WSO2CON NORTH AMERICA

May 20 - 22, 2026 | Austin, Texas, USA

Meet ThunderID

An Identity Core for the Future



Omindu Rathnaweera

Director, Head of Product & Architecture
WSO2 - IAM

The Shift in Identity

Key shifts driving the future of identity.



AI agents in production

Agents now invoke APIs, hold credentials, and act on behalf of users.

Traditional identity representations fail to capture them



Post-quantum on the horizon

The threat of "harvest now, decrypt later" is already here

IAM is a top migration target



Identity is becoming user-held

Decentralized identity is moving from spec to deployment.

Regulations like eIDAS 2.0 are scaling.

Apple/Google hold government IDs, mDLs.



Why a New Identity Core

Some things you learn from running identity at scale. Others, you cannot evolve into.

What We Learned from 15+ Years of WSO2 IS

A generation of production identity work

- **Design for complete flows:** Focus on the entire user journey rather than endpoints.
- **Configure, don't customize:** Bundled features must flex; custom code is the exception.
- **Master operational economics:** Control runtime dependencies to minimize costs.
- **Shifted integration shapes:** The developer interaction model has evolved.

Why Ground-Up, Not Incremental

Things you cannot evolve into

- Agent identities native to the architecture
- Crypto-agility deep in the runtime, not bolted on.
- A small, fast, headless runtime that fits cloud-native delivery.
- A modular foundation, not a monolithic runtime.

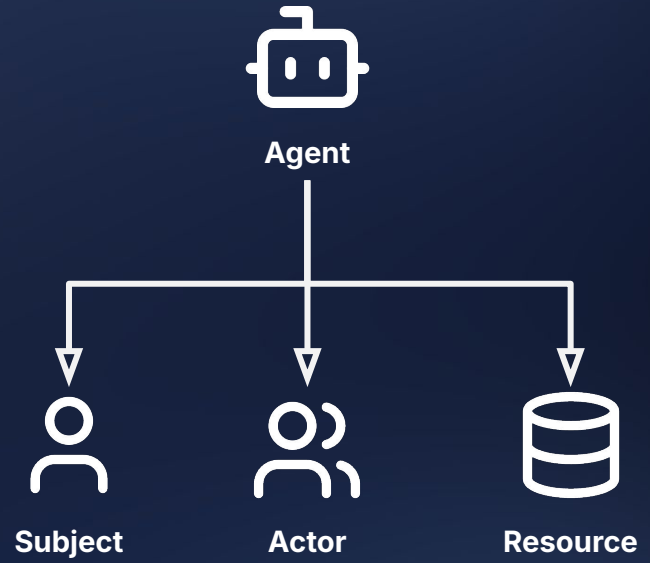
Introducing

ThunderID

Auth for the Modern Dev

https://thunderid.dev

Agent-Native Identity



WSO2

Agent-Native Identity

PILLAR 1 OF 4

Why it Matters

AI agents are landing in real production systems today. Treating an agent as a service account strips out delegation and consent. Treating it as a user strips out provenance and scoping.

Neither captures what an agent actually is: an entity acting under delegated authority, often inside another principal's session, that needs to be observed and constrained.

What ThunderID is Building

- Agents modeled as a distinct identity type with their own lifecycle and ownership
- Cryptographically anchored credentials issued for agents.
- Delegated authority with scoped permissions and time bounds.
- Consent-aware access requests with purpose, scope, duration.
- Traceability: who initiated, which agent acted, on whose behalf.

Post-Quantum Safe by Design



WSO2

Post-Quantum Safe by Design

PILLAR 2 OF 4

Why it Matters

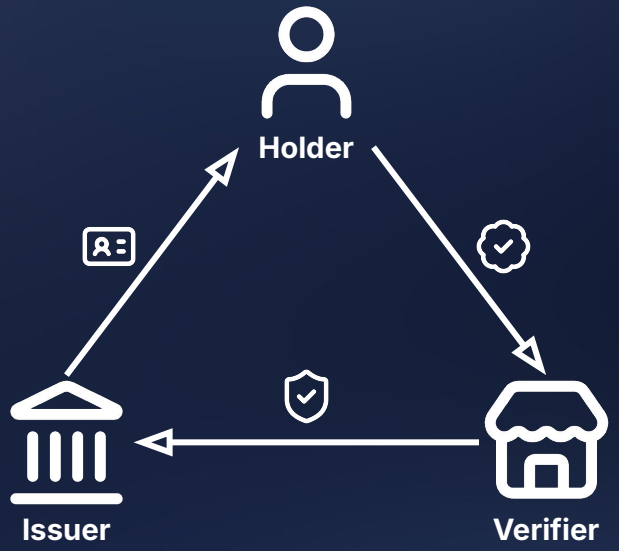
Long-lived signed assertions, federation tokens, and inter-service credentials issued today may need to remain unforgeable well into the post-quantum window. NIST has now standardized ML-KEM, ML-DSA, and SLH-DSA.

