

DUALSCAN LLC

VisaUSD PoS Administrator Setup Manual



A practical guide for the administrator responsible for a customer-facing USDC checkout terminal and a separate merchant receiving wallet.

Configure the Gate, protect administrator access, fund network gas, accept payments, reconcile transfers and handle mistaken SOL or POL receipts.

Manual edition	Application baseline	Issued
1.0	1.0.2 • Android build 3	October 21 2026

VisaUSD™ and VisaUSD PoS™ are trademarks of Dualscan LLC.

© 2026 Dualscan LLC. Intellectual property disclosure appears on the final page.

Training screenshots contain example addresses and codes. Use the address shown by your own installed terminal, never a code printed in this manual.

START HERE

Using this manual

Follow pages 3-11 to commission a terminal, pages 12-13 for checkout, and pages 14-22 for fees, safeguards and support. The final pages cover continuity, exact network identifiers, a go-live checklist and intellectual property.

- 03 Understand the Gate and vault
- 04 Prepare and install the terminal
- 05 Create the local Gate
- 06 Protect administrator access
- 07 Configure both payment networks
- 08 Save settings and enable forwarding
- 09 Add SOL through the admin window
- 10 Add POL through the admin window
- 11 Read the three green indicators
- 12 Recognize the customer checkout
- 13 Run a checkout transaction
- 14 USDC fees and settlement examples
- 15 Mistaken SOL and POL payment fees
- 16 Know the automatic handling limits
- 17 Manage the gas reserve and refill
- 18 Use history and reconcile the vault
- 19 Customize the customer display
- 20 Configure an RPC override
- 21 Resolve payment and refund issues
- 22 Resolve access and operating issues
- 23 Close a shift and transfer responsibility
- 24 Network identifiers and references
- 25 Administrator go live checklist
- 26 Intellectual property disclosure

Scope and operating baseline

This edition describes VisaUSD PoS™ app 1.0.2. The Android launcher currently displays VisaUSD™ PoS. The app accepts supported mainnet USDC on Solana or Polygon; it is a locally operated Gate rather than an always-running background forwarding service.

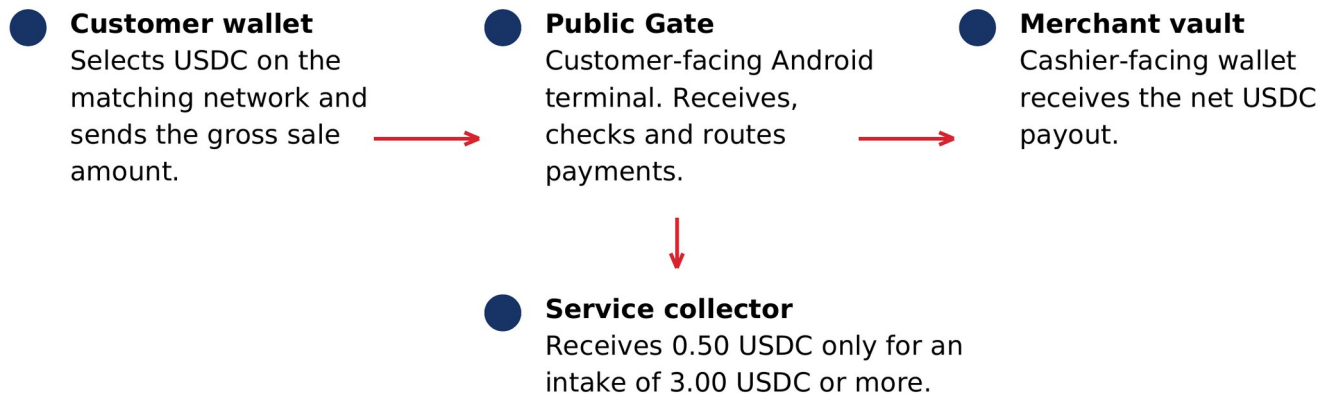
Release validation includes 421 JavaScript tests, 108 Android unit tests, 23 fresh-setup checks and 27 installed deposit-window checks. Funded end-to-end forwarding and refunds, and physical-device biometric acceptance, were not performed in that release evidence. Complete controlled funded acceptance on the actual store installation before live use.

Numbered arrows identify controls. Example codes are visibly marked to discourage accidental payment. The green-completion screenshot is a labelled interface illustration, not evidence of a real deposit.

SYSTEM OVERVIEW

Understand the Gate and vault

The customer pays the Gate address displayed on the Android terminal. The app verifies the intake and forwards the net USDC to the merchant's independently controlled vault. Only the vault's public address is entered into this app; its private key or recovery phrase is never requested.



Payment path. The separate merchant vault keeps its own signing credentials.

Mode	Payment asset	Gas coin	Customer code
VisaUSD on Solana	Canonical Solana USDC	SOL	Live Data Matrix plus small standard address QR
USDC on Polygon	Native Polygon PoS USDC	POL	Standard Gate-address QR

Both enabled networks can process independently while the app is open and unlocked. Switching the displayed code does not pause the other side. Gas, destination, enable state, history and RPC endpoint are separate for each side; appearance preferences are shared.

The vault is absent from the public payment code, but the Gate-to-vault forwarding link is visible on-chain. This is not an anonymous transfer arrangement.

COMMISSIONING

Prepare and install the terminal

1. Assign a store administrator and prepare the separate receiving vault on each network you will accept. Verify the public receiving addresses directly on that wallet.
2. Use a compatible Android device with reliable power, internet access and an Android screen lock. This build targets Android SDK 36 and has a minimum Android API level of 28; compatibility alone is not store acceptance testing.
3. Obtain the signed release APK from the authorized private GitHub release. Sign in to an account with repository access. Do not use the debug APK for the store terminal.
4. Verify version 1.0.2, build 3 and package com.dualscan.guard. If your process checks hashes, compare the APK with SHA256SUMS from the same release.
5. Install through Android's approved package-install flow. If Android asks, grant installation permission only to your chosen installer and remove that permission afterward. Device-management policy may govern this step.
6. For an update, install over the existing app using the compatible signed release. Preserve app data. Do not uninstall, clear storage or attempt a new Gate while transfers are unresolved.

Prepare the operating record

- Record the store, terminal name, administrator, app version and both public Gate/vault addresses after configuration.
- Keep the app PIN available through an authorized store process. It is not the Android device-unlock PIN.
- An APK or source backup is not a wallet backup. This app disables Android app-data backup and provides no phrase export/import or forgotten-PIN recovery.

