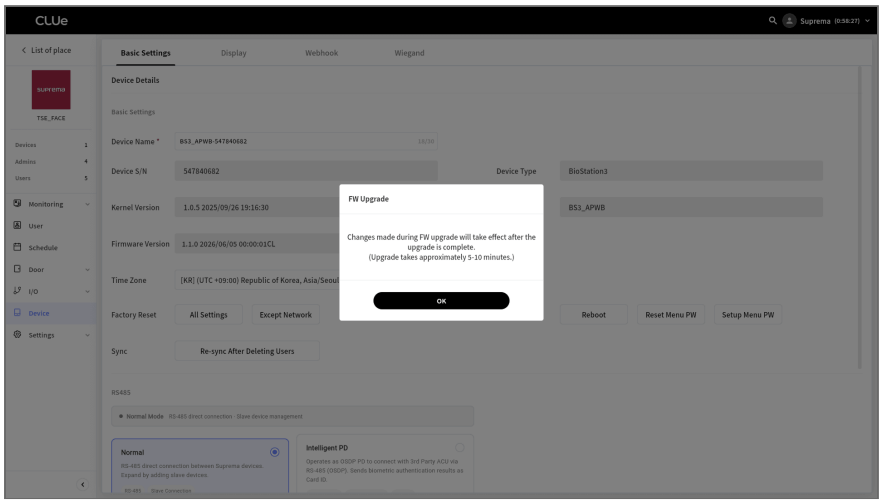


> You can select only one firmware version.

5. Click the **Apply** button in the lower right.
6. When the upgrade confirmation window appears, click the **Process** button.



7. When the message window appears, review the contents, and click the **OK** button.



Set Up Device Webhook

When you set up a webhook in the CLUe portal, the device sends real-time events to the endpoint you specify (an external server) when a specified event occurs. Use this feature for the following use cases.

- Integration with a time and attendance system
- Receive duplicated face detection events

You can also use it for various real-time, event-based integrations with systems.

Supported devices

Device	Model	Supported firmware version
BioStation 3	BS3-DB, BS3-APWB	`bs3-all_v1.1.0_20250626` or later

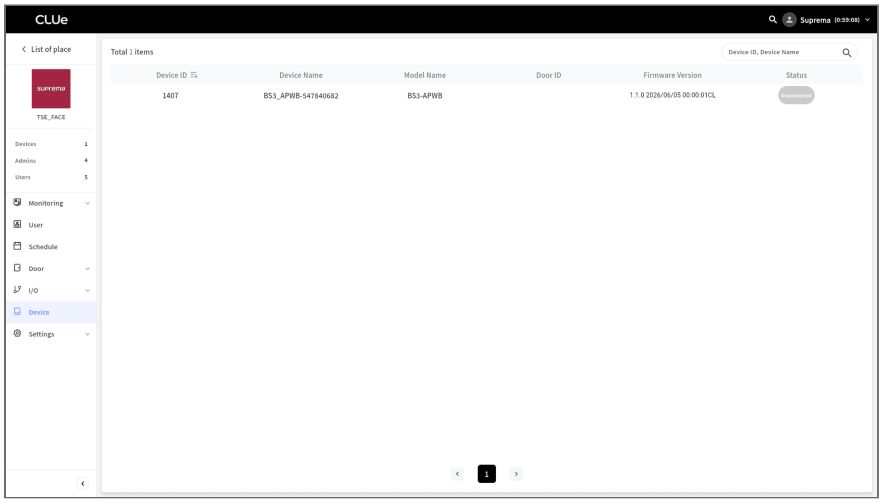
> **Info**
> The following CLUe supported devices will also support webhooks.
> - BioEntry W3, BioLite N2, X-Station 2, XPass 2

Key advantages

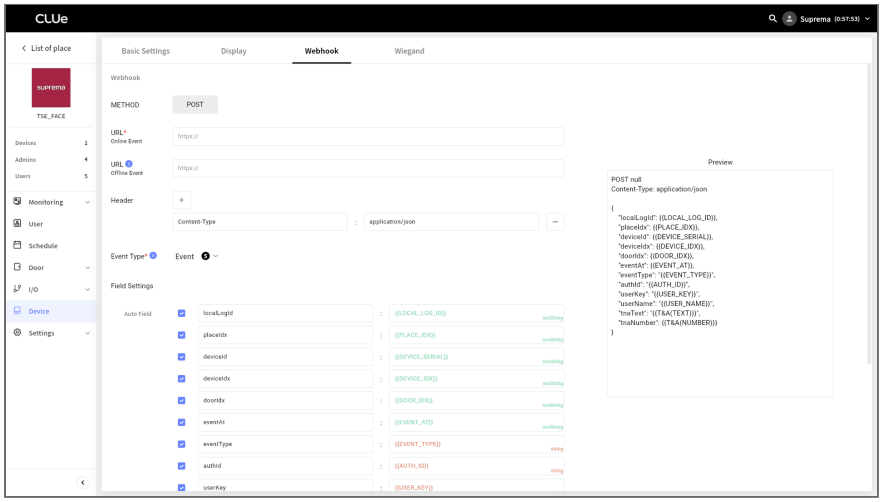
- Send the device's real-time event notifications to an external system.
- Integrate with external systems easily through webhooks.
- Supports use cases such as time and attendance integration and security event monitoring.

Webhook settings

1. Log in to the CLUe web portal.
2. Go to the Place assigned to the device where you want to set up the webhook.
3. Click **Device** in the left sidebar.
4. Select the device from the device list where you want to set up the webhook.



5. Click the **Webhook** tab at the top of the screen.



> **Info**
>
> If the **Webhook** tab does not appear, check the device's **CLUe firmware version** and update it to the supported firmware version or later.

1 Method

Webhooks use the **POST** method by default.

2 Endpoint URL settings

- **Online Event**: An endpoint that sends real-time webhook calls when a specified event occurs while the device is online.
- **Offline Event**: An endpoint that sends a list of events that occurred while the device was offline, after it comes back online.

