 set up a complete API routing system with:

1. Input Validation:
   * Joi validation schemas for all routes
   * Custom validation for ObjectIds
   * Request body, params, and query validation
2. Authentication & Authorization:
   * JWT authentication middleware
   * Role-based permission checks
   * Resource-level access control
3. Error Handling:
   * Async error catching
   * Proper HTTP status codes
   * Standardized error responses
4. Routes Organization:
   * Core User Management
   * Profile Management
   * Preferences Management
   * MFA & Security
   * Session Management
   * Account Management

The API endpoints are now ready to use. Here's how to use them:

1. Create a new user:

Code

CopyInsert

POST /api/v1/users

Content-Type: application/json

Authorization: Bearer <token>

{

"email": "user@example.com",

"password": "securepass",

"firstName": "John",

"lastName": "Doe",

"institutionId": "507f1f77bcf86cd799439011",

"roles": ["507f1f77bcf86cd799439012"]

}

1. Update user profile:

Code

CopyInsert

PUT /api/v1/users/:id/profile

Content-Type: application/json

Authorization: Bearer <token>

{

"phoneNumber": "+1234567890",

"address": {

"city": "San Francisco",

"country": "USA"

}

}

1. Enable MFA:

Code

CopyInsert

POST /api/v1/users/:id/mfa/enable

Authorization: Bearer <token>