Authorized distribution Release download

[VisaUSD PoS 1.0.2 private release](#)

INITIAL SETUP

Create the local Gate

Start with the intended payment network and the merchant vault's public address. The address field must pass the format check before the app PIN step. Solana preserves Base58 capitalization; Polygon requires a complete 0x address and valid mixed-case checksum when mixed case is used.

7:48

YOUR WALLET
Set up PoS gate

Choose the guarded destination, then create your administrator PIN.

Payment network
VisaUSD - USDC on Solana

Guarded destination
YOUR OWN VAULT ADDRESS

Address format checked.
Set the destination before choosing your 4-digit administrator PIN. Later changes require PIN or biometrics.

Create wallet

1 Select the network

VisaUSD / USDC on Solana is the first-start default. Polygon is a separate side.

2 Enter your own vault

Use the merchant receiving address. Never copy the address printed in a training screenshot.

3 Check the format result

Address format checked means valid syntax. It does not prove ownership or the intended network.

4 Create the Gate and PIN

Continue to the four-digit app PIN and confirmation. No recovery words are displayed.

Initial setup. The training address is masked; enter your own merchant vault address.

1. Choose Payment network, enter Guarded destination and wait for Address format checked.
2. Use the create button to continue. Enter a four-digit app PIN, continue, then enter the same PIN again to confirm.
3. The Gate signing secret is generated locally and encrypted. No recovery words appear. Record the public Gate address afterward; do not confuse it with the vault.

The format check does not establish ownership, correct recipient intent or funds. Compare the full destination with the separate receiving wallet before enabling forwarding.

SECURITY

Protect administrator access

An unlocked customer checkout is not permission to browse administrator controls. The tray, Guard settings, Guard History, guarded-address details and deposit window each require fresh authorization. Destination changes and Enable forwarding can request authorization again.

Access or action	Expected behavior
Tray, Guard, history or address details	Fresh app PIN or eligible enrolled Android biometric
Open deposit window	Additional fresh authorization before its funding QR appears
Cancel, wrong PIN or failed biometric	Requested private surface stays closed
Manual Lock	Ends the unlocked checkout and stops new signing
Background the app	Pauses processing and closes admin surfaces; returning may resume if still unlocked

Enable biometrics

1. Enroll eligible strong biometrics in Android under the store's device policy.
2. Open the authenticated tray, find Wallet security and turn on Biometric unlock. Complete the existing app PIN and Android biometric prompts.
3. Test on the actual device. Not every face-unlock implementation meets Android's strong-biometric requirement. The existing app PIN remains the alternate factor.

Changing the app PIN clears its biometric wrapper. Adding or changing Android biometric enrollments can invalidate it. Keep the current app PIN and re-enable biometrics in the app afterward.

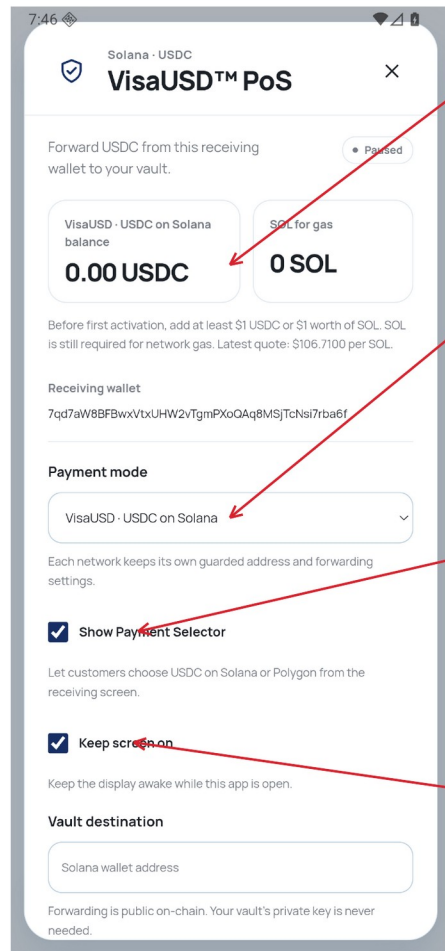
Plan for lost access

There is no in-app PIN recovery or phrase-based reset. If both the PIN and usable biometric access are lost, the app cannot recover the current Gate. Provision a fresh Gate and replace displayed payment identifiers. Funds already in the separate vault remain controlled there; remaining Gate balances may become inaccessible.

FORWARDING SETTINGS

Configure both payment networks

Tap Guard and authenticate. Confirm the payment mode and the matching vault. Configure and fund each side separately before enabling it. A saved selection is retained across launches.



1 Balances and reserve

USDC is the payment asset. SOL or POL pays network costs. Read the operational status separately.

2 Payment mode

Configure each side's vault, native gas and Enable state separately.

3 Show Payment Selector

Expose the two customer choices on the main screen. This preference is global.

4 Keep screen on

Leave on for checkout. Foreground display stays awake; Android timeout returns in the background.

Guard settings. These example balances are zero and forwarding is paused.

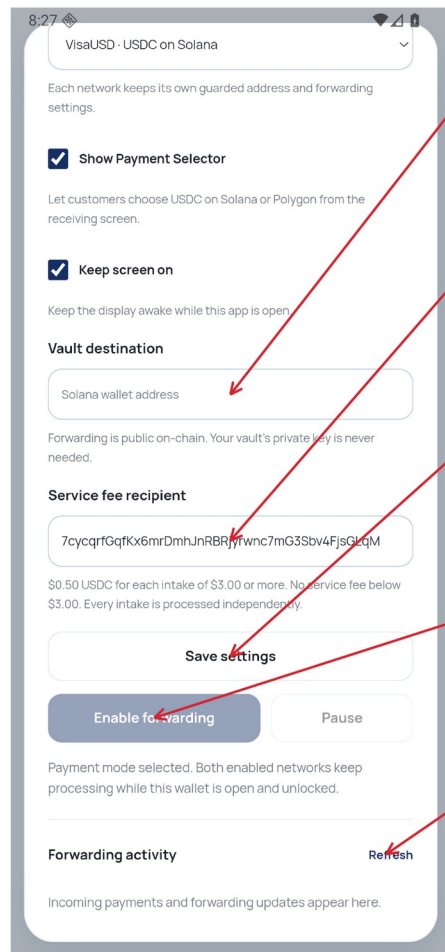
1. For the first side, check the vault, save any changed destination, complete its native gas deposit procedure, then enable forwarding after the reserve checks.
2. Change Payment mode to the other side and authorize the change. Scroll to Vault destination, enter that network's vault address, tap Save settings and authenticate. Fund its native gas and Enable forwarding separately.
3. Turn on Show Payment Selector if customers should choose their network. Leave Keep screen on enabled for attended checkout.

