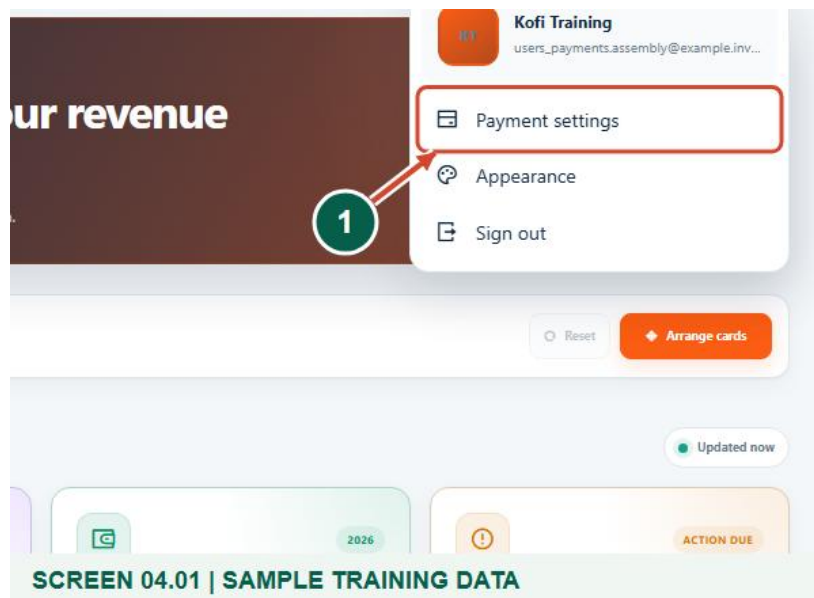


Configure assembly payment options

Configure the assembly merchant account for one supported payment gateway, distinguish sandbox from live settings, understand readiness validation and safely preserve or pause payment collection.

WHO THIS IS FOR	ALLOW ABOUT	DOCUMENT VERSION
Assembly administrators	15-25 minutes	1.0 19 October 2026



Illustrated steps with numbered arrows and clear expected results.

About the examples

Screens show the actual application in a training environment with sample data. Use your own verified account, assigned records and contact details when following the guide.

