

Distributed Systems, Inc. - Security Test Summary

Assessment date: October 6, 2026

Accountable security lead: Arthur Colle, Founder & CEO

Function: Infrastructure Security within Research & Engineering

Contact: arthur@distributed.systems

Result and scope

113 automated security regression tests passed; zero failures or errors. The local run completed in approximately 5 seconds. This assessment covers the current Tool Management API engineering checkout, including existing uncommitted changes. It is an internal engineering assessment, not an independent audit, certification, or production penetration test.

The tests exercise canonical identity authority, unified authentication, OAuth protections, customer MCP OAuth, and private native execution boundaries. Tested controls include rejecting retired identity paths and migration tokens, audience and account validation, rejecting untrusted signing keys, authorized account selection, account and tenant isolation, and private execution boundary checks.

Method

The five test suites were run together using pytest on October 6, 2026. Fixtures use test identities, generated inert signing keys, substituted JWKS transport, temporary data directories, and local test clients. This evidence is limited to the behavior exercised by those fixtures; it does not establish the security of deployed configuration, external identity providers, or all product surfaces.

Suites:

- test_canonical_identity_authority.py
- test_unified_auth.py
- test_oauth_security.py
- test_customer_mcp_oauth.py
- test_private_native_boundaries.py

The internal evidence archive retains the JUnit result, test output, source-file hashes, and checkout revision. The run emitted dependency deprecation warnings; those did not fail the tests. No vulnerability discovery or remediation is claimed by this summary.

Authorized testing and follow-up

Arthur Colle is accountable for authorizing controlled testing, reviewing findings, and prioritizing remediation. The function tests company-owned or maintained systems and explicitly authorized environments. Each engagement follows the company's written security testing rules of engagement. Potential findings require reproduction, impact assessment, an owner, and regression verification before closure.

Limits

This run did not test sandbox escapes or frontier-model attack capabilities, and it did not comprehensively assess DSCO, Chimera, GraphSub, model-routing gateways, or distributed production infrastructure. Planned evaluations of those systems will be separately scoped and authorized. It provides no claim of ISO/IEC 27001 certification, SOC 2 attestation, CVE publication, or a paid bug-bounty program.