The selector is off by default, screen-awake is on by default, and first start selects VisaUSD / USDC on Solana. Changing a vault pauses that side until it is deliberately re-enabled.

FORWARDING CONTROLS

Save settings and enable forwarding

Scroll down inside Guard to the destination, fixed service collector and operational controls. Entering an address is not enough: save and authorize the new destination before attempting to enable this network.



1 Vault destination

Confirm the merchant's receiving wallet on this network. It is not the service collector.

2 Fixed service recipient

The network's collector is configured by the app. Fee addresses are listed in the reference section.

3 Save settings

A changed destination requires authorization and pauses that side. Re-enable after checks.

4 Enable or Pause

Enable authenticates and checks funding. Pause affects only the selected network.

5 Refresh and activity

Refresh asks for a new check. It does not bypass finalization, funding or an unresolved transaction.

Current lower settings. Disabled controls in the training image reflect an unfunded paused Gate.

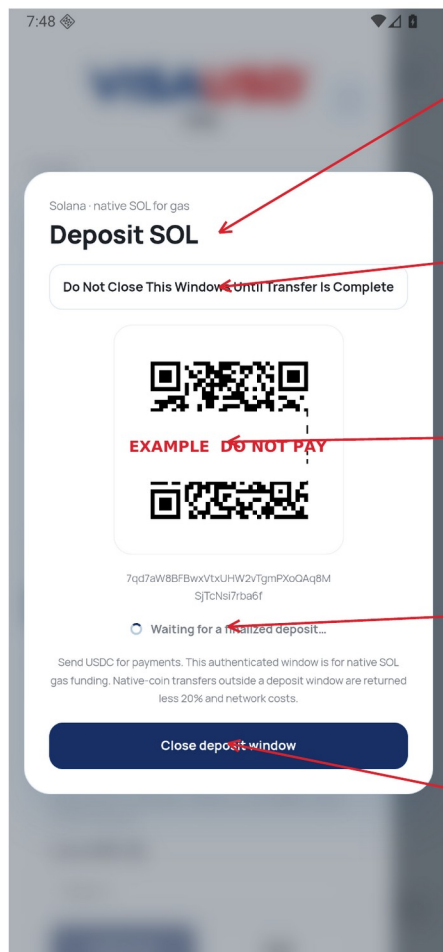
1. Verify Vault destination against the separate receiving wallet, then tap Save settings and authenticate. Changed destinations pause the side.
2. Complete the native gas funding window procedure, close that window and confirm sufficient available reserve.
3. Tap Enable forwarding and authenticate. Confirm the operational result. Use Pause for this side only, or manual Lock to end the unlocked session on both sides.

Refresh requests current information without bypassing checks. Keep a pending signed payment's existing state intact; do not clear data to force a new transaction.

NETWORK GAS FUNDING

Add SOL through the admin window

Take the terminal out of customer service while funding. Select Solana, open the administrator tray and tap Open deposit window. Authenticate again and wait for the live funding QR. Sending SOL to the normal checkout QR outside this window can trigger the mistaken-payment refund fee.



1 Match network and coin

This window is for native SOL gas funding. Verify the chain in your funding wallet.

2 Keep the window open

The required notice stays visible until the operator closes the window.

3 Use the live device QR

Wait until this QR appears after authentication. The manual's training code must not be paid.

4 Wait for finalization

Waiting is not completion. Green Deposit complete appears only after a finalized native receipt.

5 Close explicitly afterward

Green does not close the exemption. Close the window and confirm Deposit window closed.

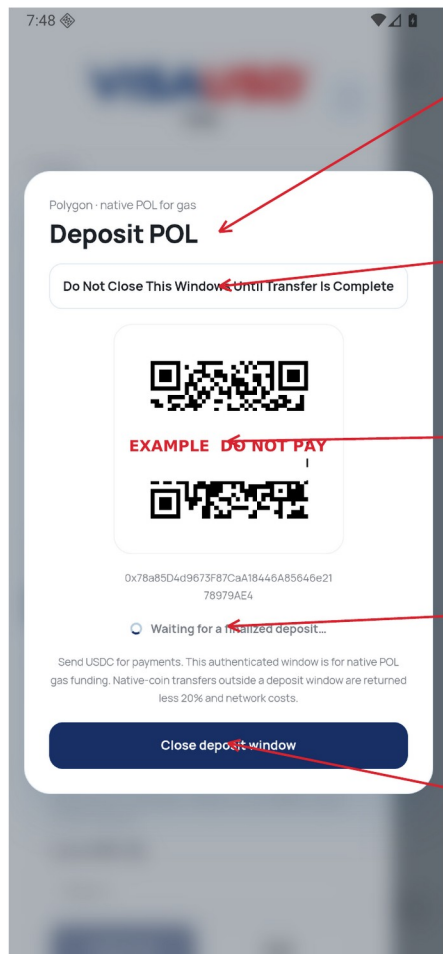
Actual unfunded Android deposit window. The marked training QR must not be paid.

1. From the funding wallet, send native SOL on Solana to the current device's Gate address. Fund at least the required \$1 value, and allow for actual network costs and possible USDC token-account rent.
2. Keep the app and this window open until the finalized-deposit indicator turns green and the received amount is shown.
3. Tap Close deposit window. Confirm Deposit window closed before presenting checkout to customers. Green alone does not close it.

NETWORK GAS FUNDING

Add POL through the admin window

Select USDC on Polygon, open the authenticated tray and start that side's deposit window. Confirm native POL on Polygon PoS in the sending wallet. A Solana balance cannot pay Polygon gas, and a Polygon balance cannot pay Solana gas.