IAM is one of the highest-value migration targets. Stacks with crypto baked deep into the runtime cannot move quickly when the algorithm landscape changes.

What ThunderID is Building

- Crypto-agile core: algorithms, key types, token protection configurable. BYOK supported.
- Post-quantum algorithms (ML-KEM, ML-DSA) supported as first-class options.
- Hybrid mode: classical and post-quantum running in parallel during transition.
- PQ TLS for inbound and outbound communication.
- PQ signatures for JWT and signed assertions.
- Foundation evolves as new post-quantum algorithms emerge.

Decentralized Identity



WSO2

Decentralized Identity

PILLAR 3 OF 4

Why it Matters

DIDs, verifiable credentials, digital wallets, trust registries: the pieces are maturing in different communities and on different timelines, and they need to come together inside actual applications.

An IAM stack designed for this ecosystem from the start lowers the integration cost for the developers and architects building those applications.

What ThunderID is Building

- Verifiable credential issuance via OID4VCI.
- Verifiable credential presentation via OID4VP.
- Standard APIs covering issuer, verifier, and holder interactions.
- Interoperability with DIDs, VCs, digital wallets, and trust registries.
- Designed for use by enterprises and public-sector deployments.

Lightweight, High Performance Runtime



WSO2

Lightweight, High Performance Runtime

PILLAR 4 OF 4

Why it Matters

Identity has to fit how modern teams deliver software: containerized, deployed with the rest of the stack, defined as code, reviewed through PRs, rolled out via pipelines.

A headless, API-first runtime stays small and operationally simple, performs efficiently in request paths, and can be integrated into whatever user experience the application requires.

What ThunderID is Building

- Built with Go. Fast startup, low CPU, memory.
- Headless and API-first. Console, SDKs, and end-user UIs sit on top.
- Declarative resources for apps, IdPs, roles, OUs, schemas, flows.
- Import / export with parameterization. GitOps-ready out of the box.
- Stateless-oriented: minimal persistence in the request path.
- Immutable runtime: ephemeral instances, no in-place mutation

Architecture at a Glance



Architecture at a Glance



Developer Experience

From hands-on to AI-assisted. Same APIs, same surfaces, human in the loop.

Hands-on Development

Build with familiar tools and standards

- Framework SDKs for React, Next.js, Vue, Nuxt with prebuilt UI components.
- OAuth 2.0 and OIDC at the protocol level. Console + RESTful APIs for management.
- Generic flow engine + visual builder: login, registration, recovery, step-up, onboarding, and custom workflows.
- Composable identity primitives that return verifiable assertions.

AI-assisted Development

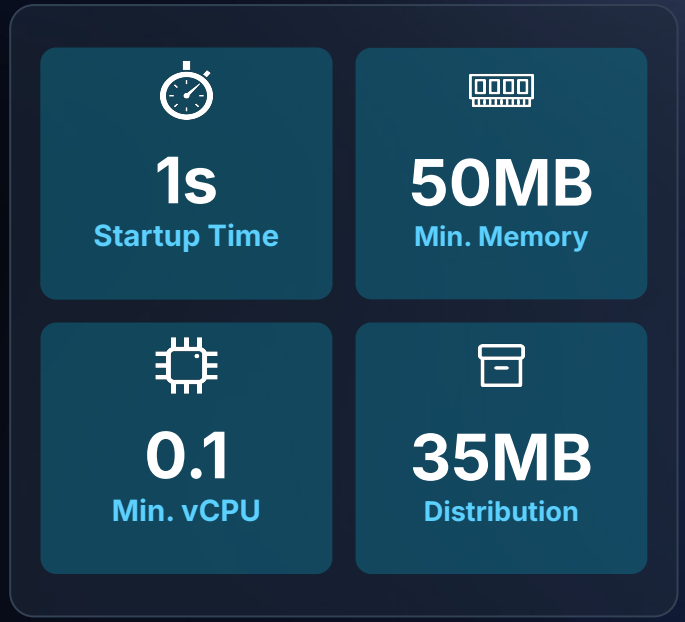
Bring agents and tools into the workflow

- Identity operations exposed as standard APIs.
- Same operations available via Model Context Protocol (MCP).
- IAM capabilities packaged as reusable agent 'skills'.



