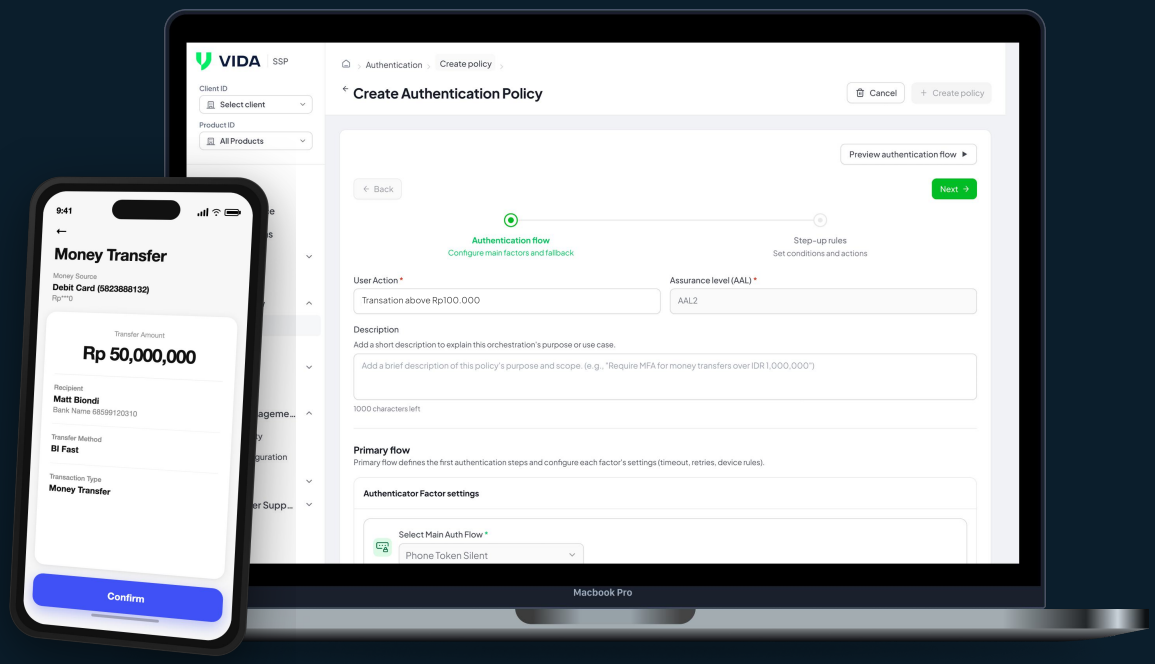
VIDA

Certified Strong Authentication

SMS OTP proved the Phone number

VIDA Proves the Person

Stop account takeover where it actually enters a new handset, a lost credential, and a payment your customer was talked into. And stay silent everywhere else.



Proven in Production

<50ms

P95 signing. Authentication your customer never waits for.

-99%

Fraud reduction, after face and device verification on credential and device changes.

Globally audited

ISO 27001:2022 · ISO 27701 · WebTrust CA · Level 3 PAD · #1 NIST FATE

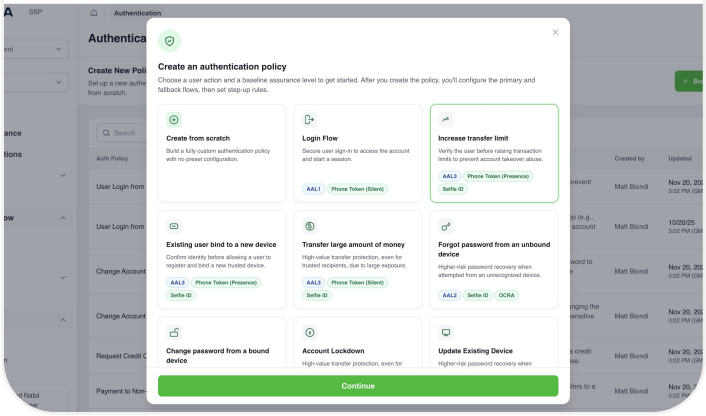
For banks, wallets, multifinance and lenders in Indonesia. Figures measured on production deployments of the VIDA Auth stack.

Let risk define the step-up

Configured in the dashboard, not in a release train.

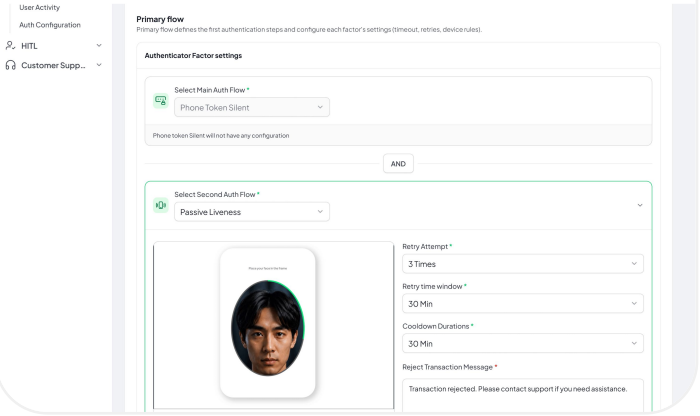
1. Start from the moment

A ready-made policy per action — or build one from scratch.