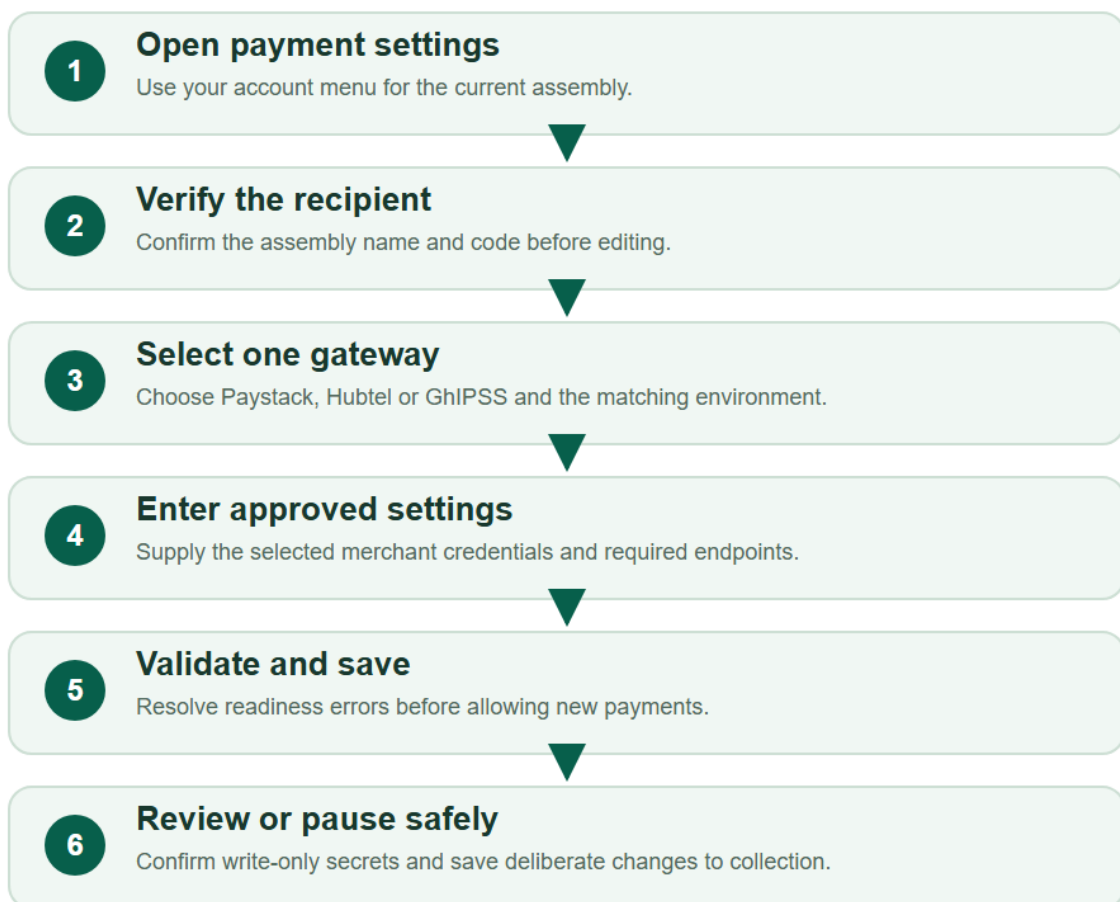
Website: assembly.gyentoboa.com

Process flow

Follow the arrows from start to finish. Optional routes are explained in the numbered steps.

Before you start

- Use an active Assembly Administrator account for your own assembly with assembly settings permission. A Super Administrator can manage a selected assembly; ordinary staff cannot configure merchant credentials.
- Obtain approved merchant credentials from the assembly authorised finance/payment administrator. Confirm which merchant account receives this assembly's funds.
- Choose Paystack, Hubtel or GhIPSS. Prepare the correct environment and provider-approved endpoints; GhIPSS requires the sponsoring bank certified integration. Never paste live secrets into a training guide or message.