- 1 Match network and coin**
This window is for native POL gas funding. Verify the chain in your funding wallet.
- 2 Keep the window open**
The required notice stays visible until the operator closes the window.
- 3 Use the live device QR**
Wait until this QR appears after authentication. The manual's training code must not be paid.
- 4 Wait for finalization**
Waiting is not completion. Green Deposit complete appears only after a finalized native receipt.
- 5 Close explicitly afterward**
Green does not close the exemption. Close the window and confirm Deposit window closed.

Actual unfunded Android POL deposit window. Use only the live device address.

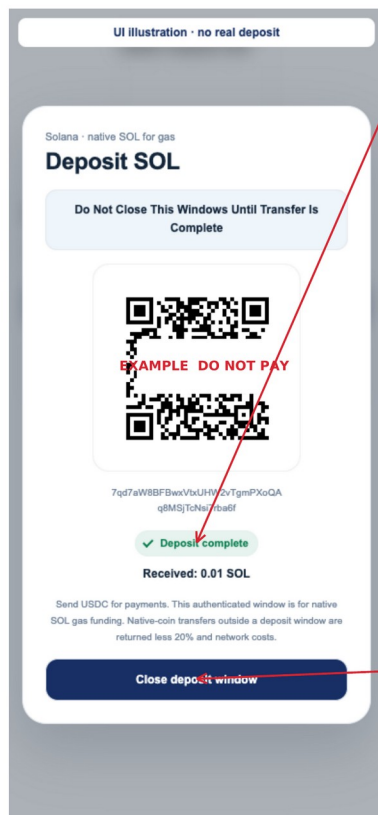
1. Send native POL to the device's current 0x Gate address only after the deposit window is ready.
2. Wait for finalization and green Deposit complete. Check the received amount against the funding or refill requirement.
3. Close the window explicitly and verify Deposit window closed. Configure or resume forwarding afterward.

Every sender's native payment received during that network's window is retained without the 20% fee. The app does not identify an administrator by sender address. Never leave the funding window open for normal public checkout.

STATUS INTERPRETATION

Read the three green indicators

Green indicator	What it means	What it does not mean
Guard shield	Fresh verified balance meets 1.00 USDC or \$1 native funding eligibility.	Forwarding is enabled, gas is sufficient, or a payout is complete.
Deposit complete	A finalized native receipt was observed in the funding window.	The received amount meets the \$1 minimum, or the window has closed.
RPC Available	The saved endpoint passed checks. Badge persists until Clear.	The provider is continuously healthy or currently online.



1

Green completion indicator

A finalized native receipt was recorded. This is not a guarantee that the \$1 reserve requirement is met.

2

Close before checkout

All native receipts are still retained until the window is closed. This screen is a labelled UI illustration.

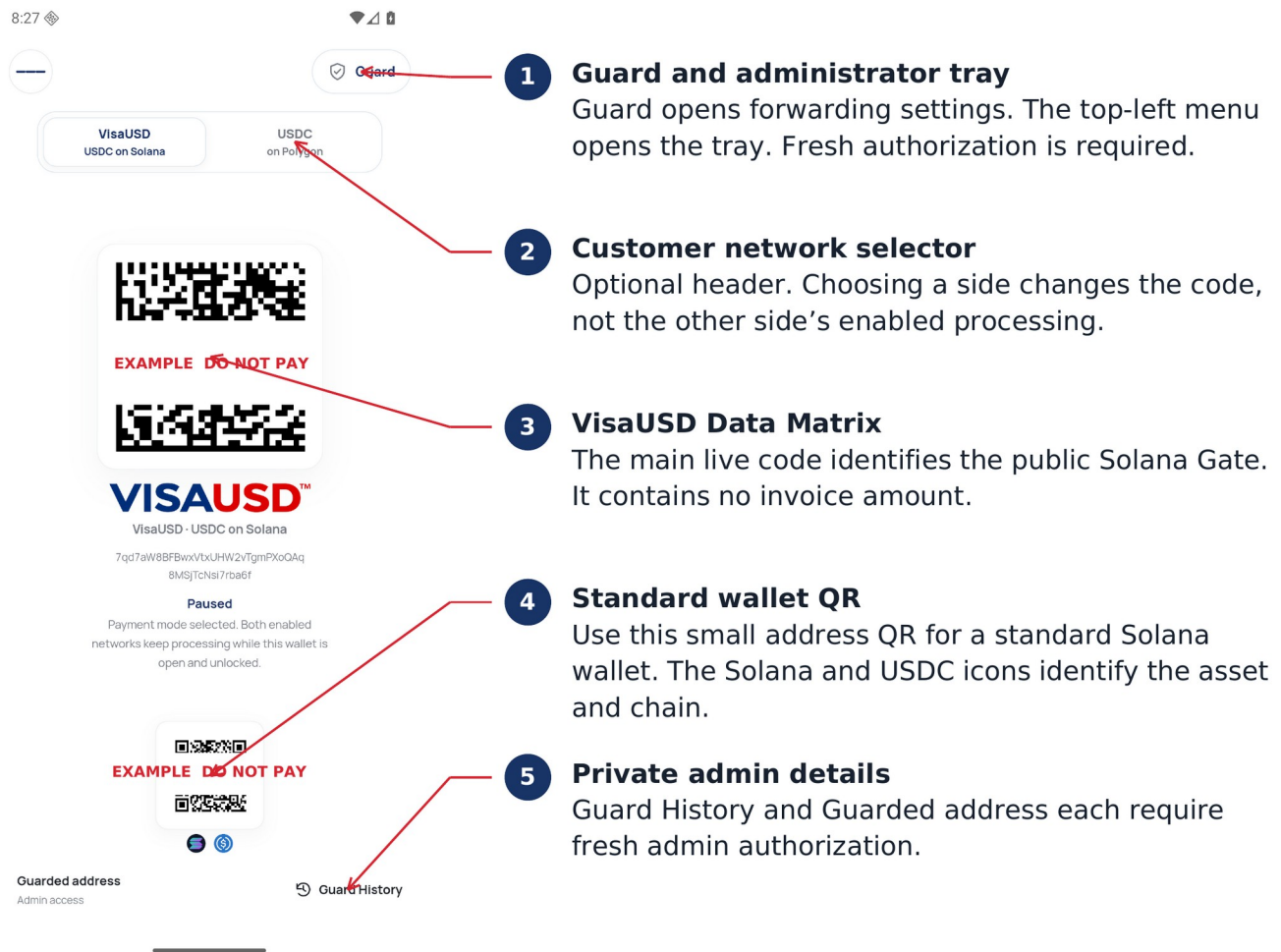
Green-completion illustration only. No real funded deposit was used for this image.