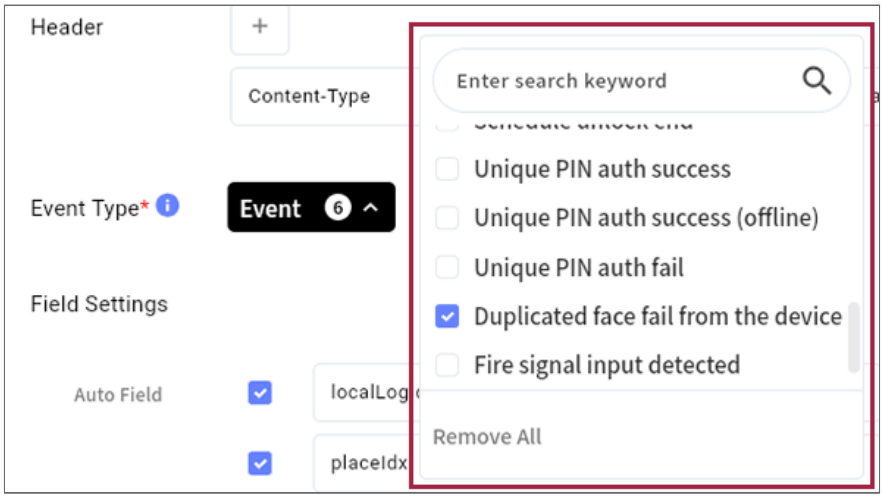
3 Header settings

Set the required keys or authentication values for the webhook server in the request headers. To add a header, click the + button.



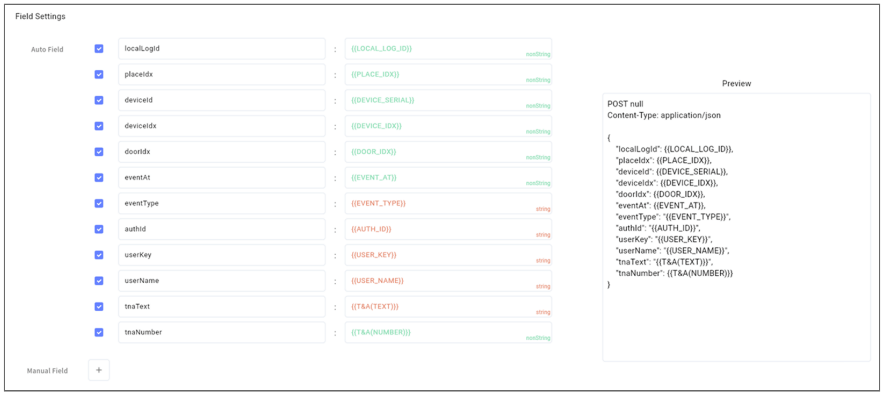
4 Select trigger events

Select the events that trigger webhook calls. In addition to the default selected events, you can also select events such as **Duplicated face fail from the device**.



5 Webhook field settings

To define the data the device sends, configure the **webhook fields**.



- **Auto Fields**: Indicates the type of data set the device can send.
- **nonString**: Refers to data types that do not use quotation marks (""), such as Boolean and int.

After selecting the required data fields, you can preview the webhook payload in the **Preview** panel.

If you also need to include fixed values, add them with **Manual Fields**. These values are sent as fixed values with the webhook payload.

6 Run a test call

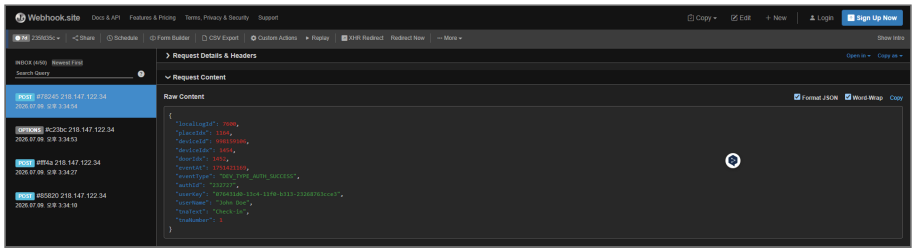
After completing the settings, you can run **Test Call**.



> **Info**
> A test call lets you check the structure and format of data sent directly from the browser to the configured endpoint, not the actual device.

Notes

Even if the server is not ready yet, you can test webhooks with a publicly available webhook testing service on the internet. For example, use Webhook.site to easily verify webhook calls.

