

ECZ-ID MCP Passport AWS Marketplace Getting Started and Technical Guide

From AWS Marketplace subscription to a canonical MCP ECZ-ID with independent Resolver proof.

MCP PASSPORT · AWS GETTING STARTED

PRIMARY READER

AWS Marketplace subscriber, cloud administrator, developer and customer administrator.

SECONDARY READER

Procurement, security architecture, AI platform operations and technical support.

WHEN TO READ THIS

You have found ECZ-ID MCP Passport in AWS Marketplace and want to activate it correctly.

RELEASE

2026.10 · 15 October 2026

WHAT YOU WILL KNOW AFTER READING

You can complete acquisition, reuse or create the supported account/Parent, obtain the MCP Passport, open Dashboard and verify it in Resolver.

WHAT THIS DOCUMENT DOES NOT ESTABLISH

AWS Marketplace supplies acquisition context. It does not become the canonical ECZ-ID identity or authority root.

NEXT

After activation, use the Operations guide to keep endpoint, tool-surface state and evidence current.

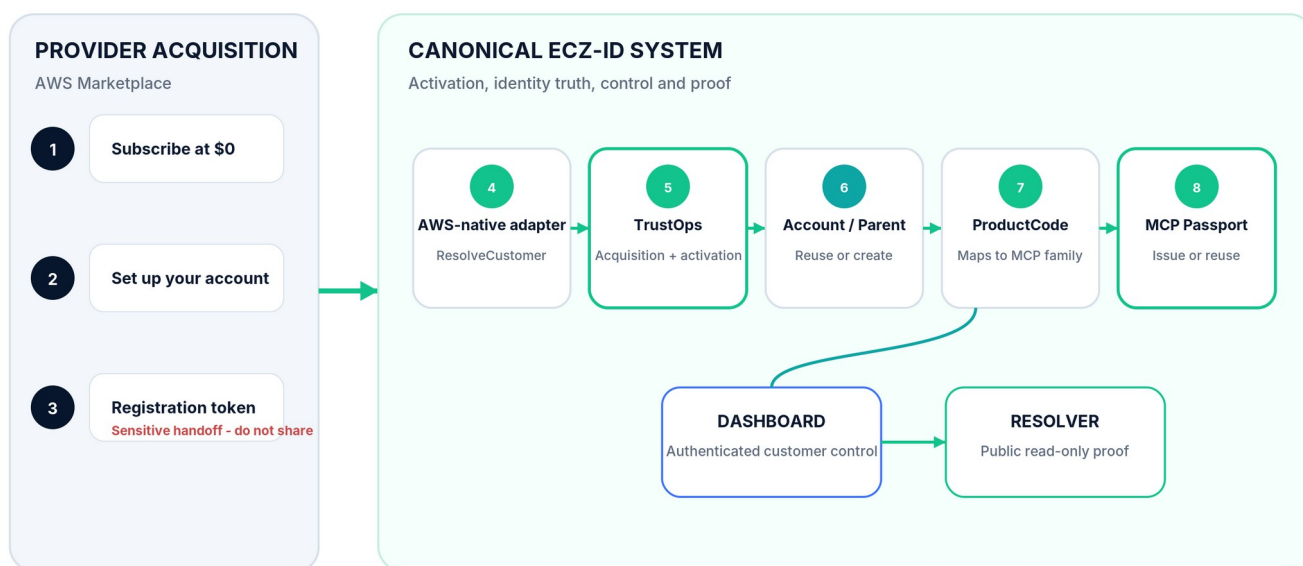
[START HERE](#)

The whole journey in one view

The Passport is permanently free. Subscribe in AWS, complete the account handoff, then verify the canonical MCP ECZ-ID in Resolver.

AWS Marketplace → canonical MCP Passport → Resolver

AWS supplies acquisition context; ECZ-ID remains the canonical identity and proof system.



PRICING

ECZ-ID MCP Passport is permanently free through this AWS Marketplace listing. It is not a time-limited Free Trial.