A small native receipt can produce Deposit complete while the Guard remains below the funding minimum. Conversely, 1.00 USDC can make the shield green while native gas is insufficient. Check the amount, operational status and Enable state independently.

CUSTOMER DISPLAY

Recognize the customer checkout

Before handing the terminal to a customer, verify the intended chain, the USDC asset label and an operational forwarding state. The screen shown here is a training example with paused forwarding.



Customer view with numbered pointers. Example codes do not request or prove payment.

The main VisaUSD Data Matrix rotates its OTP/frame; the small standard QR carries only the public Solana Gate address. Polygon shows a standard 0x address QR. A standard wallet must still choose USDC on the correct network, not SOL, POL, USDT, USDC.e or another chain.

No code in this release contains a sale amount. The customer enters the gross USDC amount in their own wallet. The app does not automatically add the 0.50 USDC fee to a retail invoice.

DAILY OPERATION

Run a checkout transaction

1. Keep the app foregrounded, unlocked and connected, with forwarding enabled on the accepted side. A green shield alone is insufficient.
2. State the exact accepted network and gross USDC amount. Explain any net settlement effect before the customer sends.
3. The customer selects USDC on the matching network, scans the appropriate live code and confirms the gross amount in their own wallet.
4. Wait for the intake and forwarding result. A customer's send screen or a visible receiving QR is not confirmation that the merchant vault received payment.
5. When needed, authenticate into Guard History and compare the selected-network record with the cashier-facing vault, net amount and transaction identifier.
6. Release the order under the store's settlement policy after the required confirmations. Do not ask for a second payment merely because an acknowledgement or RPC response is delayed.

While both sides are enabled

The customer selector changes only the displayed side. Both enabled sides continue processing while the app is foregrounded and unlocked. Pause affects the currently selected side.

Backgrounding or manually locking pauses both workers; returning can resume an already unlocked session.

Unattended display and Android pinning

Keep screen on prevents ordinary foreground display timeout. It does not provide a background service or prevent a manual lock. An enabled foreground checkout session stays unlocked; pausing both sides restores the inherited 15-minute inactivity lock.

Android app pinning can keep the terminal in this app. Enable it through the device's security settings, configure the Android unlock requirement, then pin the app from Overview. Names and paths vary by manufacturer. Pinning does not replace in-app administrator authentication. See reference R3.

FEE REFERENCE

USDC fees and settlement examples

The service fee is deducted from each individual received USDC intake. It is not automatically added on top. The same rule applies to both Solana USDC and native Polygon USDC. Separate intakes are never combined to cross the threshold.

USDC received	Service fee	Net USDC to vault
1.00	0.00	1.00
2.99	0.00	2.99
3.00	0.50	2.50
10.00	0.50	9.50
25.00	0.50	24.50
25.50	0.50	25.00
Two separate 2.00 intakes	0.00 on each	2.00 on each

Quote the amount the customer should send

If the intended merchant net is 25.00 USDC, a gross intake of 25.50 USDC produces that net under the current fee rule. At the threshold, 2.99 received nets 2.99, while 3.00 received nets 2.50. Decide the gross customer amount deliberately; this release has no automatic invoice gross-up.

Network costs are separate

The customer's wallet pays its own sending-network cost. Gate forwarding uses available SOL or POL, separately from the USDC service fee. Solana can additionally require native SOL for destination token-account creation. No automatic USDC-to-SOL/POL conversion occurs. Network costs vary; this manual does not quote a fixed gas price.

Solana combines the net payout, applicable service fee and memo in one atomic transaction. Polygon confirms the net payout before sending the service fee in a separate automated transaction. Polygon's two legs are not atomic.

CUSTOMER GUARDRAILS

Mistaken SOL and POL payment fees

USDC is the only pass-through payment asset. Outside a valid admin deposit window, a new eligible finalized direct native payment is handled as a mistaken asset. The native refund is a new on-chain return, not deletion of the original payment.

Allocation	Current rule
Percentage fee	20% of the native intake, rounded down to a whole lamport or wei; sent to the existing network service collector.
Customer return	Original native amount minus the percentage fee and required outgoing network costs.
Network denomination	SOL is refunded and charged in SOL; POL is refunded and charged in POL. The 20% fee is not a USDC charge.
Explanation	The return records USDC only. A wallet or explorer may display the note differently.

Illustrative calculations

SOL example: 0.010000000 SOL received; 0.002000000 SOL percentage fee; if the exact outgoing network fee is 0.000005000 SOL, the return is 0.007995000 SOL. This network fee is hypothetical, not a quotation.

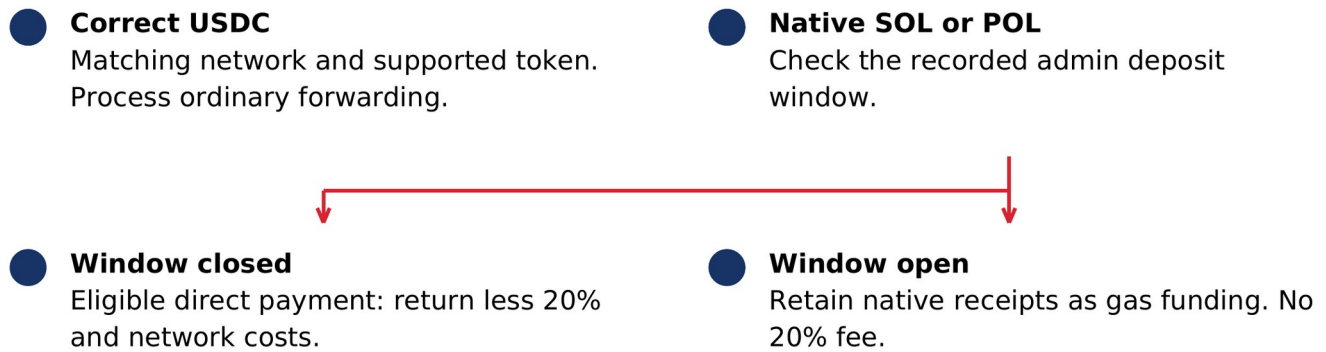
POL example: 1.000000 POL received; 0.200000 POL percentage fee; if the total required gas for both outgoing legs is 0.004000 POL, the return is 0.796000 POL. The actual gas allocation is checked by the app.