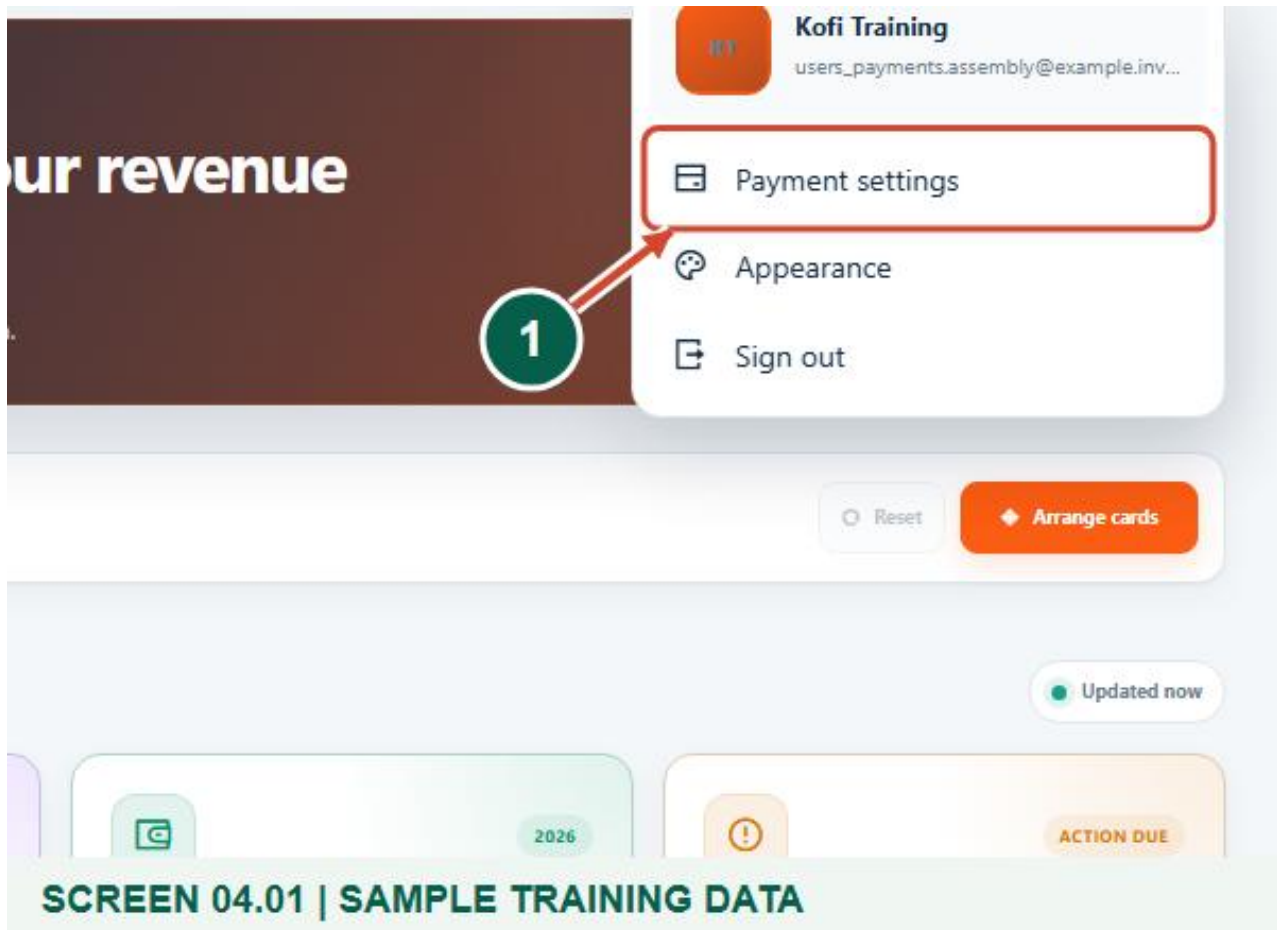


Numbered markers on screenshots identify the controls described beneath each image.

STEP 01

Open your assembly Payment settings

1. Open your account menu in the top-right corner and choose Payment settings.
2. If the link is unavailable, confirm you have the authorised administrator role and the correct assembly context.



Synthetic training data. Open your assembly Payment settings.

1 Payment settings

What should happen

The dedicated assembly payment settings page opens.

STEP 02

Confirm the assembly and single-gateway rule

1. Read the assembly name and code. These settings determine the merchant account used for this assembly's new bill payments.
2. Choose only one gateway. Accept new payments controls new online payment starts; existing requests keep their original merchant account when settings change.

ASSEMBLY PAYMENT SETTINGS

Training Municipal Assembly

Choose the account that receives this assembly's bill payments. Each assembly uses its own merchant credentials and one active gateway.

1

Online payments

Existing payment requests keep their original merchant account when you switch or update credentials.

SCREEN 04.02 | SAMPLE TRAINING DATA

Synthetic training data. Confirm the assembly and single-gateway rule.

