

SHARED FOUNDATION · 04/06

ECZ-ID Customer Dashboard and Operations Guide

How customers operate an ECZ-ID estate, distinguish authenticated control from public proof, manage identity safely and recover access.

PRIMARY READER

ECZ-ID customers, organisation administrators, platform/security operations and estate owners

SECONDARY READER

Support engineers, identity teams, auditors and governance stakeholders

WHEN TO READ THIS

You have acquired ECZ-ID and need to find Passports, understand authenticated customer controls, locate public proof and operate the estate safely.

RELEASE

2026.10
16 October 2026

What you will know after reading

You can distinguish Dashboard from Resolver, navigate the principal customer areas, avoid duplicate identity, recover access and escalate operational issues without exposing secrets.

What this document does not establish

This guide does not imply that every feature is available to every product, entitlement, role or account state, and Dashboard is not the public Resolver.

Permanent route: <https://developers.ecocitizenz.com/guides/customer-dashboard-operations/> · Support: support@ecocitizenz.com

CONTROL VS PROOF

Dashboard and Resolver have deliberately different jobs

The Dashboard is authenticated customer control. Resolver is public read-only proof. Confusing them creates both security and usability problems.

DASHBOARD**Authenticated customer control plane**

- View your ECZ-ID estate and permitted customer actions.
- Work with identity, entitlements, operations and evidence areas available to your account.
- Use recovery and organisation controls.
- Private/customer context stays in the authenticated experience.

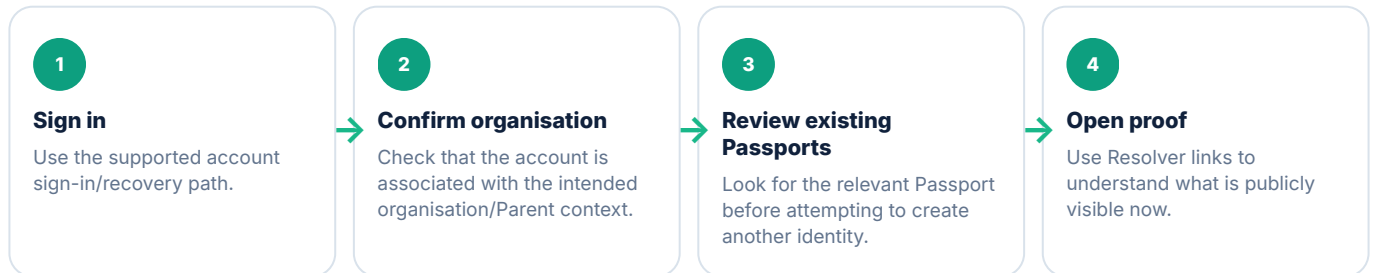
RESOLVER**Public read-only proof**

- Independent re-check by humans and machines.
- Inspect bounded public identity/state/bindings/evidence.
- Do not use Resolver to mutate canonical identity.
- Do not expose secrets or customer-private data in public proof.

FIRST LOGIN

First login: orient yourself before changing anything

A safe first session should establish the organisation context and existing identity estate before creating or changing records.



Duplicate prevention: if the expected Parent or Passport already exists, use the supported reuse/recovery path rather than intentionally minting another canonical identity.

NAVIGATION

Estate overview: understand the main customer areas

The exact features visible depend on current product, entitlement, role and account state. The principal customer areas are organised around identity, operations and evidence.

Overview

A summary of the ECZ-ID estate and current customer context.

Passports & Identity

Locate Parent/Passport identity records and relevant lifecycle context.

Products & Entitlements

See products, access or entitlement context that is available to the account.

Operations

Work with supported bindings, Graph/Monitoring or other operational surfaces where entitled.

Evidence & Proof

Inspect evidence/proof-related customer views and handoff to public Resolver proof.

Badges & Sharing

Use supported badge, QR or sharing mechanisms without exposing private data.

