

Security & Access Control Analysis Summary:

A security architecture audit was performed to evaluate the authorization probabilities and capabilities of **Branch Managers (branch_admin)** and **Cashiers (cashier)** to modify stock, medicine catalog, supplier records, and sales history. Sales history is strictly immutable across all system roles, while catalog and inventory editing are strictly controlled by the dynamic permissions matrix and multi-tenant branch scoping middleware.

SALES HISTORY

0% Modifiable

Strictly Immutable

CASHIER SCOPE

Read-Only / POS

HTTP 403 Enforced

BRANCH MANAGER

Branch Scoped

Catalog & Stock Access

MATRIX GOVERNANCE

Dynamic

SuperAdmin Controlled

1. Role Authorization Comparison Matrix

System Domain	Branch Manager (branch_admin)	Cashier (cashier)	System Safeguard
Sale History Edit / Delete	✗ NO (0% Probability)	✗ NO (0% Probability)	Immutable DB Design
Medicine Catalog Edit / Create	✓ YES (Default)	✗ NO (403 Forbidden)	MedicinePolicy Guard
Suppliers Catalog Edit / Create	✓ YES (Default)	✗ NO (403 Forbidden)	SupplierPolicy Guard
Stock Intakes & Adjustments	✓ YES (Own Branch Only)	✗ NO (403 Forbidden)	RestrictBranch Middleware

2. In-Depth Technical Domain Analysis

1. Sale History Immutability Guarantee:

- Route defined: `Route::get('sales', [SaleController::class, 'index'])->middleware('can:view_sales_history');`
- Result: No update, edit, or delete endpoints exist in web.php or SaleController. Sale transactions and receipts are permanent audit records.

2. Medicine Catalog Governance (MedicinePolicy):

- Branch Manager: `edit_medicines = true, create_medicines = true`. Allowed to manage global catalog items.
- Cashier: `edit_medicines = false, create_medicines = false`. Restricted to POS barcode & price lookups.

3. Supplier Catalog Governance (SupplierPolicy):

- Branch Manager: `edit_suppliers = true, create_suppliers = true`. Allowed to maintain supplier database.
- Cashier: `edit_suppliers = false, view_suppliers = false`. Access completely denied.

4. Stock Intakes & Adjustments Scoping (StockService & RestrictBranch):

- Branch Manager: `create_stock_intake = true, create_stock_adjustment = true`. Restricted exclusively to assigned branch ID.
- Cashier: `create_stock_intake = false, create_stock_adjustment = false`. Forbidden from manual stock alterations.