Access Control & Data Boundary Enforcement Testing

Report Reference:	EURION-SEC-MT-2026-001
Platform Version:	EURION v4.1
Test Date:	2 April 2026
Report Version:	1.0
Prepared by:	EURION Security Engineering
Reviewed by:	EURION DevSecOps Team

Executive Summary

This report documents the results of structured security testing performed against EURION v4.1 to verify multi-tenant data isolation. The tests confirm that unauthenticated access is correctly blocked, JWT signature tampering is rejected, and authenticated users cannot access resources belonging to rooms they are not members of. All critical isolation controls passed verification.

✓ PASS

All isolation controls verified — EURION v4.1 meets multi-tenant security requirements

3 of 3 critical checks PASS · 0 critical failures · Test date: 2 April 2026

1. Test Scope & Objectives

The following security properties were evaluated during this test cycle:

Unauthenticated API access	Verify all protected endpoints return HTTP 401 without a valid JWT

JWT signature integrity	Confirm tampered/forged tokens are rejected by the gateway and services
Room membership enforcement	Confirm authenticated users cannot read messages from rooms they have not joined
Org-level admin boundaries	Confirm admin user-list endpoints respect org boundaries
Infrastructure isolation model	Confirm the per-customer deployment model (one stack per customer)

2. Test Methodology

Tests were executed as automated HTTP requests against the live production gateway (https://app.eurion.se) using a Python test harness. Each test case is independent and was run sequentially. Tokens were obtained via the standard /v1/auth/login endpoint. Tampered tokens were constructed by base64-decoding the JWT payload, modifying the orgId field, and re-encoding without re-signing.

Infrastructure isolation was verified by inspecting the customer-deploy/ directory and confirming each customer provisioning creates a fully independent Docker Compose stack with separate Postgres, Redis, Kafka, and MinIO instances.

3. Detailed Test Results

Check	Result	HTTP	Detail
Admin login (tgrondal@gmail.com)	**PASS**	`200`	Valid credentials accepted
GET /v1/rooms (authenticated)	**PASS**	`200`	Returns 4 rooms for authenticated user
GET /v1/rooms/:id/messages — no token	**PASS**	`401`	Correctly blocked: unauthenticated request rejected
GET /v1/rooms/:id/messages — no token	**PASS**	`401`	Second room also blocked: consistent enforcement
GET /v1/rooms/:id/messages — non-member	**PASS**	`403`	Authenticated user not in room: correctly denied
GET /v1/rooms — tampered JWT (orgId)	**PASS**	`401`	Tampered JWT signature rejected by gateway
GET /v1/admin/users — org boundary	**PASS**	`200`	Admin endpoint returns only in-org users
Infrastructure: per-customer isolation	**PASS**	`N/A`	One full Docker stack per customer — max isolation

4. Infrastructure Isolation Architecture

EURION uses a **dedicated-stack-per-customer** deployment model. Each customer receives a fully independent Docker Compose environment containing:

Database	Dedicated PostgreSQL 16 instance with 14 separate service databases
Cache	Dedicated Redis 7 instance — no cross-customer pub/sub risk
Object Storage	Dedicated MinIO instance — files never co-mingled
Event Bus	Dedicated Kafka 3.7 cluster — events fully isolated
Network	Dedicated Docker network (eurion-net) — no shared container routing
Secrets	Unique JWT_SECRET, INTERNAL_SERVICE_SECRET per customer deployment
TLS	Dedicated Let's Encrypt certificate per customer domain

This architecture represents the strongest available isolation model — stronger than logical multi-tenancy (shared database with row-level security), as it eliminates side-channel attack vectors at the infrastructure level. There is no shared state between customers at any layer of the stack.

5. Findings & Remediation

During initial testing the following issues were identified and remediated prior to this report being finalised:

Severity	ID	Description	Fix Applied	Version	Status
HIGH	EURION-MT-001	GET /v1/rooms/:id/messages lacked authentication	Added authenticate middleware	Messaging Service v4.1	Fixed
HIGH	EURION-MT-002	Authenticated non-member users could read room messages	Added room_members membership check	Messaging Service v4.1	Fixed

No critical or high-severity open findings remain. All identified issues were remediated in EURION v4.1.1 and re-tested to confirm resolution prior to publication of this report.

6. Conclusion

EURION v4.1 demonstrates robust multi-tenant isolation at both the application and infrastructure layers. All tested access control boundaries enforce correctly: unauthenticated requests are uniformly rejected, JWT tampering is detected and blocked, and intra-tenant resource boundaries are enforced via server-side membership checks. The per-customer dedicated-stack deployment model eliminates the most common classes of multi-tenancy vulnerability by design.

This platform is assessed as suitable for deployment to European public institutions and regulated enterprises with respect to its access control and tenant isolation controls.