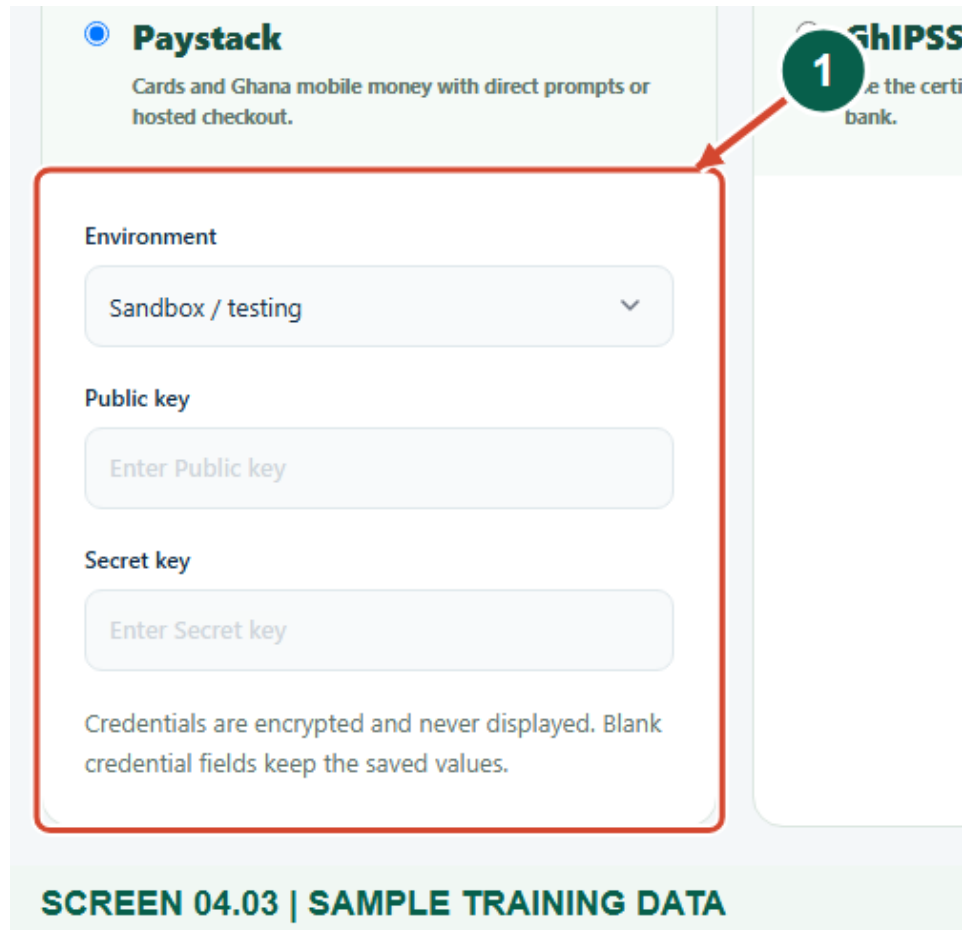
1 Receiving assembly**What should happen**

You have verified the receiving assembly and understand that only one saved gateway is active for new payments.

STEP 03

Configure the selected Paystack environment

1. Select Paystack and choose Sandbox / testing or Live settlement to match the approved merchant account.
2. Enter that assembly Public key and Secret key. Test keys must match sandbox, and live keys must match live. Keep the entries masked and use real authorised values only in the live service.



Paystack
Cards and Ghana mobile money with direct prompts or hosted checkout.

Environment
Sandbox / testing

Public key
Enter Public key

Secret key
Enter Secret key

Credentials are encrypted and never displayed. Blank credential fields keep the saved values.

SCREEN 04.03 | SAMPLE TRAINING DATA

Synthetic training data. Configure the selected Paystack environment.