Benchmarks and Footprint

What it actually takes to run ThunderID

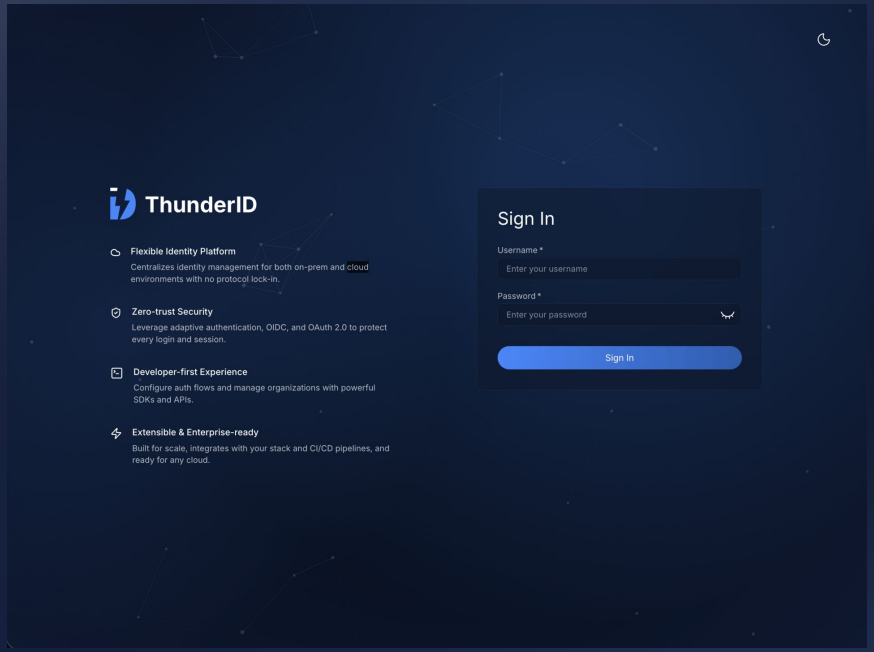


vCPU: 0.1, Memory: 50MB, Concurrency: 10

Grant type	Transaction Step	p95 latency
Client Credentials	Get access token	303 ms
Authorization Code	Send authorize request	207 ms
	Start authentication flow	198 ms
	Perform authentication	293 ms
	Get authorization code	203 ms
	Get access token	200 ms