On Solana, native return and percentage fee are atomic. On Polygon, the refund confirms before the percentage-fee transaction is sent. Automation needs that network enabled and the app foregrounded and unlocked. Finalization, network availability and safeguard checks can delay it.

A refund cannot spend existing gas to make an uneconomic intake work. Too-small or ambiguous receipts are recorded and held. Do not promise an instant or unconditional 80% return.

CUSTOMER GUARDRAILS

Know the automatic handling limits



Asset handling. Admin funding is an explicit, network-specific exception for native coins.

Receipt or condition	Operator expectation
Supported USDC on correct network	Ordinary per-intake forwarding and flat-fee rules.
Verified direct native SOL/POL outside window	Return less 20% and network costs when eligible.
Native receipt while window is open or green complete	Retained as gas funding; no 20% fee. Close explicitly.
Detected interrupted or unverifiable funding interval	Held for review and excluded from spendable gas.
Detected unsupported Solana program credit or restricted POL sender	Automatic return is not assumed; held/review behavior applies.
Internal Polygon contract transfer	Direct full-block scanning may not detect or attribute it. Do not promise automatic detection, reservation or refund.
Wrong token, bridged USDC.e or wrong chain	Not supported pass-through. No general recovery or automatic return is promised.

A return goes to the verified on-chain sender. For an exchange or custodial sending wallet, that may be the provider's address rather than the customer's account. A successful return does not guarantee that the provider credits the individual customer.

FUNDING MAINTENANCE

Manage the gas reserve and refill

Threshold	Meaning and required action
First activation	At least 1.00 USDC or \$1 worth of the selected native coin meets eligibility. Actual native gas is still required.
After activation below \$0.10 native value	Forwarding pauses and records a refill baseline. Add at least another \$1 worth of native coin above that recorded balance.
USDC in the Gate	May satisfy initial eligibility but does not become gas. It cannot satisfy an existing native refill requirement.
Reserved mistaken-native obligations	Excluded from available gas. Do not treat the raw explorer balance as fully spendable.

Refill procedure

1. Pause customer service and select the network that requests a refill. Read the exact native amount and recorded requirement shown by Guard.
2. Use Open deposit window and wait for readiness before sending native SOL/POL. Send at least the displayed minimum; the app does not convert a dollar amount automatically.
3. Wait for finalized completion, verify the received amount and close the window. Refresh Guard and confirm the refill requirement is cleared before returning to service.

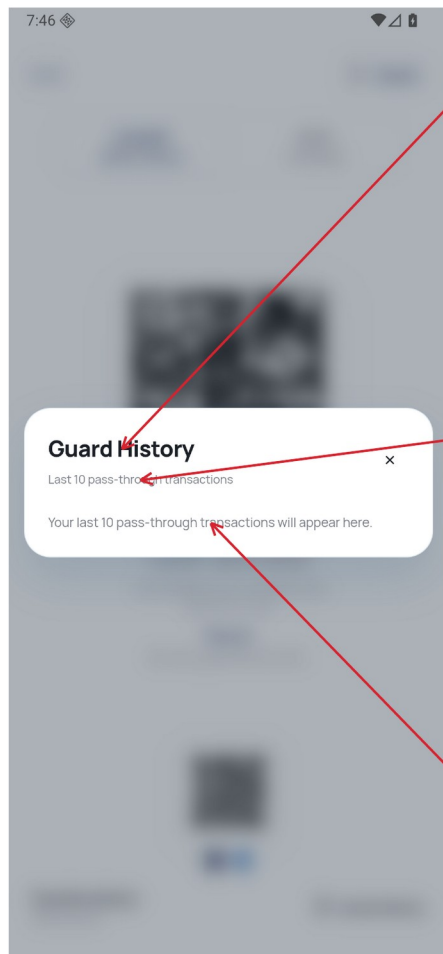
Example: if the saved requirement is an additional 1.00 unit above a 0.05-unit baseline, a total of 1.00 unit does not satisfy it; a total of at least 1.05 is required. This is an arithmetic example, not a SOL/POL market-price assumption.

Native price quotes can fail or expire, pausing checks that depend on them. More gas than the required minimum can be retained through an admin window. USDC sent during the window still follows ordinary forwarding; the window does not hold USDC as gas.

RECONCILIATION

Use history and reconcile the vault

Select the relevant network, tap Guard History and authenticate. The app shows the latest ten selected-network records, including native handling. The example below is an unfunded wallet with empty history.

**1 Selected-network history**

Guard History is private and shows the latest ten recorded entries for the selected side.

2 Read amount and outcome

For populated records, compare customer, fee, net or refund, transaction identifier and status.

3 Empty training wallet

This real screenshot contains no completed sale. It is not a payment receipt or funded test.

Empty training history. A photographed empty list is not a completed-payment example.

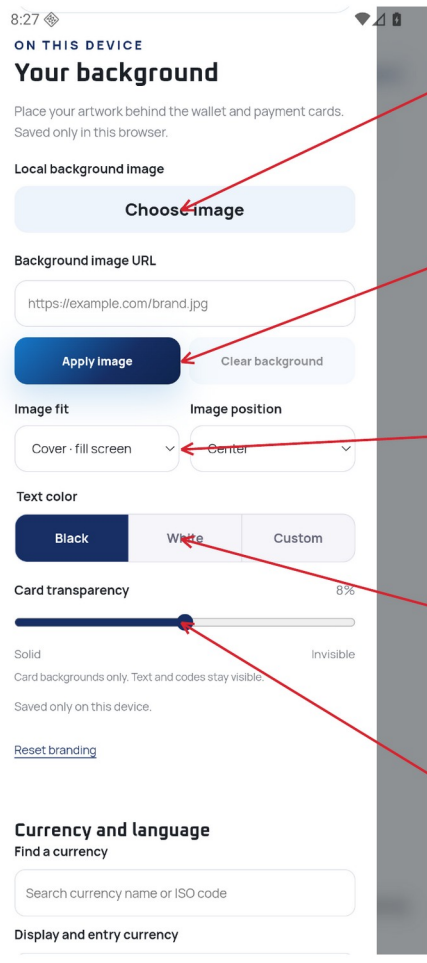
1. For a real record, compare the original customer address, intake amount, fee, net payout or native refund, status and transaction identifier.
2. Confirm the expected net USDC in the separate vault. On Polygon, the service-fee leg can follow the already-confirmed vault payout.
3. If a receipt is queued, pending, failed, ambiguous or held for review, retain the transaction identifier and exact status. Do not clear app data or try to force a duplicate payment.

