Authentication & Authorization

JWT Authentication

1. **Login Flow**
   - User authenticates through external auth service
   - Receives JWT token
   - Token contains: `user_id`, `username`, `store_id` (if applicable)
2. **Token Usage**

```
// Token verification in middleware
const token = req.headers.authorization?.split(' ')[1];
const decoded = jwt.verify(token, process.env.JWT_SECRET);
```

3. **Token Refresh**
   - Implement token refresh logic in auth service
   - Tokens typically expire after 24 hours

Passport Strategies

Basic HTTP authentication for admin/internal endpoints:

```
// In middleware/passport.js
passport.use(new BasicStrategy(
  function(username, password, done) {
    // Validate credentials
  }
));
```

Authorization Levels

1. **Public** - No authentication required
2. **Authenticated User** - Requires valid JWT

3. **Store Owner** - Requires JWT with store_id
4. **Admin** - Requires Basic Auth or special admin JWT
5. **Affiliate** - Requires JWT with affiliate permissions

Middleware Chain Example

```
app.post(
  '/product/add',
  verifyCross,           // Verify JWT token
  getStoreID,            // Extract store ID
  validator.validate(),  // Validate request
  productController.addProduct
);
```

Revision #1
Created 24 February 2026 09:23:23 by ondeliveloper
Updated 24 February 2026 09:23:40 by ondeliveloper