PASSPORT MANAGEMENT

Operate identity without creating duplicate truth

Most operational changes should update the context around a stable identity, not create a new ECZ-ID for every infrastructure change.

Before creating a Passport

- Check the organisation/Parent.
- Search for the existing Passport.
- Confirm whether the same legitimate object is already represented.
- Use account recovery/reuse if the issue is access rather than identity.

When the environment changes

- Update supported endpoint/provider/repository/runtime bindings where appropriate.
- Refresh evidence when the supporting source changes.
- Re-check published state.
- Preserve the ECZ-ID if the legitimate underlying object is the same.

OPERATIONS

Operations and entitlements: use what is actually enabled

The Dashboard may expose products, entitlements, bindings, graph/monitoring or other operational capabilities depending on the customer's actual estate.

Products & Entitlements

Treat the visible entitlement state as account-specific. Do not assume access merely because a capability exists elsewhere in ECZ-ID.

Bindings

Keep the supported external references aligned with the current object. Incorrect bindings can create misleading verification outcomes.

Graph / Monitoring

Where enabled, use operational relationship/monitoring surfaces as customer controls - not as substitutes for public Resolver proof.

Principle: Dashboard is the place to operate your estate; Resolver is the place another party independently re-checks the bounded public result.

EVIDENCE & SHARING

Evidence, proof, badges and sharing

Customer operations should preserve a clear separation between the private control context and what is intentionally published for counterparties.

Evidence & Proof

Review the evidence/proof context available to your account. Treat evidence by source, scope and freshness; do not convert presence into a universal "safe" verdict.

Resolver proof

Use the public read-only record when a counterparty needs independent verification. Machine consumers can use the documented machine-readable route.

Badges / QR / sharing

Share supported proof links or badges only when they point to the correct canonical record and do not expose private customer information.

Receipts where present

Where receipt evidence is available, use the supported customer/Resolver presentation rather than copying sensitive transaction inputs into public surfaces.

ACCOUNT & ORGANISATION

Organisation, account activity, billing/plans and recovery

Some administrative areas are account-specific. Use the controls actually presented to your role and entitlement rather than assuming a universal layout.

Organisation

Manage supported organisation context and review which Parent/estate you are operating. Do not confuse account membership with action authority.

Activity & Recovery

Use supported activity/recovery mechanisms to regain access. An access problem should not be “solved” by creating duplicate identities.

Billing & Plans

Where displayed, use the Dashboard for the account’s current commercial/plan context. Free Passport identity should not be presented as a paid trial.

Alerts

Treat visible alerts as operational signals to investigate. Confirm current Resolver proof when public state/freshness is relevant.

SECURITY & RECOVERY

Safe operations and troubleshooting

Good support evidence accelerates troubleshooting; secrets in support material create risk.

PROBLEM	FIRST SAFE ACTION
Cannot sign in	Use the supported recovery path. Do not create another organisation/identity to work around access.
Passport not visible	Confirm the organisation/Parent, acquisition state and the ECZ-ID you expect.
Resolver proof differs from expectation	Distinguish a copied-identifier error, missing/incorrect binding, stale evidence or lifecycle state change.
Wrong provider/endpoint reference	Correct the supported binding through the authenticated control plane rather than creating a new ECZ-ID.
Need support	Send ECZ-ID, failed step, visible error and time. Never send passwords, API keys, AWS registration tokens or certificates.

QUICK REFERENCE

One-minute customer operations checklist

Use this checklist after acquisition and before escalating an operational problem.

Operate

- Correct organisation/Parent selected
- Existing Passport located before creating another
- Current state reviewed
- Bindings/evidence reviewed where relevant
- Resolver proof opened for public verification
- Private information kept inside authenticated surfaces

Recover / escalate

- Use supported sign-in recovery
- Capture visible error and occurrence time
- Include ECZ-ID / Passport ID where available
- Do not send secrets
- Contact support@ecocitizenz.com

Next: For public verification use the Resolver guide. For security/policy boundaries use Security, Trust Boundaries and Safe Interpretation.