The USDC forwarding memo records the verified on-chain sender and intake identity. Native returns carry their USDC-only explanation. A memo does not identify a person or guarantee a particular display in Trust Wallet or another app. Keep a separate store sales record; the latest-ten view is not a complete accounting archive.

APPEARANCE

Customize the customer display

Open the authenticated tray and scroll to Your Background. Artwork, text color and card transparency apply globally to both network sides and are stored locally on the terminal.



1 Local image

Choose image imports artwork into the app's local storage. It is not a cloud wallet backup.

2 URL or clear background

Apply an HTTPS image URL, or remove a background. Avoid confidential information in artwork.

3 Fit and position

Cover fills the screen. Choose positioning and check the customer-facing result.

4 Text color

Black, White or Custom must remain readable over both cards and artwork.

5 Card transparency

Move toward Solid or Invisible. Text and payment codes remain visible; appearance is shared across sides.

Current appearance controls. Screen examples use the default light background.

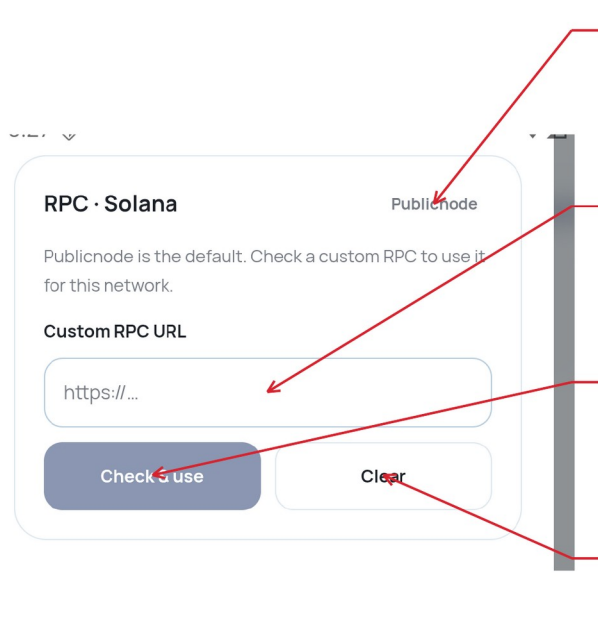
1. Choose image for a local file, or enter an approved HTTPS Background image URL and use Apply image.
2. Use Cover and a suitable Image position for an edge-to-edge design. Check both network views and the system status area.
3. Choose Black, White or Custom text for contrast. Adjust Card transparency toward Solid or Invisible, then inspect the code, status, network labels and admin-entry controls.
4. Use Clear background or Reset branding if the design becomes difficult to read. These controls are not wallet-reset or recovery operations.

Do not place another scannable payment code, sensitive personal information or a misleading network label in the background. Codes and operational messages must remain easy to recognize on the actual checkout display.

NETWORK ADMINISTRATION

Configure an RPC override

Publicnode is the default on both sides. A custom RPC is optional. Open the authenticated tray and find that network's RPC card below the admin gas-deposit section. It is independent of the other side's endpoint.



The screenshot shows the 'RPC · Solana' configuration screen. At the top right is a green 'Publicnode' badge. Below it, text states 'Publicnode is the default. Check a custom RPC to use it for this network.' A 'Custom RPC URL' section contains a text input field with 'https://...' and two buttons: 'Check & use' and 'Clear'. Red arrows point from numbered callouts to these elements: 1 to the badge, 2 to the URL input, 3 to the 'Check & use' button, and 4 to the 'Clear' button.

- 1 Endpoint badge**
Publicnode is the default. Available records saved checks, not continuous uptime.
- 2 Custom HTTPS URL**
Paste an approved endpoint, including its required path or query key.
- 3 Check and use**
Runs ordered read-only checks before saving and activating this side's endpoint.
- 4 Clear**
Restores Publicnode for this side. Clear before entering a different endpoint.

Current default RPC controls. A custom endpoint is not active in this training screenshot.

1. Paste the full approved HTTPS endpoint into Custom RPC URL. Paths and query keys are supported; protect any provider credentials.
2. Tap Check & use. Wait for the ordered read-only checks: endpoint access, correct mainnet, finalized data, supported USDC reads, fees and history. Exact check labels vary by network.
3. When verification succeeds, the endpoint is saved and the URL is locked. A failed candidate does not replace the active endpoint.
4. Use Clear before replacing a saved endpoint or to restore that side's Publicnode default.

Available is saved verification, not live uptime. A later outage can pause processing while the badge remains green. The app does not silently change providers to make a failing custom endpoint appear healthy.

TROUBLESHOOTING

Resolve payment and refund issues

Symptom	Checks and next action
No vault receipt yet	Confirm correct network and supported USDC, app foreground/unlocked, side enabled, native gas/refill status and RPC connectivity. Check the original transaction and Guard History before requesting another send.
Customer sent SOL or POL	Confirm whether an admin funding window was open. Outside it, only eligible direct native payments follow the 20%-plus-gas return rule. Wait for finalization and inspect native history.
Native amount is too small	It can remain held because the refund cannot pay its own network costs without consuming old gas. There is no general operator release button in this build.
History says review or ambiguous	Record the identifier/status and escalate through the store's technical process. Preserve the installation and journals. Review is a safeguard state, not an available recovery workflow.
Wrong token or wrong chain	This build does not bridge, swap or generically recover unsupported assets. Do not repeat the same transfer or promise an automatic refund.
Custodial customer has not received a return	An on-chain refund may have reached the exchange's sender wallet. The customer must follow that provider's crediting process using the return identifier.
Customer asks for a merchandise refund	Mistaken-native handling is not a retail refund function. Use the merchant's separate sales/refund process; this Gate exposes no arbitrary manual-send control.

A new deposit window cannot retroactively turn an already received native payment into administrator funding. A pending transaction is never made confirmed by pressing Refresh.