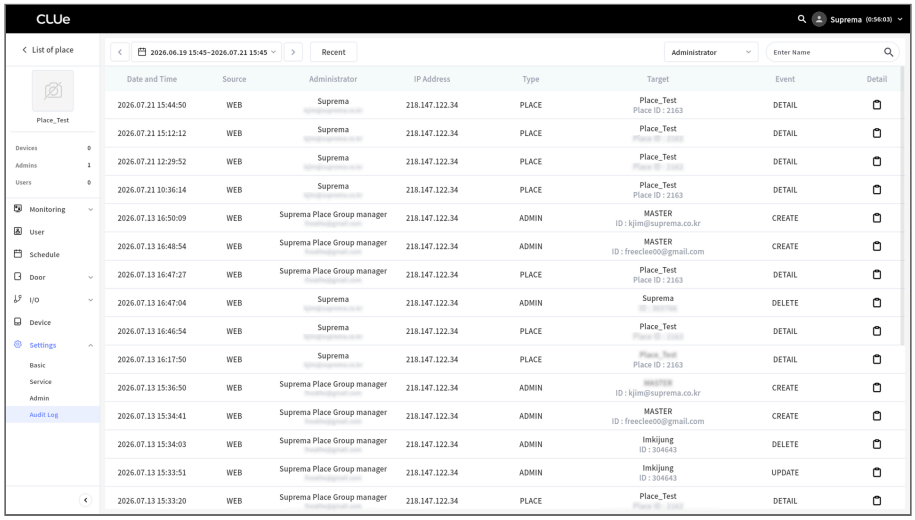

Webhook.site
Docs & API
Features & Pricing
Terms, Privacy & Security
Support
Copy
Edit
New
Login
Sign Up Now
Share
Schedule
Form Builder
CSV Export
Custom Actions
Replay
XHR Redirect
Redirect Now
More
Show Intro
INBOX (4/50)
Newest First
Search Query
POST #78245 218.147.122.34
2026.07.09. 오후 3:34:54
OPTIONS #c23bc 218.147.122.34
2026.07.09. 오후 3:34:53
POST #ff4fa 218.147.122.34
2026.07.09. 오후 3:34:27
POST #85820 218.147.122.34
2026.07.09. 오후 3:34:16
Request Details & Headers
Open in
Copy as
Request Content
Raw Content
Format JSON
Word-Wrap
Copy
{
"incallogId": 7600,
"placeId": 1150,
"deviceId": 69015190,
"doorIds": 3854,
"doorIdx": 105,
"eventAt": 1751421169,
"eventType": "DEV_TYPE_AUTH_SUCCESS",
"authId": "232727",
"userKey": "07643180-11c4-11f0-8313-2326876ccea3",
"userName": "John Doe",
"tnalext": "Check-in",
"cnaNumber": 1
}

View Audit Logs

The Audit Log feature records and tracks all activities that occur in a Place in the CLUe portal. Administrators can use **Audit Log** to check who performed which activity and when, and meet security and compliance requirements.

View audit logs

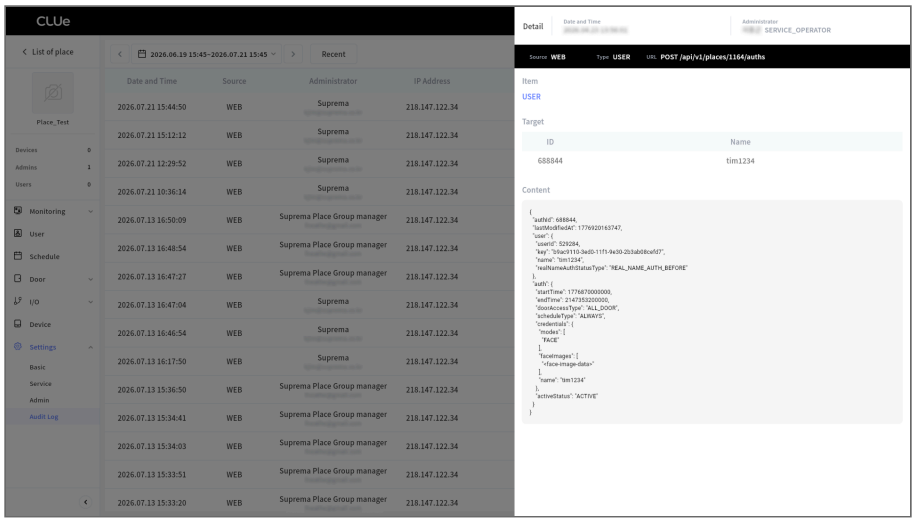
1. Log in to the CLUe web portal.
2. Select the Place where you want to view audit logs.
3. In the left sidebar, click **Settings** → **Audit Log**.



The most recent audit logs appear first in the list. Each log entry lets you check the **Date and Time**, **Source**, **Administrator**, **IP Address**, **Type**, **Target**, and **Event** for the activity.

View details

To view detailed information for an audit log entry, click the button in the **Detail** column at the far right of the list. The **Detail** panel appears on the right side of the screen.



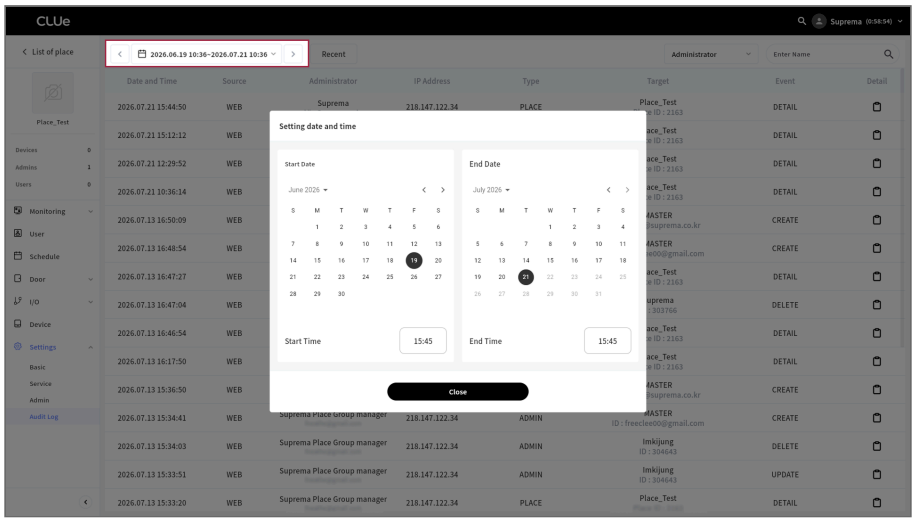
In the **Detail** panel, you can check **Source**, **Type**, and related APIs along with the date, time, and administrator account. It also provides the following information:

- **Item**: Shows the category where the activity occurred.
- **Target**: Shows the ID and name of the target where the activity applied.
- **Content**: Shows the API request body data. If no request body exists, it appears as an empty value ({}).

Set search period

To change the search period by the currently set unit, click ‹ or › at the upper left of the audit log list.