AWS

Acquisition / provider context

ECZ-ID

Canonical identity + activation

Resolver

Independent public re-check

STEP-BY-STEP ACQUISITION

1. Subscribe → 2. Set up your account → 3. handoff

AWS Marketplace provides the customer acquisition context; the registration token is sensitive and must not be copied into public or support channels.

1 SUBSCRIBE AT \$0

Open the ECZ-ID MCP Passport listing and subscribe at \$0. There is no ECZ-ID software charge for the Passport.

2 SET UP YOUR ACCOUNT

Choose Set up your account so AWS can continue into the ECZ-ID fulfillment path.

3 REGISTRATION TOKEN

AWS passes a registration token to ECZ-ID. Treat it as sensitive operational input.

FULFILLMENT ENDPOINT

<https://trustops.ecocitizenz.com/aws/marketplace/fulfill>

SECURITY

Do not copy the AWS Marketplace registration token into screenshots, chat, tickets or public documentation. If setup fails, record the visible error and time instead.

RESOLVECUSTOMER AND TRUSTOPS

4. identify the AWS customer → 5. activate the ECZ-ID acquisition flow

The AWS-native adapter resolves the Marketplace customer and hands acquisition into TrustOps.

AWS-NATIVE ADAPTER

Uses the AWS Marketplace integration to resolve AWS customer context. Provider-native identifiers remain acquisition/binding context, not the ECZ-ID authority root.

TRUSTOPS

Processes acquisition and activation, applies supported account/Parent reuse and hands the customer into the canonical lifecycle.

ARCHITECTURE LAW

AWS Marketplace = acquisition/provider context. TrustOps = acquisition/activation. Core = canonical identity truth. Dashboard = control. Resolver = read-only proof.

ACCOUNT, PARENT AND PASSPORT REUSE

6. reuse or create account + Parent → 7. map ProductCode → 8. issue or reuse Passport

The target outcome is one canonical identity for the intended MCP server/tool surface, not a new Passport for every subscription click.

ACCOUNT

Reuse the supported existing EcoCitizen account when appropriate; otherwise follow the canonical account acquisition path.

PARENT

Reuse the relevant Parent/organisation relationship where supported; avoid deliberate duplication.

MCP PASSPORT

ProductCode maps to the MCP Passport family. Issue a new Passport only when the logical object needs one; otherwise reuse the canonical one.

DUPLICATE-PREVENTION RULE

The same logical MCP surface should keep the same canonical MCP ECZ-ID where supported. Update endpoint/tool context as bindings/evidence rather than minting another identity.

FIRST CUSTOMER CONTROL

9. continue to Dashboard

Dashboard is the authenticated customer control plane; Resolver is the public proof surface.

DASHBOARD - PRIVATE CONTROL

Use Dashboard to inspect the permitted customer estate, Passport state, bindings/evidence and organisation/account context available to your role.

RESOLVER - PUBLIC PROOF

Use Resolver to present and independently re-check the bounded public MCP Passport record. Resolver is not the mutation plane.

FIRST CHECK

Confirm the expected MCP Passport exists, the intended Parent/operator context is visible where supported, and Resolver returns the expected record.

