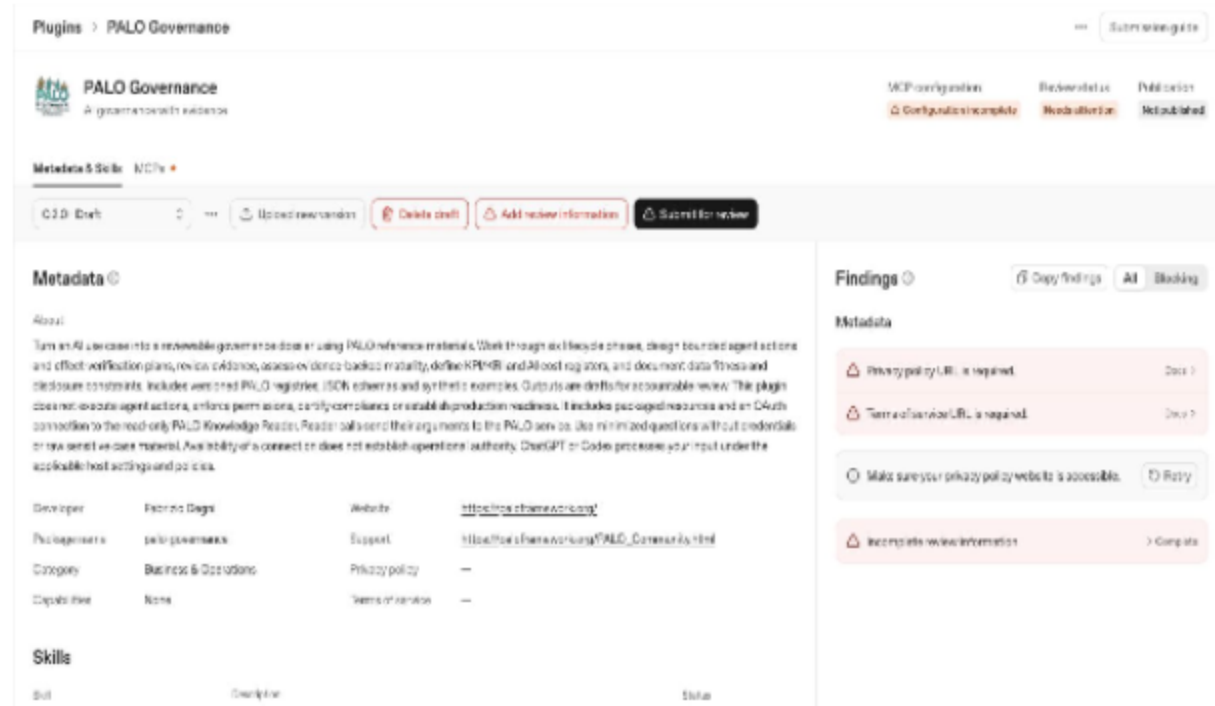


BUILDING THE PLUGIN

AI governance, with evidence at every step

A technical account of skill packaging, source provenance, OAuth integration and release qualification.

**Connected draft. Qualification in progress.
Not submitted or published.**



The screenshot shows the PALO Governance plugin interface. At the top, there's a header with the PALO logo and the text "PALO Governance - A governance with evidence". Below this, there's a section for "Metadata & Skills" with a "NCPs" dropdown. The main content area is divided into two columns. The left column contains "Metadata" with a description of the plugin and a table of metadata. The right column contains "Findings" with a list of issues.

Developer	Package name	Website
Fabrizio Degni	palogovernance	https://github.com/fabrizio-degni/palo-governance
Package name	palogovernance	Support
Concept	Business & Operations	Privacy policy
Capabilities	None	Terms of service

Findings

- Privacy policy URL is required. (Doc ?)
- Terms of service URL is required. (Doc ?)
- Make sure your privacy policy website is accessible. (Doc ?)
- Incomplete website information. (Complete)

Actual OpenAI Platform draft
Configuration incomplete / Needs attention / Not published

Fabrizio Degni

PALO creator & maintainer



fabriziodegni.com



paloframework.org

PALO GOVERNANCE / DEVELOPMENT RECORD

27 October 2026 • Connected draft 0.2.0

Accountable people review and approve the documentation produced by each workflow

01 Lifecycle Assessment

Case brief, six-phase control/evidence matrix and next review actions. Unknown fields stay explicit.