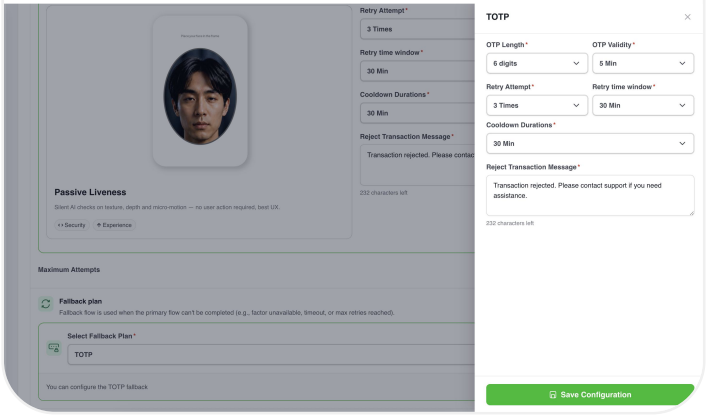
2. Choose and tune the factors

Attempts, expiry, prompt mode and device rules, per factor.



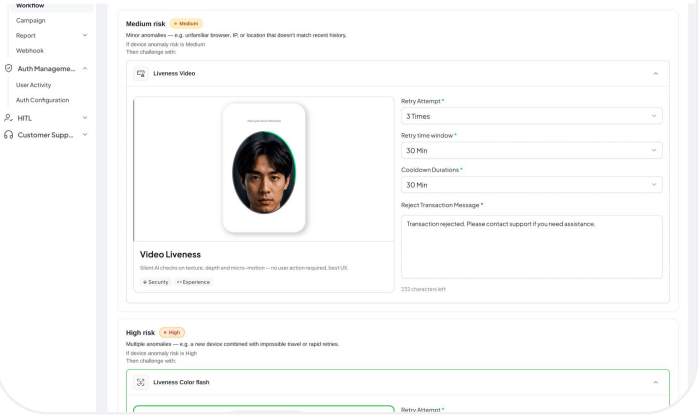
3. Set the fallback

A ready-made policy per action — or build one from scratch.



4. Let risk pick the challenge

Powered by ID Fraud Shield — anomaly sets the risk level.



Two Ways to buys

PACKAGE 1

Phone Token or Face Token

Choose the rung the moment needs — silent device proof for the everyday, a live person for the actions that move money.

PACKAGE 2

Package 1 + ID Fraud Shield

400+ device and behaviour signals, scored in under 200 ms. It decides when the risk is real; your policy decides what the challenge is worth.

Ready to prove the person?

Start with one flow. A proof of concept runs four to six weeks, with pass/fail criteria agreed before it begins.

The Platform

Two Tokens. One ladder

Risk decides when to challenge. The ladder ends at a verified person, not a possessed gadget.

VIDA Phone Token



A key sealed in the phone's chip. Signs silently, keeps re-checking the device.

- Non-exportable at silicon level. Malware finds nothing to steal.
- Cloud sync off by design. A restored backup on another phone produces no valid signature.
- Signs exact amount and payee. Change one character and the signature breaks.
- < 50ms On-device, no network.

Face Token



Trusted device plus the customer's live face, matched against the enrolled identity.

- Server-side match against the enrolled record — not whatever is saved on the handset.
- PAD Level 3 presentation-attack testing: 750 attacks, five species, zero succeeded.
- Color Flash liveness: a sequence no 3D mask or AI avatar can mimic. Fraud resistant on 4K and 5K screens and deepfake injection attacks"

Four kinds of proof, only as many as the moment needs.

Proof of phone number

The network confirms the SIM and flags recent swaps.

Coming soon · February 2027

Proof of device

A key locked in the phone approves in the background.

Proof of presence

One touch. Fingerprint or face unlock in under a second.

Proof of person

A live selfie, matched to the account's identity. No code to give.

Why It Matters

Not all authentication is created equal.

Identity is established once. Everything after that is inference.

Level 1 | Person not present

A password. A code. A token.

Proves possession of a thing, or knowledge of a secret. No human is verified at all.

Level 2 | Person Asserted

Fingerprint unlock. Face unlock

This feels like level 3. It is not.

The check runs locally. Anyone the phone saved passes — including a fraudster's own face.

Level 3 | Person Present

The solution we recommend

Proof of the Person, not the phone

Live	Matched	Bound
Real human, present Right now	Against Your Identity Record	Tied to this exact action

Implementation use case

Three Moments where Fraud is most likely.

1 A New Handset

Device binding. Once a fraudster's face is enrolled, every later approval carries your confidence.

Face Token

2 A Lost Credential

The reset path inherits your weakest factor. Takeover walks in through it.

Face Token

3 A Payment they were Talked Into

The victim approves it themselves. Nothing to intercept the scammer coaches them through.

Face Token

Phone Token