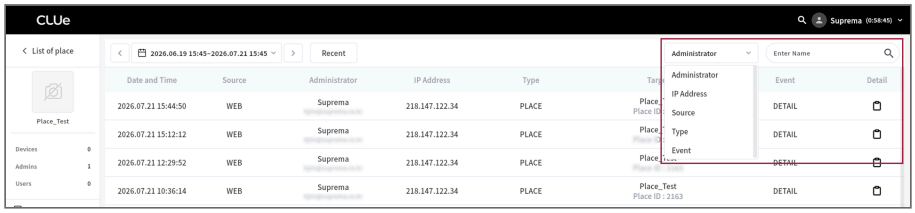
To view audit logs for a certain period, click the date and time area ( ). When the **Setting date and time** window appears, set the start date and time, and the end date and time. You can view audit logs for the set period.



> **Info**
> To clear the set search period, click the **Recent** button.

Search

Search or filter the data you need based on each column value in the audit log list. Use the search tools at the upper right of the audit log list.



- **Administrator**: Enter an administrator name to search. Searches are case-sensitive.
- **IP Address**: Search by IP address. Enter the exact IP address.

  > *Example: 192.168.1.1*

- **Source**: Select the condition for the platform where the user acted.

> *Web(**WEB**), Mobile(**MOBILE**), API(**API_TOKEN**)*

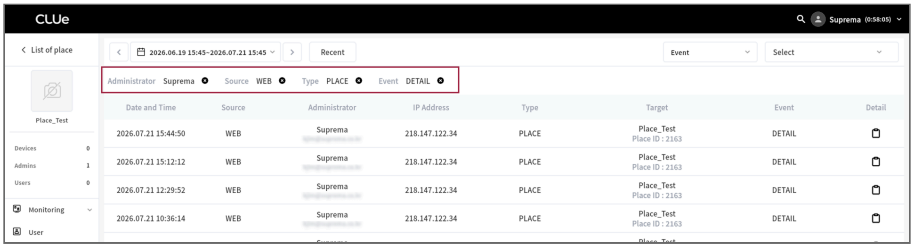
- **Type**: Select the user's activity category.

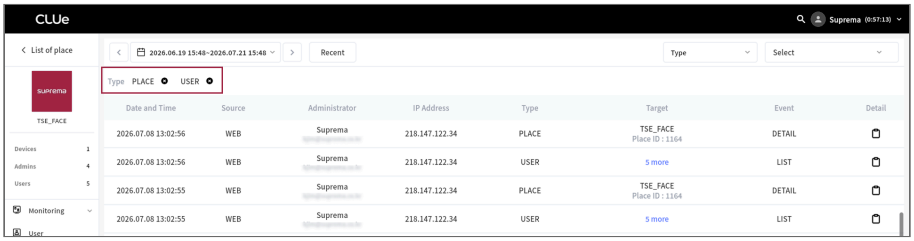
  > ***DEVICE**, **DOOR**, **PLACE**, **USER**, **PLACE STRATEGY**, **ADMIN**, **Access to personal information***

- **Event**: Select the following event condition.

  > ***DETAIL**, **LIST**, **CREATE**, **UPDATE**, **DELETE**, **COMMAND***

Select multiple filter fields together to filter. If you select different fields, filtering uses the AND condition. If you select multiple values for the same field, filtering uses the OR condition. To clear filtering, click the ✕ button.





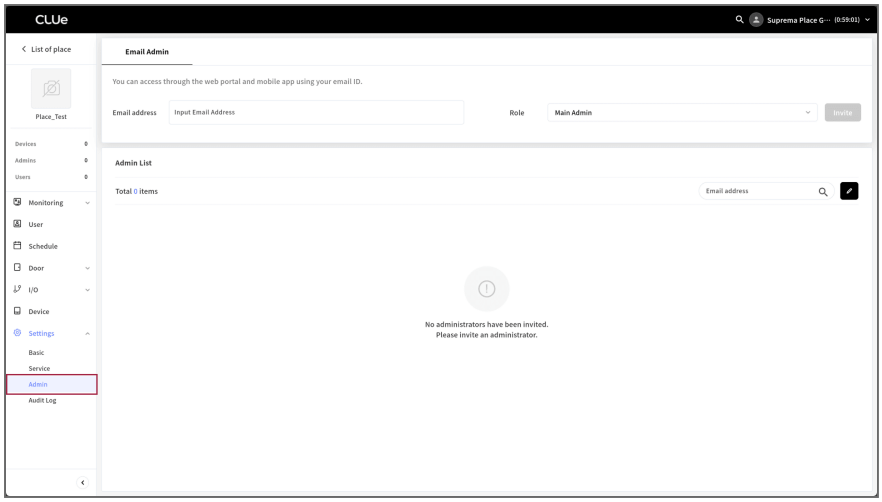
Using the Mobile App

With the CLUe mobile app, control doors remotely from your smartphone, manage users, and check place events in real time. This guide covers everything from how to invite place managers to downloading the app, signing in, and using the main features.

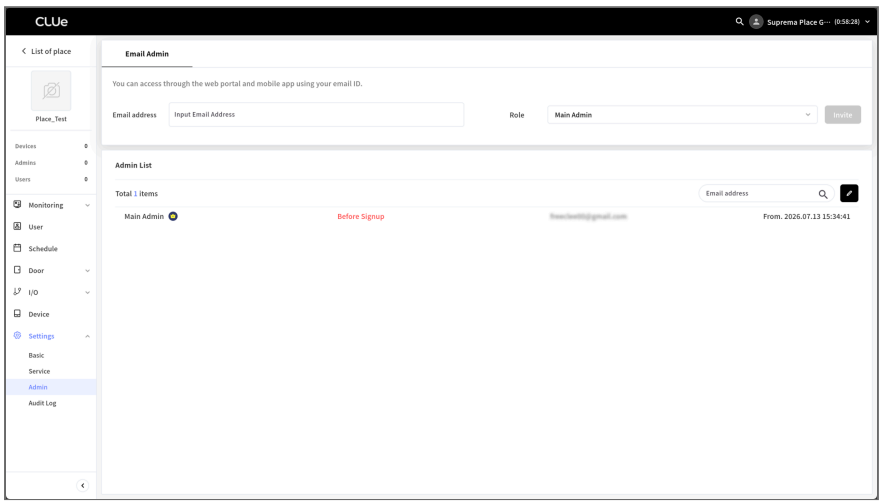
Inviting CLUe mobile app admins

A place group admin can invite place admins by email in Place settings.