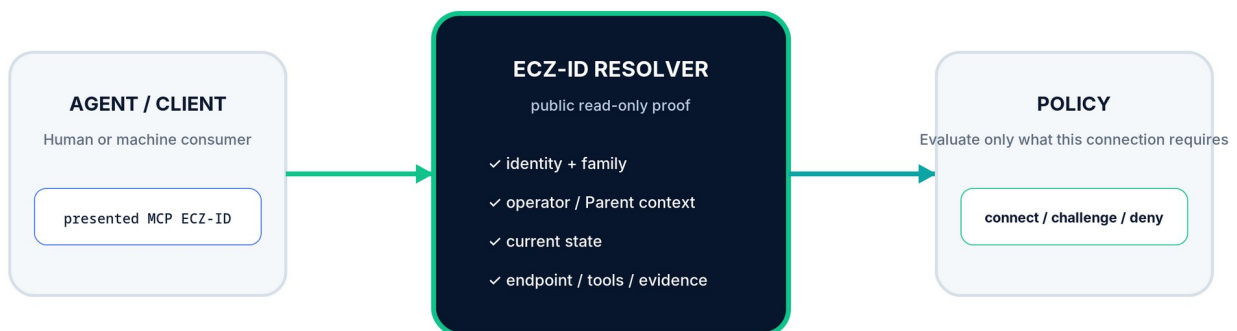
FIRST RESOLVER VERIFICATION

10. re-check the MCP Passport

A successful AWS acquisition is not complete from the customer perspective until the MCP ECZ-ID can be independently resolved and interpreted correctly.

Independent re-check before an agent connects or invokes

Human and machine consumers can resolve the same MCP ECZ-ID again when endpoint, tools or state may have changed.



GET https://api.ecocitizenz.com/api/p/{ecz_id}.json

Absent required data = not established. Re-resolve according to freshness and change policy.

MACHINE-READABLE ROUTE

GET https://api.ecocitizenz.com/api/p/{ecz_id}.json

- Validate Passport family = MCP.
- Check expected operator / Parent relationship where relevant.
- Read current published state.
- Inspect endpoint/tool bindings and evidence needed for the connection.
- Apply local authentication, authorization and runtime policy separately.

CONNECT SAFELY

Use Passport proof before connection or invocation

The Passport helps answer “is this the MCP surface I intended, and what current context supports that identity?” It does not answer every security question by itself.

Re-check the MCP surface before connection or consequence

Use MCP Passport proof as input to local policy - not as a universal safe/unsafe verdict.

**BOUNDARY**

MCP Passport identifies and contextualises the server/tool surface; it does not grant tool permission or certify behaviour.

BOUNDARY

MCP Passport does not grant tool permission, replace authentication, or certify tools as safe. Apply your own policy using the proof you require.

SECURITY AND SECRET HANDLING

What must never enter public proof or support channels

The AWS registration token and other credentials are operational secrets; the Passport is designed to publish bounded proof, not secrets.

NEVER SEND

Passwords
API keys
AWS registration tokens
Certificates/private keys
MCP credentials or bearer tokens

SAFE SUPPORT CONTEXT

Failed stage
Visible error
Occurrence time
AWS account context where appropriate
ECZ-ID / Passport ID if available

MCP-SPECIFIC RULE

Do not publish server credentials, API keys, authorization headers or private tool configuration into Resolver, screenshots or support messages.

Support

support@ecocitizenz.com
Support covers AWS setup, activation, Passport issuance/reuse, account access, Resolver verification and troubleshooting.

TROUBLESHOOTING

Diagnose the failed stage before taking action

The fastest recovery path is to identify where the journey stopped, preserve the canonical identity and avoid repeating actions that create confusion.

SUBSCRIBE / SETUP

Confirm the listing is visible to the permitted AWS account. Record visible errors and time; do not expose the registration token.

RESOLVECUSTOMER / ACTIVATION

Contact support with AWS account context and the failed stage. Do not repeatedly create accounts or Passports as a workaround.

ALREADY HAVE ECOCITIZENZ

Use the supported existing-account path rather than intentionally creating a duplicate Parent or MCP identity.

RESOLVER MISMATCH

Confirm acquisition completed, the ECZ-ID is correct and the expected endpoint/tool bindings are current before escalating.

60-SECOND COMPLETION CHECK

Know when you are done

Use this checklist before treating the AWS acquisition as complete.

- AWS subscription is active at \$0.
- Set up your account completed without exposing the registration token.
- Supported account / Parent was reused or created as intended.
- ProductCode mapped to MCP Passport.
- Canonical MCP Passport was issued or reused.
- Dashboard access works for the customer role.
- Resolver returns the expected MCP ECZ-ID.
- Operator context, state and relevant endpoint/tool bindings look correct.

NEXT

Read the MCP Passport Operations, Lifecycle and Troubleshooting Guide to keep the proof current over time.