completed the implementation of the auth service with all the required features. Here's a summary of what has been implemented:

1. **Authentication Features**:
   * Login with username/password
   * JWT-based token management (access & refresh tokens)
   * Password reset functionality
   * Secure password validation and hashing
2. **Multi-Factor Authentication (MFA)**:
   * TOTP-based MFA setup and verification
   * QR code generation for easy setup
   * Backup codes generation and management
   * MFA enable/disable functionality
3. **Security Features**:
   * Rate limiting for sensitive endpoints
   * Token rotation and invalidation
   * Password complexity requirements
   * Session management
   * IP-based security
4. **Email Notifications**:
   * Password reset emails
   * MFA status change notifications
   * Login alerts
   * Password change notifications
5. **Redis Integration**:
   * Token storage and management
   * Rate limiting implementation
   * MFA setup temporary storage
   * Session tracking
6. **Configuration**:
   * Environment-based configuration
   * Secure defaults
   * Comprehensive environment variables

To use the service, you'll need to:

1. Copy **.env.example** to **.env** and fill in your environment-specific values
2. Install the new dependencies:

npm install

1. Ensure Redis is running and accessible
2. Configure your SMTP server details for email notifications
3. Start the service:

npm run dev

The service is now ready to handle authentication requests with enhanced security features.