1. Log in to the CLUe web portal.
2. Select the place where you want to invite a mobile app admin.
3. In the left sidebar, click **Settings** → **Admin**.

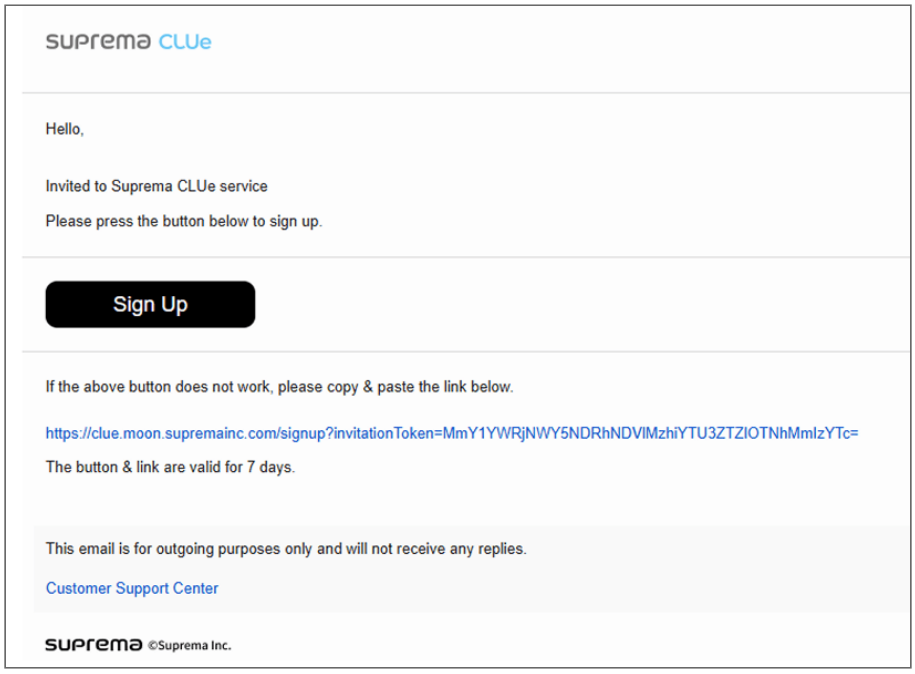


4. Enter the email address and select a role.
5. Click the **Invite** button.

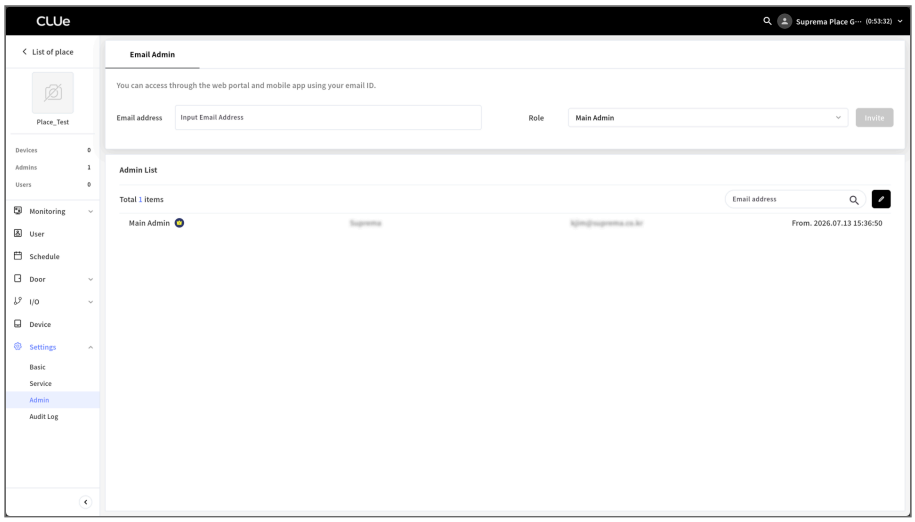


   Check the invitation status in the **Admin List** list.

After the invitation completes, the system sends an invitation email to the admin. The invited admin can join through the link in the email.



After joining, check the status change in the admin list.



Can I join directly in the CLUe mobile app?

Admins who cannot access the CLUe web portal can download the CLUe app and join from the mobile app. However, for actual use, the system must invite them to the place.

Download the CLUe app

Download the CLUe app from the link below or by scanning the QR code.

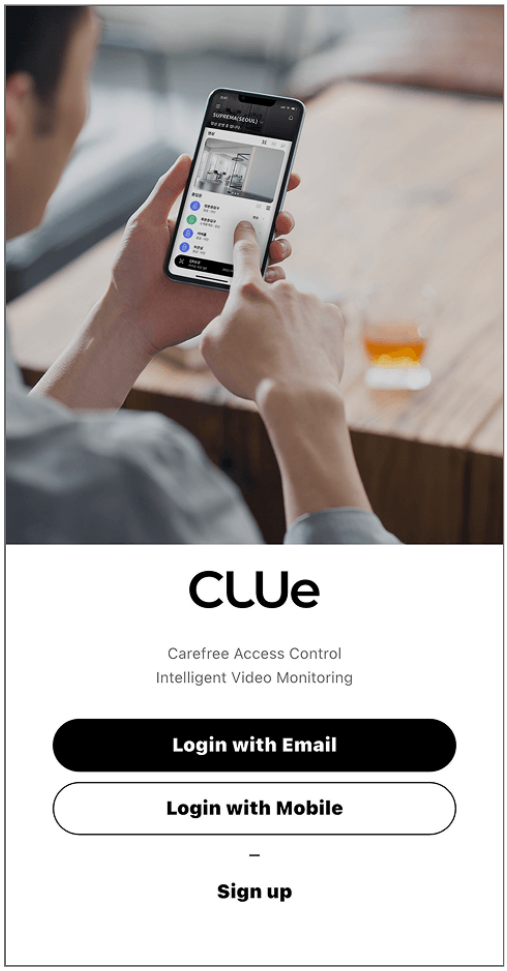
Platforms	Download link	QR code
iOS	App Store	
Android	Google Play	

Info
If you cannot find the app, search for "suprema clue" in the app store.