Methodology: Postgres + in-memory cache, Single ThunderID instance

ThunderID in Action

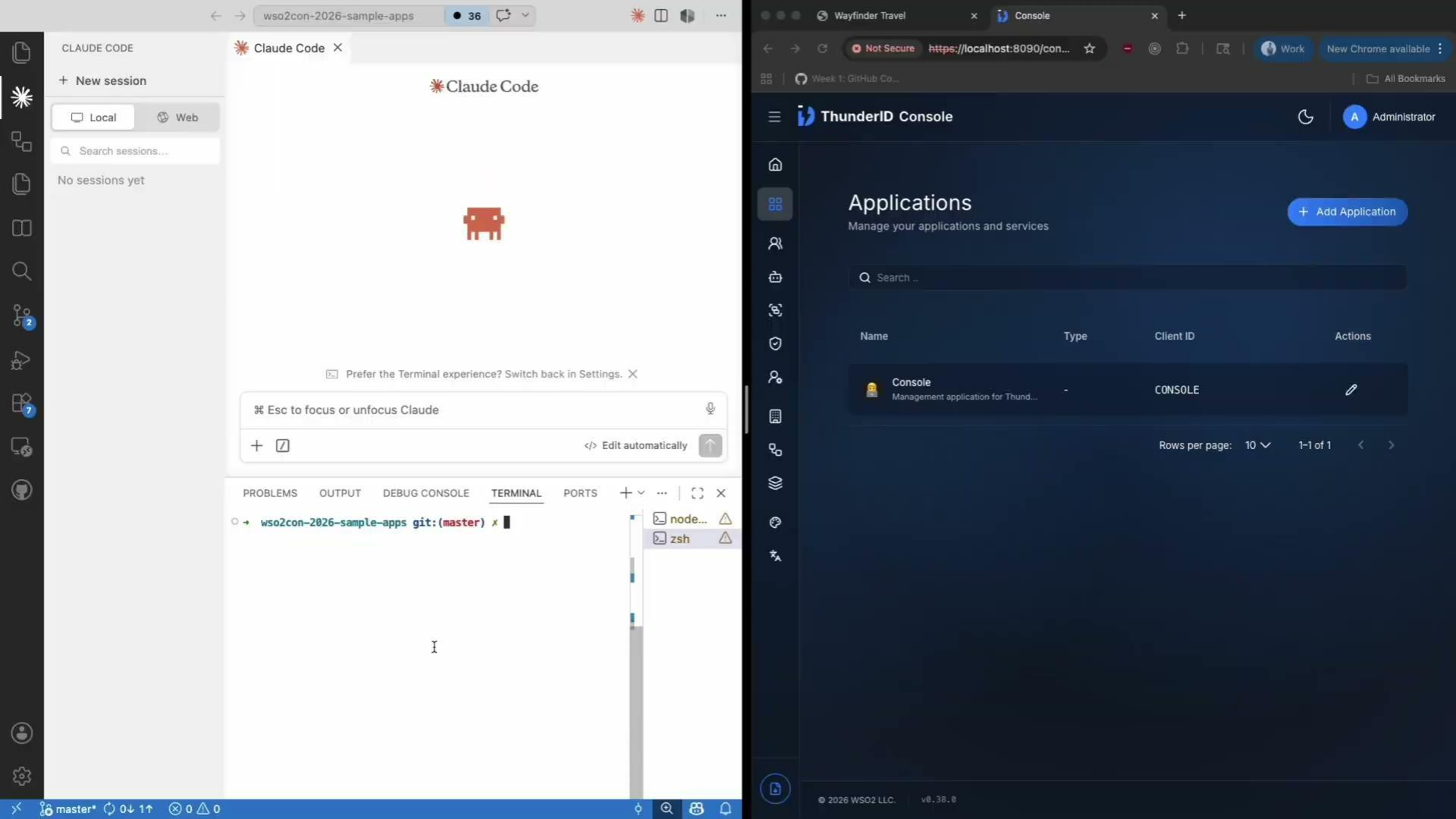


WSO2

Scenario - 1

Securing application with ThunderID
through an Agentic workflow

WSO2

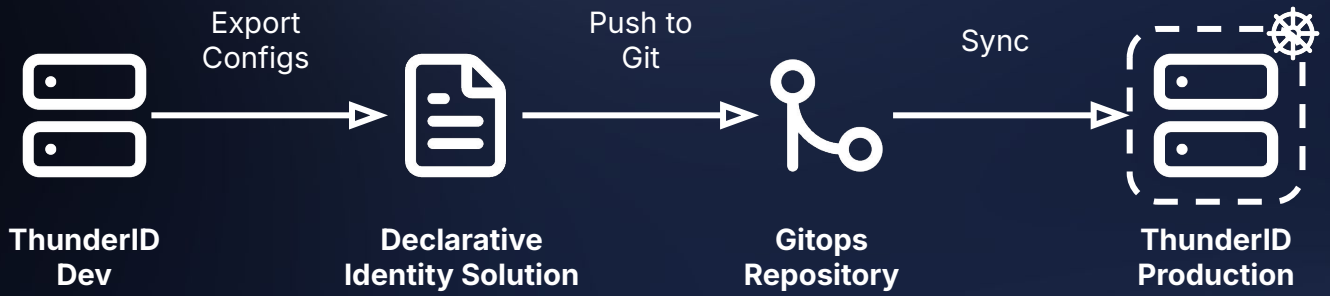

wso2con-2026-sample-apps
36
CLAUDE CODE
New session
Local
Web
Search sessions...
No sessions yet
Claude Code
Claude Code
Prefer the Terminal experience? Switch back in Settings.
⌘ Esc to focus or unfocus Claude
Edit automatically
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
wso2con-2026-sample-apps git:(master) ✗
node...
zsh
master*
Wayfinder Travel
Console
Not Secure
https://localhost:8090/con...
Work
New Chrome available
All Bookmarks
ThunderID Console
Administrator
Applications
Manage your applications and services
Add Application
Search ..
Name
Type
Client ID
Actions
Console
Management application for Thund...
-
CONSOLE
Rows per page:
10
1–1 of 1
© 2026 WSO2 LLC.
v0.38.0