02 Agentic Action Design

Draft Action Claim and Effect Contract, delegation limits, effect checks and a negative test plan.

03 Evidence Review

Claim-to-evidence matrix, contradictions, incident timeline and tests needed to close findings.

04 Maturity Assessment

Two-lens profile of deployment capability and governance. Missing evidence limits the assessment.

05 KPI, KRI and AI FinOps

Indicator register and cost reconciliation plan. Uncertain billing and undefined ratios remain visible.

06 Data Governance

Data flows, provenance and fitness requirements, disclosure constraints and evidence gaps.



Build workflow and package structure

03

Every skill carries the same frozen reference snapshot, with local paths and file hashes

Canonical PALO
references

Six autonomous
skill directories

Validate paths,
hashes and manifest

Freeze ZIP and
upload new draft

```
palo-governance/  
  plugin.json  
  mcp.json  
  assets/palo-logo.png  
  skills/  
    palo-agentic-action-design/  
      SKILL.md  
      references/  
        operating-contract.md  
        corpus/ ...  
    ... five other skill folders
```

185

files in connected version 0.2.0

Six skills × 26 canonical references.
Each directory is self-contained; no sibling
skill dependency is required.

ARCHIVE SHA-256

```
c453a94f736b2c38750023d646161083  
311e5b2fd64b27bffa2bdee1fe7440e3
```

Fabrizio Degni

PALO creator & maintainer



fabriziodegni.com



paloframework.org

PALO GOVERNANCE / DEVELOPMENT RECORD

27 October 2026 • Connected draft 0.2.0

```
name: palo-agentic-action-design
```

```
"Use when designing a future agent action:  
mandates, delegation limits, Action Claims,  
Effect Contracts, approval requirements  
or recovery plans."
```

```
"For an actual timeout, incident or disputed  
past result, start with PALO Evidence Review."
```

```
"Keep authorization, execution, observed effect  
and business outcome separate."
```

```
"Never mint an executable claim, signature,  
token or approval."
```

Four separate conclusions

Authorization, an execution receipt, an independently observed effect and a business outcome each require their own evidence.

Design versus incident

A design specifies evidence to collect later. An uncertain past attempt stays unknown or inconclusive until observations resolve it.



Sanitized excerpt: tenant identifiers, issuer URLs and outer wrapper are omitted

```
"palo-reader": {
  "type": "streamable-http",
  "url": "https://guide-api.paloframework.org/mcp-guide",
  "extensions": { "com.openai": { "auth": {
    "type": "oauth",
    "client": {
      "mode": "provided",
      "tokenEndpointAuthMethod": "client_secret_post"
    },
    "baseScopes": [
      ".../palo:guide",
      ".../palo:knowledge:read"
    ]
  } } }
}
```

ChatGPT host
Selects a PALO workflow



Authenticated MCP request
Minimized tool arguments



PALO Knowledge Reader
Canonical sources, read only

Reader calls retrieve guidance only.
Business actions require separate
authority and execution controls.



Actual Microsoft Entra configuration after the approved, limited permission change

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for MSFT

API / Permissions name	Type	Description	Admin consent requ...	Status
✓ PALO Knowledge Reader API (2) ...				
palo:guide	Delegated	Use PALO Knowledge Reader	Yes	✓ Granted for MSFT ...
palo:knowledge:read	Delegated	Read PALO canonical knowledge	Yes	✓ Granted for MSFT ...

Client identity and consent

Existing single tenant. Graph User.Read removed. Only palo:guide and palo:knowledge:read granted as delegated API permissions.

Runtime admission remains separate

The Reader allowlist still lacks the ChatGPT client. Entra consent does not automatically admit a client at the service boundary. No write permission was added.