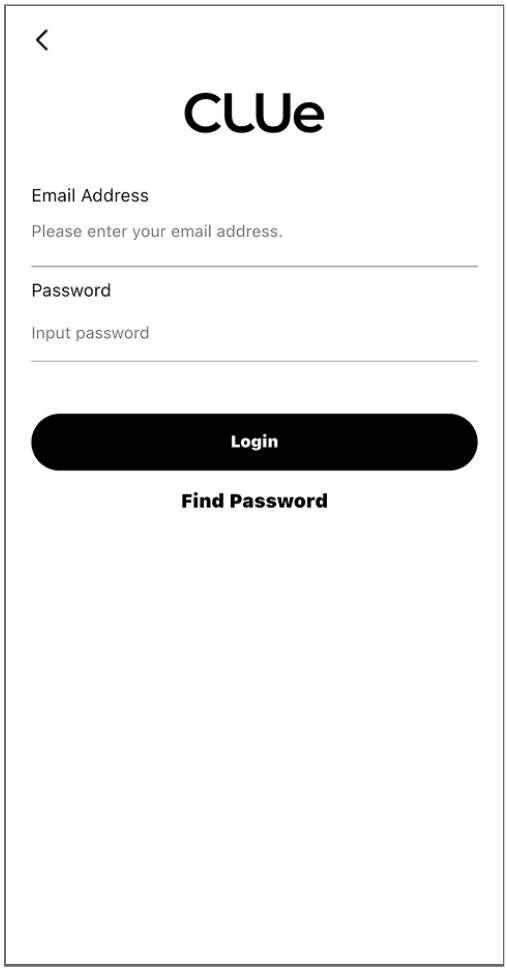
Log in

After installing the app, sign in with the invited email address.

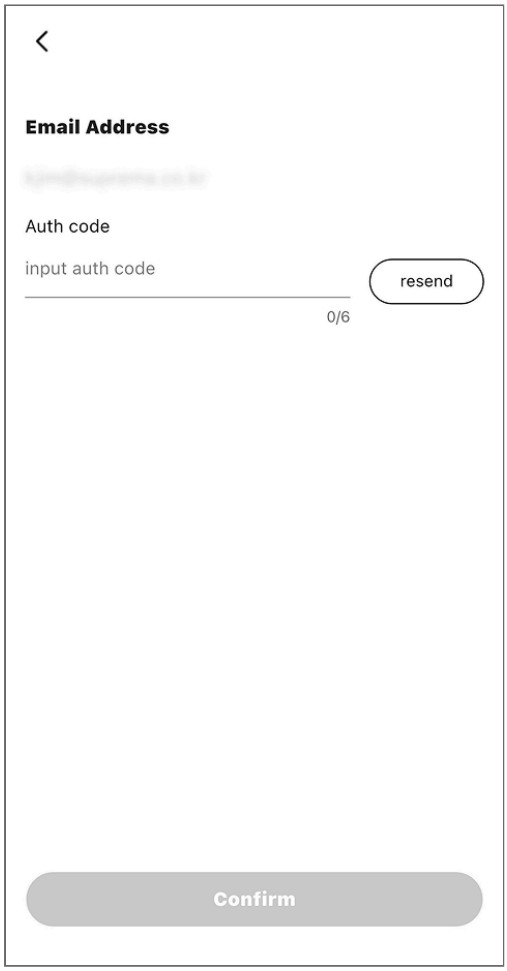
1. Open the CLUe app on your mobile device.
2. Select **Login with Email**.



3. Enter the email address and password, then tap the **Login** button.

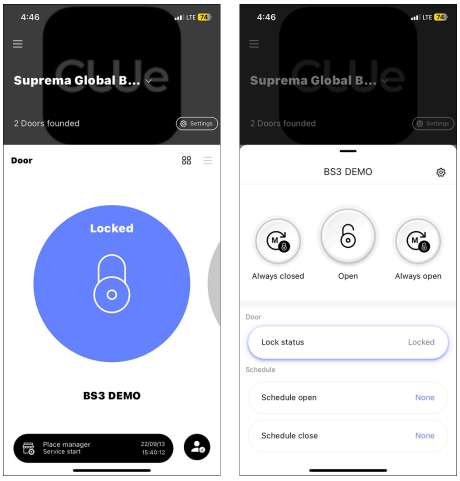


4. Enter the verification code sent to your email address, then tap the **Confirm** button.



You stay signed in until you sign out.

Main features of the CLUe app



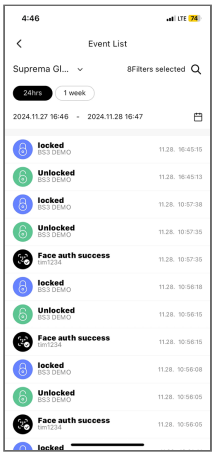
Remote door control

Check the current lock status of doors and control them remotely. Set a schedule to open or close doors automatically at specified times.



User Management

Invite or manage users. Use the CLUe mobile app and Suprema devices to enroll credentials such as face, fingerprint, and RF card.



Event monitoring

Check place events in real time, including door lock and unlock events, and authentication success and failure. View events by 24 hours or 1 week, or apply filters to quickly find the event you need.

CLUe API Guide

This document helps you integrate with Suprema CLUe API quickly and easily. This guide provides the basic information needed to use the CLUe API, from how to issue API keys to request and response formats, error codes, and rate limits. The CLUe API works with Suprema CLUe portal settings. If you do not have a CLUe portal account, request one first.