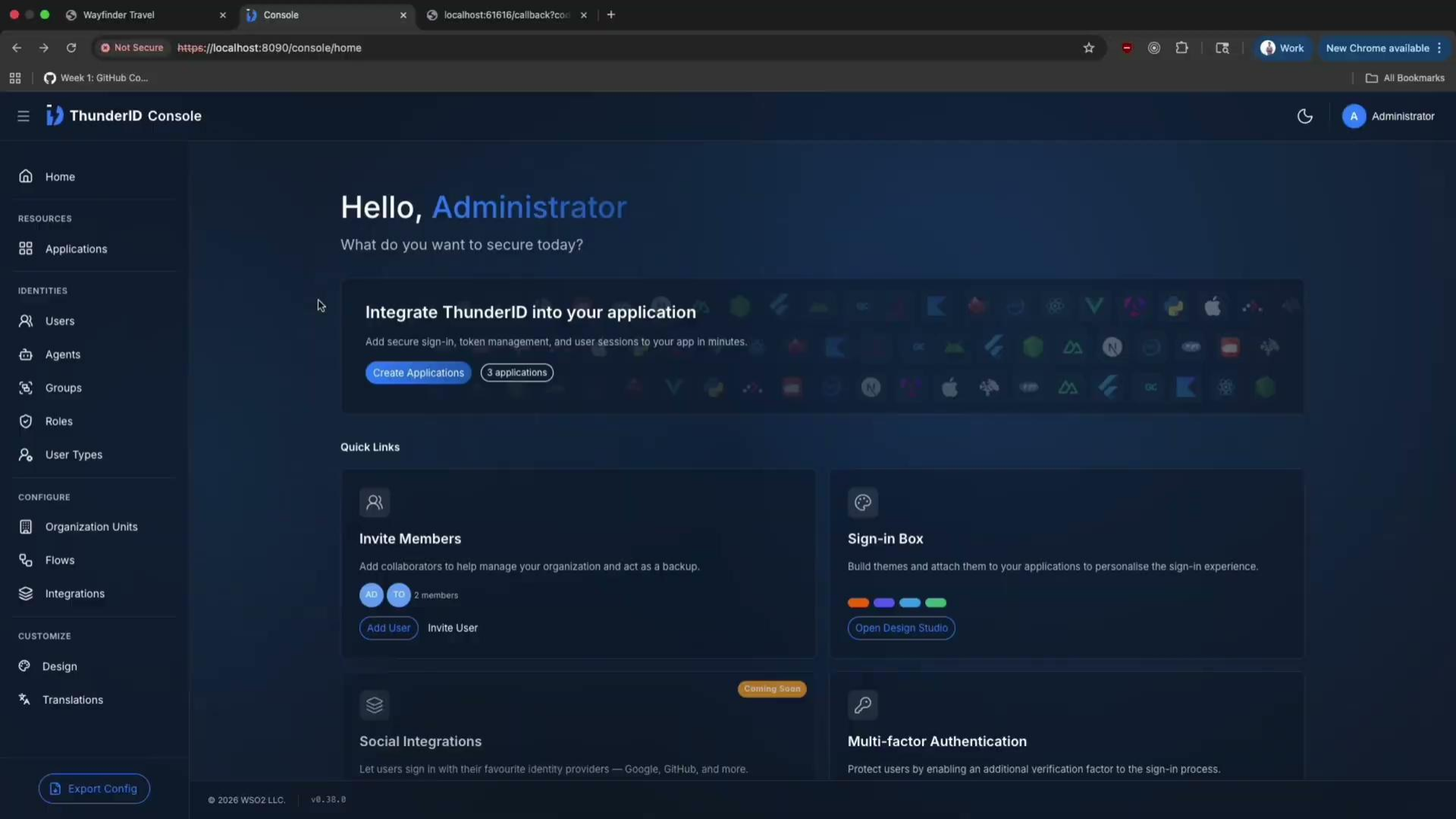
Scenario - 2

Gitops with declarative resources

WSO2

CI/CD Flow with ThunderID




Wayfinder Travel
Console
localhost:61616/callback?co
Not Secure
https://localhost:8090/console/home
Work
New Chrome available
Week 1: GitHub Co...
All Bookmarks
ThunderID Console
Administrator
Home
RESOURCES
Applications
IDENTITIES
Users
Agents
Groups
Roles
User Types
CONFIGURE
Organization Units
Flows
Integrations
CUSTOMIZE
Design
Translations
Export Config
Hello, Administrator
What do you want to secure today?
Integrate ThunderID into your application
Add secure sign-in, token management, and user sessions to your app in minutes.
Create Applications
3 applications
Quick Links
Invite Members
Add collaborators to help manage your organization and act as a backup.
AD
TO
2 members
Add User
Invite User
Sign-in Box
Build themes and attach them to your applications to personalise the sign-in experience.
Open Design Studio
Coming Soon
Social Integrations
Let users sign in with their favourite identity providers — Google, GitHub, and more.
Multi-factor Authentication
Protect users by enabling an additional verification factor to the sign-in process.
© 2026 WSO2 LLC.
v0.38.0

Scenario - 3

Securing Agent Interactions with ThunderID

WSO2

Wayfinder

john.doe@example.com

Welcome back, john.doe@example.com.



Flexible fares
Compare routes, cabins, and timings from one calm workspace.

Protected bookings
Keep booked trips connected to secure Asgardeo sign-in.

Fast comparisons
Filter practical options for routes, dates, and travelers.

FRESH PICKS

Flight ideas for your next window of free

Start searching →

Where we are

What's shipping today, and what's coming next.

1.0.0 GA

July, 2026

ThunderID will be contributed to

OpenWallet FOUNDATION

Hosted at the Linux Foundation EU

Supported Today

- Identities for users, AI agents, and workloads, with attributes and credentials
- Hierarchical OU model for managing identity resources
- Standards-based auth: OAuth 2.1 and OIDC
- Flow engine for login, registration, recovery, and step-up flows
- Fine-grained authorization and policy-based consent
- White-labeling and localization of end-user interfaces
- Developer tools: Console UI, SDKs, APIs, and MCP

Early Adopters

Real systems building on ThunderID today

NATIONAL ID

MOSIP eSignet 2.0

eSignet is the national digital identity authentication and eKYC module of MOSIP. eSignet 2.0 will be built on top of ThunderID.

