06 - Security & Permissions

# 🔐 Communication & Authentication

- HTTPS-only communication to prevent data interception  
- Token-based API access using API Key + Secret per shop  
- Tokens tied to specific user roles with limited permissions  
- IP Whitelisting (optional) to limit access to known hosts

# 👥 Role-Based Permissions

🔹 HQ Roles

Role: Sync Admin / System Manager  
- Can push Items, Prices, Rules  
- Can pull Sales, Stock, Returns  
- Full access to Sync Logs, Retry Queue, Conflict UI

🔹 Shop Roles

Role: Shop Sync Agent  
- Can push Sales Invoice, Stock Entry, Payment Entry, Customer  
- Cannot access Item/Price doctypes  
- Used only for sync API user

# 🧩 Sample Role Permissions JSON (Shop)

{  
 "role": "Shop Sync Agent",  
 "doctype": ["Sales Invoice", "Stock Entry", "Payment Entry", "Customer"],  
 "read": true,  
 "create": true,  
 "write": false,  
 "submit": true,  
 "cancel": false,  
 "delete": false  
}

# 🛡️ Validation & Protection

- All incoming records must include a `reference\_number`  
- Conflicts logged and blocked until resolved  
- Retry queue isolated by shop  
- Only Sync Admins can view/edit logs  
- Submit-only privilege to prevent mid-stage data push

# 🔒 Additional Security Recommendations

- Rate limit API access using Nginx or Traefik  
- Use secrets manager or .env files to store API Keys securely  
- If extended to mobile or 3rd party: use OAuth2 or JWT tokens  
- Encrypt backup files before transfer  
- Audit logs weekly