TROUBLESHOOTING

Resolve access and operating issues

Symptom	Checks and next action
Green shield but paused	Read Enable state, actual native gas and refill requirement. USDC eligibility or a small completed deposit can coexist with insufficient gas.
Deposit complete but funding still insufficient	Compare the received amount with the minimum or additional-refill requirement. Completion alone is not a dollar-value check. Close the window explicitly.
Deposit window interrupted	Do not assume the receipt became retained gas or an automatic refund. Check its recorded classification; uncertain intervals are held. Start a fresh authenticated window only for a new deposit.
RPC Available but processing fails	Available persists until Clear. Inspect the current operational error and provider health; use the saved check or restore default through Clear as appropriate.
Biometric access stopped working	Use the existing app PIN. Changes in enrolled Android biometrics or the app PIN may require re-enabling biometric unlock. Do not attempt a phrase reset.
Both PIN and biometrics unavailable	There is no in-app recovery. Withdraw the old payment display from service and provision a fresh Gate under the store's continuity process.
App left the foreground or device locked	Background pauses both networks. A manual lock requires normal unlock. Returning may resume if the wallet session remained unlocked; verify state before checkout.

For support, record app version, terminal identifier, network, exact status text and public transaction identifiers. Do not send an app PIN, device-unlock code, private key, seed phrase or RPC credential in a support screenshot.

STORE OPERATIONS

Close a shift and transfer responsibility

End of shift

1. Reconcile the selected network's latest records with the vault and store register. Repeat for the second enabled side.
2. Confirm both admin deposit windows are closed. Check for unresolved signed, pending or review entries.
3. Use manual Lock to deliberately end the unlocked checkout session. Backgrounding alone is only a processing pause and may not erase an unlocked session.
4. Keep the physical terminal secured and preserve app storage. Do not uninstall or clear storage as a routine close procedure.

Change of administrator

Maintain an authorized continuity plan for the current app PIN and eligible enrolled Android biometrics. Test any PIN or biometric change while the outgoing administrator can still authenticate. Changing enrollment can invalidate the existing biometric wrapper; changing the app PIN requires re-enabling biometrics.

If access is irretrievably lost, create a fresh Gate configuration and public payment addresses. Replace old customer displays and reconfigure each new network side. The app cannot import the former Gate's phrase or use an administrator recovery bypass. Do not describe the software/source backup as a way to restore lost Gate access.

Updates and device replacement

An authorized compatible update should preserve local state. Before update or replacement, account for pending transactions and save the store's public operational records. Do not discard a pending journal or keep advertising an address that the store can no longer operate. Existing vault control is separate from Gate control.

REFERENCE

Network identifiers and references

These identifiers describe the app 1.0.2 configuration. Token identifiers identify accepted USDC; service collectors receive app fees. Neither is the merchant vault or a general deposit address.

Accepted USDC identifiers

Polygon PoS mainnet, chain ID 137

0x3c499c542cef5e3811e1192ce70d8cc03d5c3359

Solana mainnet USDC mint

EPjFWdd5AufqSSqeM2qN1xzybapC8G4wEGGkZwyTDt1v

Fixed service collectors

Polygon: 0x838886dB9c2048BC96afa3F042Fd05eb6176e29E

Solana: 7cycqrfGqfKx6mrDmhJnRBRjyrwnc7mG3Sbv4FjsGLqM

The flat USDC fee and the mistaken-native percentage fee use the existing collector on their own network. Never enter a collector as the merchant vault by copying this manual.

Default RPC endpoints

Polygon: <https://polygon-bor-rpc.publicnode.com>

Solana: <https://solana-rpc.publicnode.com>

Document references

R1 [App 1.0.2 source and release](#) • [commit 558ebeb](#)

R2 [Circle](#) • [USDC contract addresses](#)

R3 [Android Help](#) • [Pin and unpin screens](#)

External references checked October 21 2026. R2 confirms network token identifiers; R3 describes Android screen pinning. App-specific fees and safeguards are defined by the released source and release evidence, not by the external references.

Publicnode's free Solana discovery fallback checks the standard USDC associated token account and previously known accounts. It cannot discover every unknown nonstandard token account. Do not treat unavailable indexed discovery as proof that no payment exists.

QUICK REFERENCE

Administrator go live checklist

Complete this checklist on the actual store installation before customer service. Each supported network needs its own checks; the global appearance and screen preferences can then be inspected across both views.

- Authorized signed APK installed; app version 1.0.2 and correct release provenance recorded.
- Store administrator can authenticate with the app PIN; any configured eligible biometric has been tested on this physical device.
- Merchant vault address compared with the separate receiving wallet, including full address and network.
- Native gas funded through an explicit deposit window; finalized amount verified; Deposit window closed confirmed.
- Initial minimum or additional native refill requirement met; actual gas and Solana account-rent needs considered.
- Forwarding deliberately enabled on every network offered to customers; unused side remains paused.
- Show Payment Selector matches store policy; changing customer display does not unexpectedly disable another side.
- Codes, asset/network labels, status and menu controls remain readable with chosen artwork and transparency.
- Controlled funded USDC settlement verified against the vault and the per-intake service fee; native-refund acceptance tested under the store's controlled procedure before relying on it.
- Customer-facing gross amount and 20%-plus-network-cost mistaken-native policy explained to staff.
- History and pending/review escalation procedure understood; no expectation of a general manual-send or recovery control.
- Power, internet, Keep screen on and any Android app-pinning policy checked; terminal can be manually locked at close.

Store record

Store and terminal _____

Administrator and review date _____

Solana vault verified by _____

Polygon vault verified by _____

Keep public operational records separately. Do not write a PIN, private key or seed phrase into this manual.

DUALSCAN LLC

Intellectual property disclosure



VisaUSD™ and VisaUSD PoS™ are trademarks of Dualscan LLC.

United States design patents

Dualscan LLC identifies VisaUSD™ and VisaUSD PoS™ as covered by the following United States design patents.

Patent identifier	Type
US-D769296	United States design patent
US-D826955	United States design patent
US-D857054	United States design patent
US-D931899	United States design patent
US-D947939	United States design patent

Registered copyright derivative

Registered Copyright Derivative Of: VA0002308747.

© 2026 Dualscan LLC.

USDC, Solana, Polygon, Android and other third-party names or marks remain the property of their respective rights holders. Their use in this guide identifies compatible assets, networks or device functions.