1 Assembly Paystack keys

What should happen

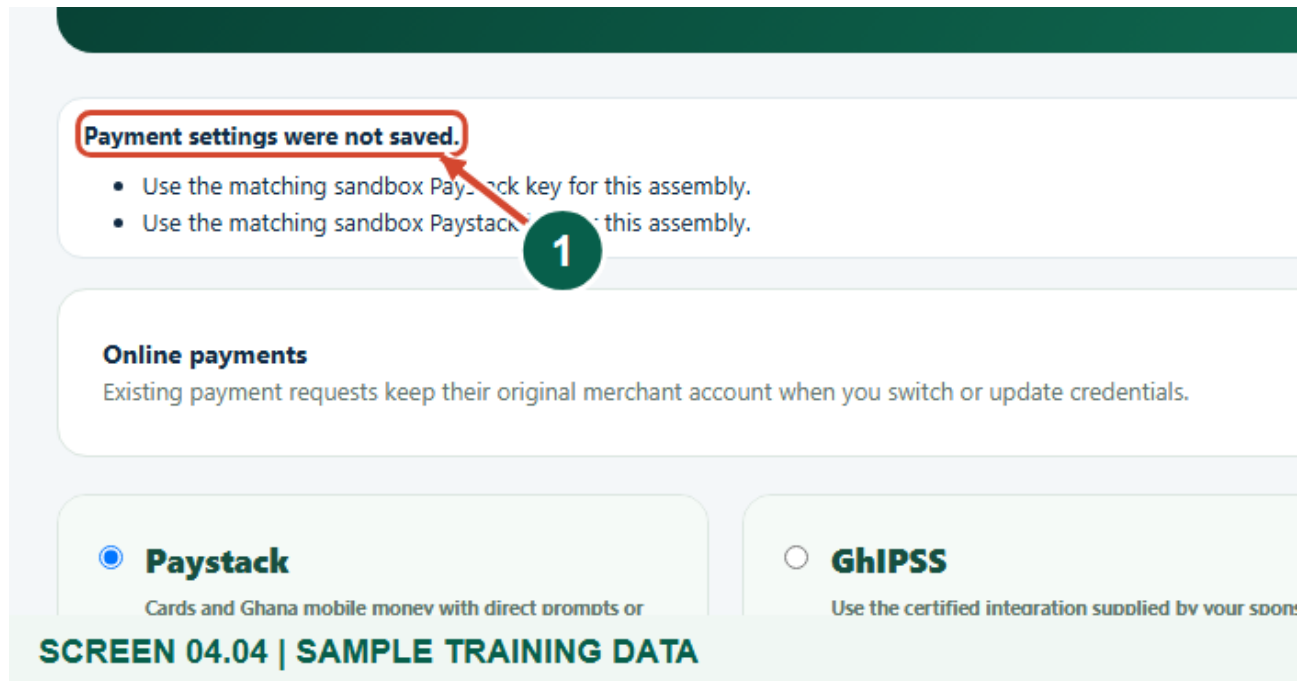
The selected gateway has matching environment credentials ready for validation.

Helpful note: The guide uses a synthetic sandbox configuration. It does not demonstrate a live merchant connection or a real payment.

STEP 04

Resolve readiness errors before enabling collection

1. When you are ready to accept new payments, turn on Accept new payments and choose Save payment settings.
2. If Payment settings were not saved appears, read each error and correct the selected gateway configuration. Incomplete credentials cannot be enabled.



Synthetic training data. Resolve readiness errors before enabling collection.

1 Settings were not saved

What should happen

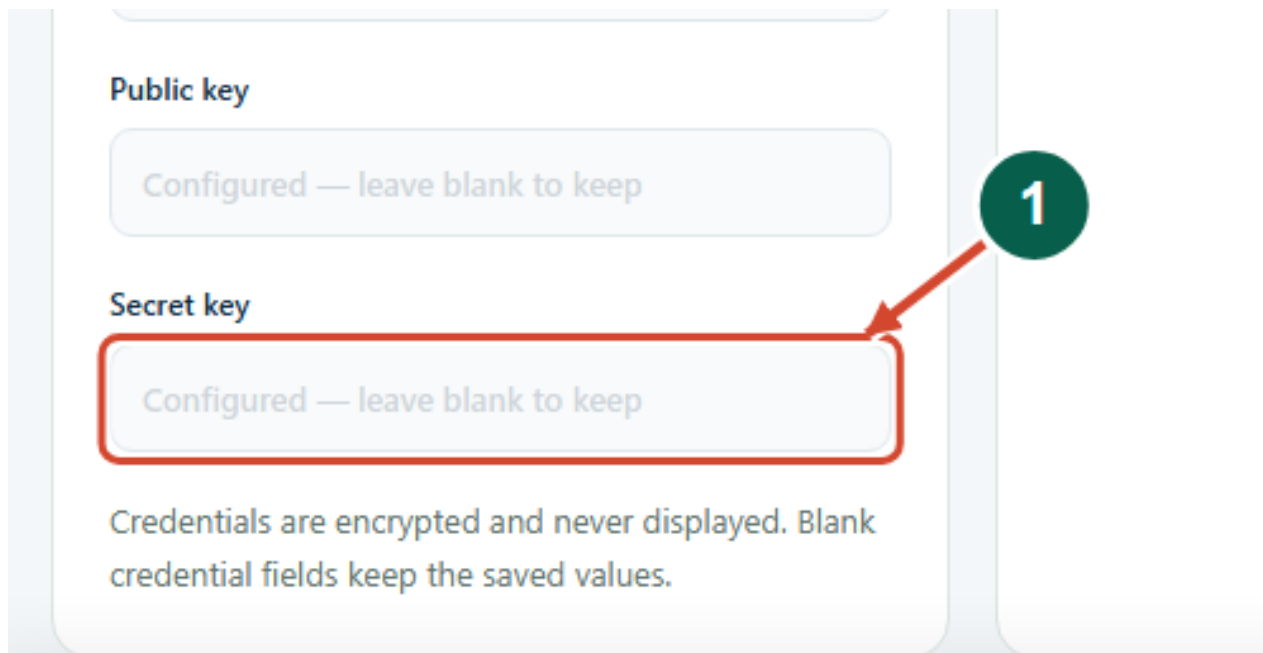
A rejected save leaves the previous saved payment configuration in force.