Learn more about using the CLUe API.

What is an API key

An API key is required to call the CLUe API. You can issue one from the administrator menu for the place group. CLUe API requires an API key as a Bearer token in the request header. You can issue and manage API keys in the CLUe portal.

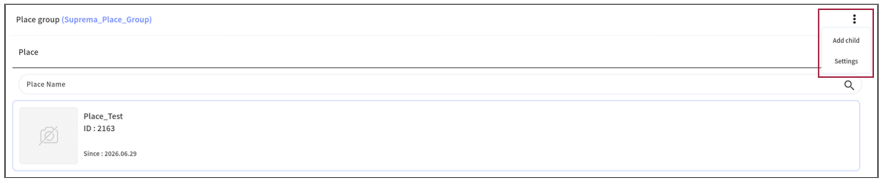
To sign up, get an invitation from a higher-level administrator or an administrator in the same place group.

What are Place and Place Group?

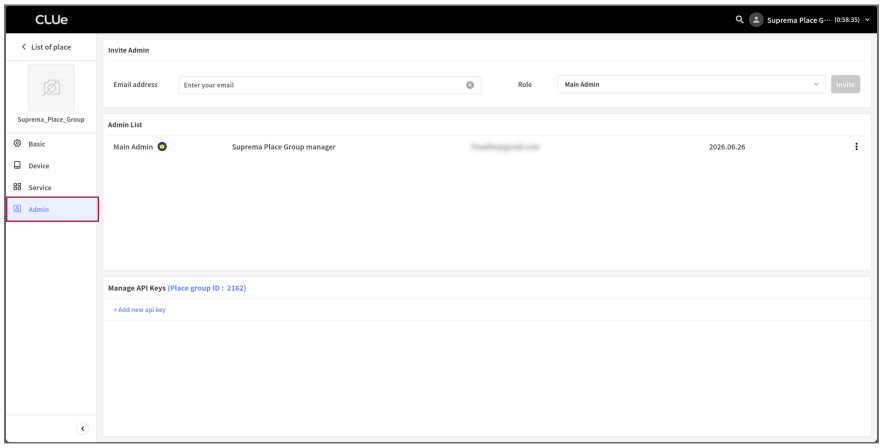
Because CLUe supports a multi-tenant system, a **Place** refers to an independent unit such as a company or Branch, and a **Place group** is a higher-level concept that manages multiple Places together.

Generate an API key

1. Log in to the CLUe web portal.
2. Select the place group for API integration.
3. Click ⋮ → **Settings** in the upper right of the screen.



4. Click **Admin** in the left sidebar.



5. In the **Manage API Keys** section, click **+ Add new api key**.
6. Select the desired validity period.



> If you select **Custom**, you can set the validity period for up to 365,000 days.

7. To issue a new API key, click the **Add** button.
8. When the new API key is created, click the **Copy** button and use it as a Bearer token when calling the CLUe API.



> **Caution**
> The API key grants access to the CLUe API, so keep it secure and do not expose it externally. Suprema is not responsible for problems caused by misuse.

CLUe API basics

Base URL

The base URL for all API requests is `https://api.moon.supremainc.com/v1`. Send all API requests over HTTPS.

CLUe API follows RESTful principles as much as possible and performs most operations on pages and database resources with `GET`, `POST`, `PATCH`, and `DELETE` requests. The request body and response body are both encoded in JSON.

API success response

When the response succeeds, the following status is returned.

HTTP status code: `200`

Field	Description	Optional
code	API response code	
status	API response status	
message	API response message	true
data	API response data	true

API failure response

When the response fails, one of the following statuses is returned.

HTTP status code: 400 / 500

Field	Description	Optional
errors	API failure response	
errors.code	Failure error code	
errors.message	Failure reference message	
errors.details	Failure details	true

Common error codes

Code	Description
e1000	Internal server error
e1001	Permission denied
e1002	Not supported
e1003	Invalid format
e1004	JSON parse error
e1005	Invalid method argument
e1006	Bad request
e1007	Resource not found

Code	Description
e1008	Method argument type mismatch
e1009	Missing request header

API rate limits

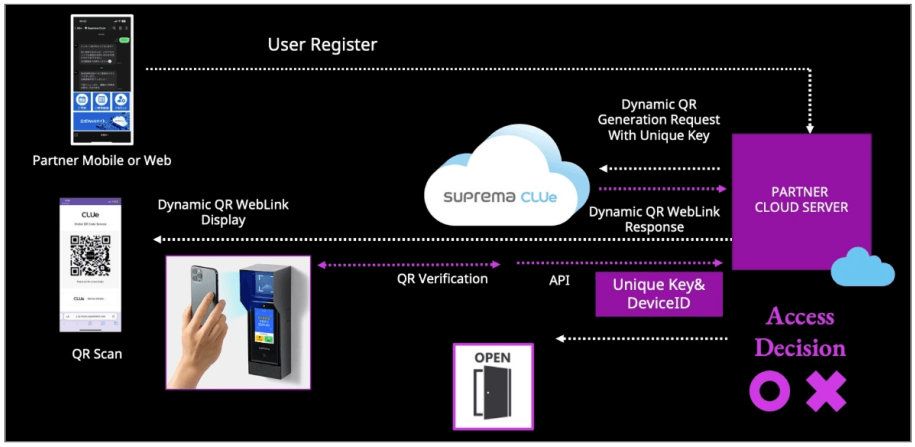
> **Caution**
> CLUe limits each API to 300 calls per 5 minutes, and this limit applies per call source. However, APIs that add facial images include processing tasks such as template extraction and generation, so we recommend waiting a short time between calls.

Integrate Dynamic QR Code

CLUe Dynamic QR is an integrated QR solution that supports the entire process from generation to verification. This guide targets developers who want to integrate CLUe Dynamic QR Code with their own systems and explains the steps from issuing an API key to setting up the service.