Fabrizio Degni

PALO creator & maintainer



fabriziodegni.com



paloframework.org

PALO GOVERNANCE / DEVELOPMENT RECORD

27 October 2026 • Connected draft 0.2.0

Six skills passed the portal checks

07

Actual screenshot from 27 October 2026; automated scans cover one layer of readiness

Skills

Skill	Description	Status
palo-agentic-action-design	Use when designing a future agent action: mandates, delegation limits, Action Claims, Effect Contracts, approval requirements or recovery plans. For an actual timeout, incident or disputed past result, start with PALO Evidence Review.	Checks passed
palo-data-governance	Use when designing data provenance, purpose and fitness checks, AI-system data lineage, or bounded data disclosures for a PALO governance case.	Checks passed
palo-evidence-review	Use when reviewing supplied evidence or an actual incident, timeout, execution receipt or disputed past agent result. Identify gaps between permission, execution and observed outcome. For designing a future action, start with PALO Agentic Action Design.	Checks passed
palo-kpi-kri-finops	Use when defining PALO KPI/KRI indicators or an AI workload cost and evidence register, including budget reservations, uncertain billing and reconciliation.	Checks passed
<u>palo-lifecycle-assessment</u>	Use when a user wants to turn an AI use case into a PALO lifecycle governance dossier, identify applicable controls, or prepare an accountable review.	Checks passed
palo-maturity-assessment	Use when assessing AI deployment capability and governance maturity using the PALO two-lens rubric for a defined organization or system and observation period. For a single future action use PALO Agentic Action Design; for an actual incident or disputed result use PALO Evidence Review.	Checks passed

6 / 6

SKILL CHECKS PASSED

The package is saved as draft 0.2.0.
The public listing remains unpublished.

Remaining review inputs

Privacy and terms, reviewer information and connected MCP qualification remain incomplete. A passed scan is not publication approval.

Fabrizio Degni

PALO creator & maintainer



fabriziodegni.com



paloframework.org

PALO GOVERNANCE / DEVELOPMENT RECORD

27 October 2026 • Connected draft 0.2.0

Static package 0.1.0 in local Codex; these results do not qualify connected Reader 0.2.0

16

passed within scope

1

failed no-echo test

1

infrastructure block

Representative checks

Tool success stayed separate from effect verification.
Missing maturity evidence stayed unresolved.
Undefined ratios stayed undefined. Embedded
instructions remained untrusted evidence.

N4 and P7 remain open

N4 echoed a synthetic API placeholder and failed its
criterion; no real secret was supplied. P7 timed out
before output during workspace routing. Neither was
reclassified as a pass.

Harness: isolated plugin installation, read-only sandbox, recorded responses and trace audit.

Fabrizio Degni

PALO creator & maintainer



fabriziodegni.com



paloframework.org

PALO GOVERNANCE / DEVELOPMENT RECORD

27 October 2026 • Connected draft 0.2.0

Reviewer scope, accepted corrections and disproved findings remain distinct

GLM-5.3 High

Reviewed the extracted manifest, six skills and shared contract. The full corpus and runtime were outside scope. Identified resource isolation, path and routing risks.

Gemini 4, high reasoning

Reviewed action design, evidence review and maturity after the broader attempt failed. Three critical skills; no installed-host test or final ZIP approval.

Changes checked against the source evidence

Resource isolation: every skill carries its own reference snapshot.

Evidence: future observations stay pending; existing uncertainty stays explicit.

Routing: future design and actual incident review have separate entry points.

Maturity: required items and limits from missing evidence remain visible.

A claimed invisible-character defect was disproved by a byte-level check.