Helpful note: This deliberate training attempt shows validation with missing keys. Saving settings is not proof of provider onboarding, endpoint reachability or successful settlement.

STEP 05

Confirm the saved gateway and protect stored secrets

1. After a valid save, read the success message and confirm the intended selected gateway and Accept new payments state.
2. Saved credentials remain blank with Configured - leave blank to keep placeholders. Leave them blank to preserve existing values; enter a replacement only for an approved credential change.



Public key

Configured — leave blank to keep

Secret key

Configured — leave blank to keep

Credentials are encrypted and never displayed. Blank credential fields keep the saved values.

© 2026 Gye Ntobia

Powered by Melchia

SCREEN 04.05 | SAMPLE TRAINING DATA

Synthetic training data. Confirm the saved gateway and protect stored secrets.

- 1 Configured keys stay blank

What should happen

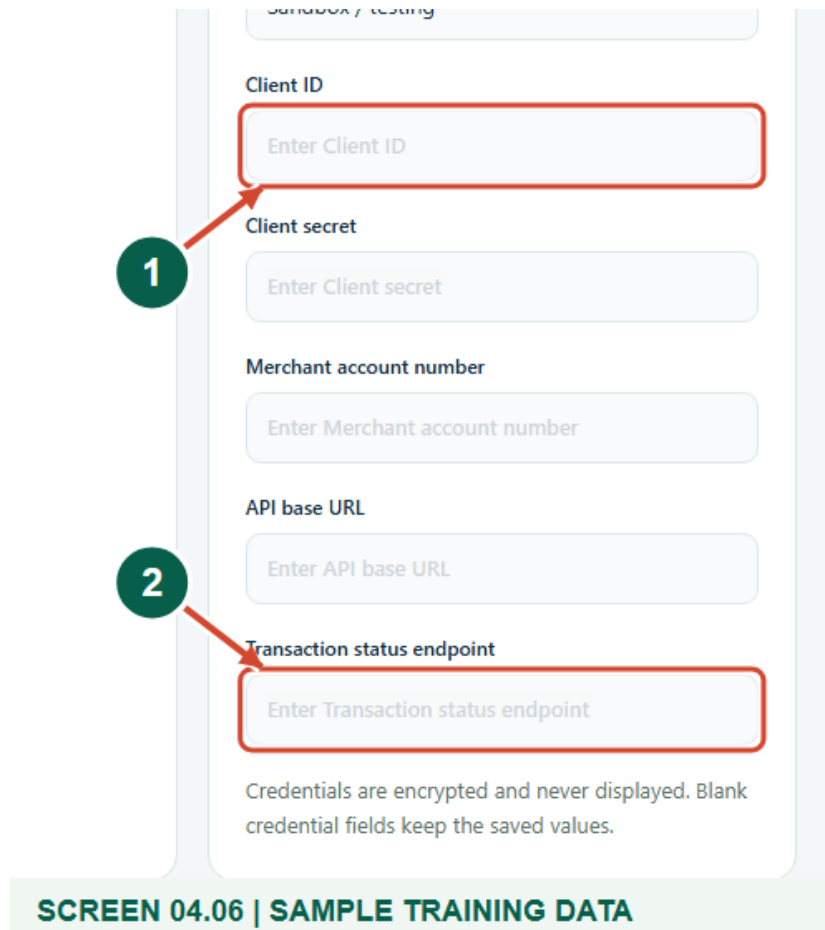
The selected gateway is saved for new payments without displaying stored credentials.