GOV PROJECTS

LSF (Lanka Software Foundation)

Uses ThunderID as the IdP for Sri Lanka government-focused open-source projects.

CNCF SANDBOX

OpenChoreo

OpenChoreo is a developer platform for Kubernetes. ThunderID ships as the built-in STS for OpenChoreo.

API PLATFORM

WSO2 API Platform

An open-source platform for managing APIs and AI services. ThunderID ships as the built-in STS for the platform.

AGENT PLATFORM

WSO2 Agent Platform

An open-source unified control plane for AI agents. ThunderID powers the platform's Agent IAM capabilities.

Commercial Offerings Around ThunderID

Three productized profiles, all powered by ThunderID's Purpose-Built Profiles capability.

ALL-IN-ONE

Access Manager

A productized identity service for human users covering employee, customer, partner, and citizen identities.

July 2026

MACHINE / API

STS

A focused security token service for machine-to-machine, API, and service identities.

July 2026

AI AGENT IDENTITY

Agent ID

A productized identity service for AI agents: delegation, consent, traceability, and verifiable credentials.

Q1 2027

Same OSS foundation, three productized profiles. Each product is ThunderID running with a focused capability set, hardened, and supported.

What this Means for WSO2 Identity Server

Read this slide as an FYI, not a deadline.

ROADMAP

WSO2 IS continues

The Identity Server line is fully supported. Roadmap is intact. New releases continue.

Identity Server 7.4.0 - 2027 Q1



MIGRATION

No force migration

There is no requirement to move to Access Manager. Adoption is opt-in, on your timeline, when it makes sense for you.



PATH

Seamless when you're ready

When you choose to evaluate Access Manager, we'll provide a supported migration path. Coexistence is fine; many architectures will run both.



Join the ThunderID Effort

Open project. Contributions and critique welcome.

- **Test Drive & Feedback:**
  Quickstart in under a minute.
- **Join the Conversation:**
  Join a discussion or ask questions
- **Contribute:**
  Help fix an open issue

Show your support:

⭐ Star the repository on GitHub

github.com/thunder-id/thunderid

MOSIP eSignet 2.0 is co-engineered with us. We're open to more partnerships at that level.

WSO2CON NORTH AMERICA

May 20 - 22, 2026 | Austin, Texas, USA

Thank You!



Omindu Rathnaweera

Director, Head of Product & Architecture
WSO2 - IAM