What is CLUe Dynamic QR Code

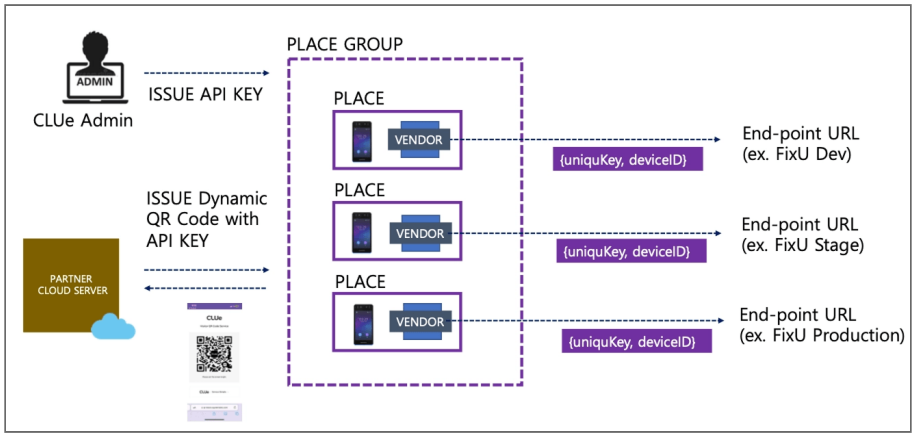
CLUe Dynamic QR Code is an integrated solution that supports the entire process from generation to verification. It is designed so customers can easily integrate QR Code features into their own systems without developing them from scratch.



> **Info**
> CLUe Dynamic QR Code can be used with the **customer verification** (**Vendor**) service method. For more information about the **customer verification** setting, see Service Settings.

Before you start

CLUe Dynamic QR Code is intended for integration, so it requires a Place group API key and a vendor code for testing.



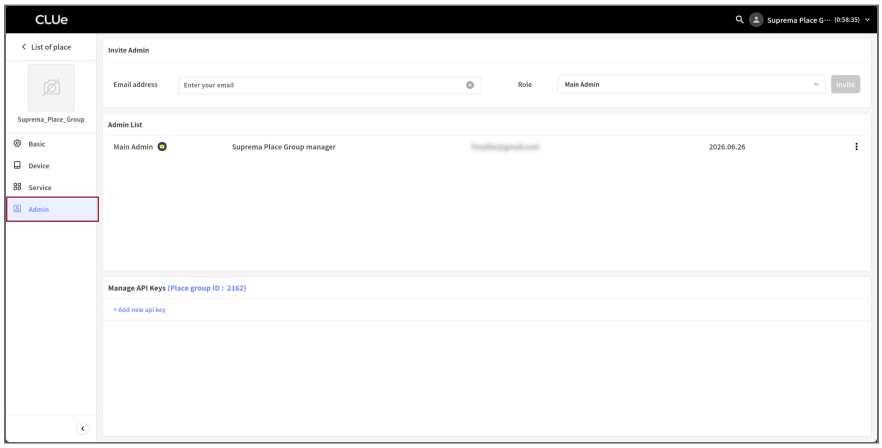
Generate an API key

1. Log in to the CLUe web portal.

2. Select the place group for API integration.
3. Click ⋮ → **Settings** in the upper right of the screen.



4. Click **Admin** in the left sidebar.



5. In the **Manage API Keys** section, click **+ Add new api key**.
6. Select the desired validity period.



> If you select **Custom**, you can set the validity period for up to 365,000 days.

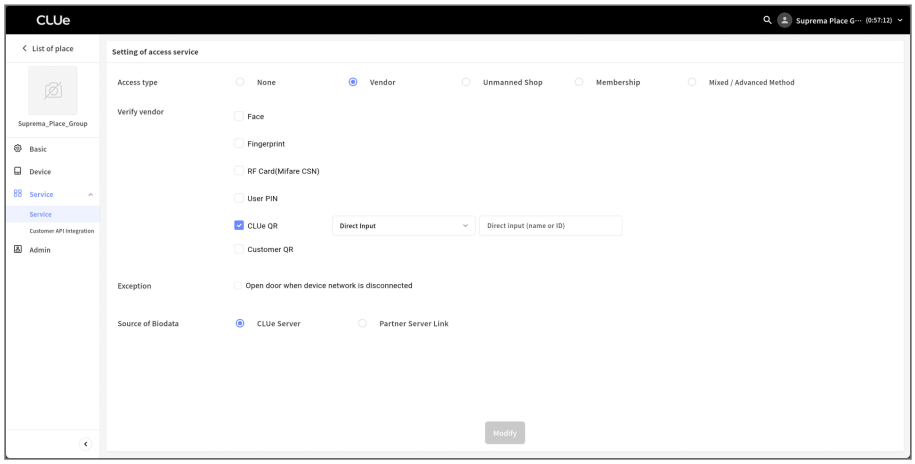
7. To issue a new API key, click the **Add** button.
8. When the new API key is created, click the **Copy** button and use it as a Bearer token when calling the CLUe API.



> **Caution**
>
> The API key grants access to the CLUe API, so keep it secure and do not expose it externally. Suprema is not responsible for problems caused by misuse.

Service Settings

Set **Access type** to **Vendor** in the Place group **Service**, then select **CLUe QR**.



The customer verification code must be issued by the Suprema CLUe team and configured according to the QR integration procedure.

> Can I test without a customer verification code?
>
> Yes. However, set a **test customer verification code** in the system. Contact your Suprema representative and request support. The test customer verification code allows access without verifying access rights or validity period.

Next step

See more details about using the Dynamic CLUe QR API.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

For more information about Suprema's global branch offices,
visit the webpage below by scanning the QR code.
https://supremainc.com/en/about/global-office.asp

© 2026 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc.
All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies.
Product appearance, build status and/or specifications are subject to change without notice.