Helpful note: Inactive gateway credentials remain stored for reconciliation. Existing payment requests retain their original provider and merchant settings when you switch or rotate credentials.

STEP 06

Use the Hubtel alternative only with approved merchant details

1. To configure Hubtel, select its radio card and choose the correct Environment. Enter Client ID, Client secret and Merchant account number.
2. Enter the required Transaction status endpoint and, if supplied, API base URL. Use official Hubtel public HTTPS endpoints supplied for the merchant, then save only when the intended switch is approved.



The screenshot shows a configuration form for Hubtel. It includes fields for Client ID, Client secret, Merchant account number, API base URL, and Transaction status endpoint. Two red circles with numbers 1 and 2 are placed to the left of the form. Red arrows point from circle 1 to the Client ID field and from circle 2 to the Transaction status endpoint field. The fields are labeled 'Enter Client ID', 'Enter Client secret', 'Enter Merchant account number', 'Enter API base URL', and 'Enter Transaction status endpoint'. Below the fields, a note states: 'Credentials are encrypted and never displayed. Blank credential fields keep the saved values.'

SCREEN 04.06 | SAMPLE TRAINING DATA

Synthetic training data. Use the Hubtel alternative only with approved merchant details.

- 1 Client ID
- 2 Transaction status endpoint

What should happen

Only the Hubtel fields are editable while its radio card is selected.

Helpful note: This screenshot reviews an unsaved alternative. Selecting a radio alone does not change the saved gateway; you must deliberately save a valid configuration.

STEP 07

Use the sponsoring bank GhIPSS integration details

1. For GhIPSS, enter the sponsoring bank approved Merchant / biller ID, Client ID and Client secret in the matching Environment.
2. Use the bank-approved Certified initiation endpoint and Certified status endpoint, both public HTTPS addresses. Save only after the assembly's authorised provider setup is ready.

Client ID

Enter Client ID

Client secret

Enter Client secret

Certified initiation endpoint

Enter Certified initiation endpoint

Certified status endpoint

Enter Certified status endpoint

Use the merchant credentials and HTTPS endpoints approved by your sponsoring bank.

SCREEN 04.07 | SAMPLE TRAINING DATA

Synthetic training data. Use the sponsoring bank GhIPSS integration details.

- 1 Client ID
- 2 Certified status endpoint

What should happen

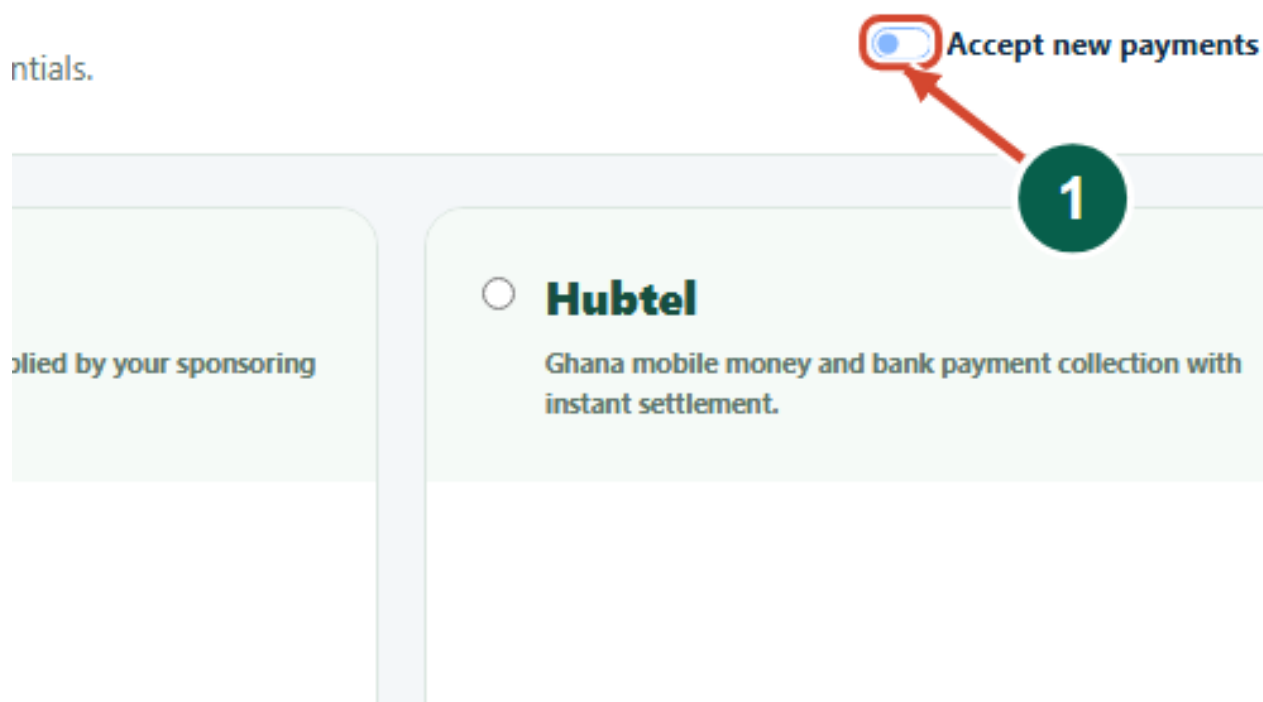
The GhIPSS card identifies the credentials and certified endpoints required by the sponsoring institution.