Fabrizio Degni

PALO creator & maintainer



fabriziodegni.com



paloframework.org

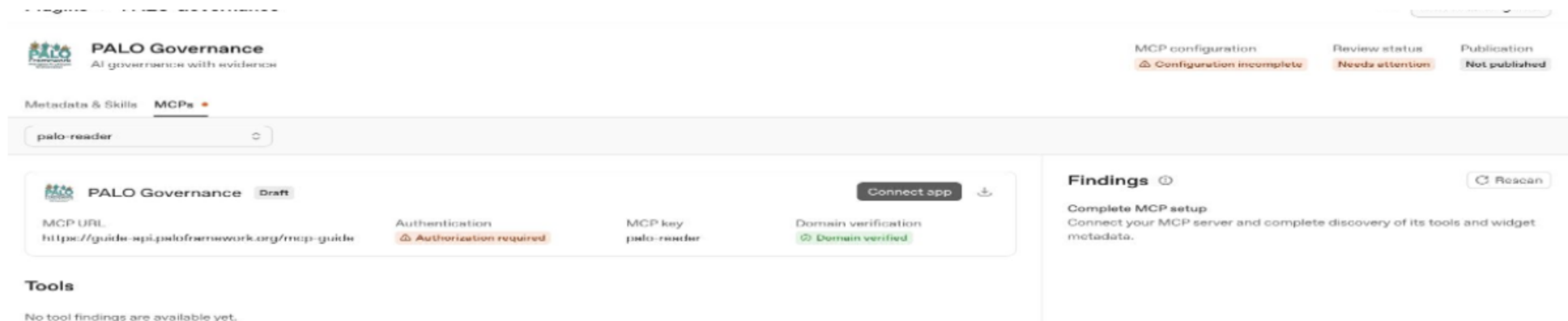
PALO GOVERNANCE / DEVELOPMENT RECORD

27 October 2026 • Connected draft 0.2.0

OAuth completion remains blocked

10

The verified domain and incomplete authentication appear together in the actual Platform state



The screenshot shows the PALO Governance interface. At the top, there's a header with the PALO logo and navigation tabs: 'Metadata & Skills' and 'MCPs'. Below this, a search bar contains 'palo-reader'. The main content area displays the MCP configuration for 'palo-reader'. It includes fields for 'MCP URL' (https://guide-api.paloframework.org/mcp-guide), 'Authentication' (Authorization required), 'MCP key' (palo-reader), and 'Domain verification' (Domain verified). A 'Connect app' button is visible. To the right, a 'Findings' section shows a 'Complete MCP setup' finding with the instruction 'Connect your MCP server and complete discovery of its tools and widget metadata.' Below the main content, a 'Tools' section states 'No tool findings are available yet.'

OpenAI starts
Microsoft sign-in

Entra returns
AADSTS500113

Exact OpenAI callback
still required

“No reply address is registered for the application.” Token exchange and authenticated tool discovery have not completed. The callback must match this specific connection.

Fabrizio Degni

PALO creator & maintainer



fabriziodegni.com



paloframework.org

PALO GOVERNANCE / DEVELOPMENT RECORD

27 October 2026 • Connected draft 0.2.0

Actual support acknowledgement; no secrets, tokens or personal contact details are shown

Thank you. This is the public ...



Plugins/Apps submissions. I can provide a redacted screenshot of the connection drawer if needed. No secret, token or credential should be requested in this conversation.

✓ Escalation requested >

Escalated to a support specialist; You can expect a response in the coming days. Replies will also be sent via email. You can add additional comments to this conversation if needed.



Help Center conversation
27 October 2026

Escalation acknowledged

The request includes draft identifiers and the missing-callback diagnosis. No authoritative callback or human technical answer had arrived at the recorded snapshot.

Frankfurt server, Lithuania backups

Read-only checks confirmed the Reader VPS in Frankfurt and weekly backups in Lithuania. nginx retains 14 nonempty rotated archives, not a guaranteed 14-day deletion period.

Application logging, backup deletion and processor terms still require completion.

Fabrizio Degni

PALO creator & maintainer



fabriziodegni.com



paloframework.org

PALO GOVERNANCE / DEVELOPMENT RECORD

27 October 2026 • Connected draft 0.2.0

The next milestone is a reviewable submission; publication remains a later OpenAI decision

**Complete exact callback
and Reader admission**

**Run 5 positive and
3 negative MCP cases**

**Reviewer access, real demo
and public policies**

Eight connected cases prepared

Positive: explain, route, plan integration, list sources and retrieve with provenance. Negative: unsupported certification, operational payment execution and private cross-customer retrieval. All remain to be run in the intended host.

Evidence still needed

Record a genuine demonstration and establish secure reviewer access. Complete privacy, terms and publisher attestations. Preserve an actual submission receipt before describing the candidate as submitted.

Project, research and media: [linkedin.com/in/fdegni/](https://www.linkedin.com/in/fdegni/) • info@paloframework.org

Fabrizio Degni

PALO creator & maintainer



fabriziodegni.com



paloframework.org

PALO GOVERNANCE / DEVELOPMENT RECORD

27 October 2026 • Connected draft 0.2.0