Helpful note: The application does not provide a universal GhIPSS merchant contract or certify a bank integration. This figure shows an unsaved configuration panel, not a live certified connection.

STEP 08

Pause new online payments deliberately

1. To pause new payment starts, keep the intended supported gateway selected and turn off Accept new payments.
2. Choose Save payment settings and verify the saved off state. Do not clear credentials merely to pause collection; blank credential fields preserve the stored values.



SCREEN 04.08 | SAMPLE TRAINING DATA

Synthetic training data. Pause new online payments deliberately.

- 1 Accept new payments is off

What should happen

New online payment starts are disabled while saved merchant settings and existing request associations are preserved.

Helpful note: Coordinate payment changes with the finance team. Pausing new starts does not cancel, refund or reassign an existing payment request.

Check your result

- The assembly identity, selected single gateway and sandbox/live environment are correct.
- The intended new-payment state was saved without exposing merchant secrets.
- You understand that gateway previews are unsaved until submitted, and existing requests retain their original merchant association.

If you need help

Payment settings is forbidden or missing

Use an active authorised Assembly Administrator account for that assembly, or ask a Super Administrator to open the selected assembly context. Confirm assembly update permission.

An enabled save rejects missing credentials or environment

Fill the selected gateway required values and choose the correct environment. For Paystack, use matching test or live keys. Leave collection off while preparing an incomplete draft.

An endpoint is rejected

Use the provider-approved public HTTPS address without embedded credentials, query strings or fragments. Hubtel activation requires an official Hubtel host; ask the provider or bank instead of weakening the address rules.

A gateway change reports unresolved historical payments

Stop and ask the authorised finance or technical administrator to review the original merchant context. Do not remove payment history or force a new account onto an old request.

Saved settings do not result in a confirmed payment

Check merchant onboarding and the provider/bank integration through the authorised support process. Settings validation alone is not settlement confirmation; never mark a bill paid because a form save succeeded.

Useful things to know

- All payment credentials in this training were synthetic, masked and confined to the isolated training database. No live provider request or money movement occurred.
- Exactly one of Paystack, Hubtel or GhIPSS can be activated for new payments. Previously saved inactive credentials may remain available for historical reconciliation.
- Provider onboarding, merchant settlement arrangements, bank certification, refunds and payment reconciliation are outside this configuration guide.
- A sandbox setting identifies the configured environment; it does not by itself prove that the external provider endpoint is a sandbox or that a merchant account is live.

Continue learning

- Guide 01: Access your assembly administrator account

[Download all 13 guides in this collection](#)

For account or bill-record corrections, contact the relevant assembly using its verified contact details. Keep your account or bill reference available when requesting assistance.