📚 File Sharing Backend API Documentation

🏗️ Tổng quan

Hệ thống chia sẻ file tạm thời với các tính năng:

✅ Upload file và tạo link chia sẻ
✅ Thiết lập quyền truy cập (public/password-protected/private)
✅ Thời gian hiệu lực linh hoạt (from/to)
✅ Bảo vệ bằng mật khẩu
✅ Chia sẻ với danh sách người dùng cụ thể
✅ Tự động xóa file hết hạn

📋 Mục lục

🧩 1. Authentication & User Management

`POST /api/auth/register`

Tạo tài khoản mới (không bắt buộc để upload).

Request Body

```
{
  "username": "nam123",
  "email": "nam@example.com",
```

```
  "password": "123456",
  "enableTOTP": true,
  “role”: “user”
}
```

Field	Type	Required	Description
username	string	✅	Tên người dùng (unique)
email	string	✅	Email (unique)
password	string	✅	Mật khẩu (tối thiểu 6 ký tự)
enableTOTP	boolean	❌	Bật xác thực 2FA
role	enum	✅	Phân quyền của người dùng trên hệ thống

Response (200 OK)

```
{
  "message": "User registered successfully",
  "userId": "550e8400-e29b-41d4-a716-446655440000",
  "totpSetup": {
    "secret": "JBSWY3DPEHPK3PXP",
    "qrCode": "..."
  }
}
```

Lưu ý: Quét mã QR bằng Google Authenticator để kích hoạt 2FA.

POST /api/auth/login

Đăng nhập để lấy JWT token.

Request Body

```
{
  "email": "nam@example.com",
  "password": "123456"
}
```

Response (200 OK - không bật TOTP)

```
{
  "accessToken": "eyJhbGciOi...",
  "user": {
    "id": "550e8400-e29b-41d4-a716-446655440000",
    "username": "nam123",
    "email": "nam@example.com"
  }
}
```

Response (200 OK - có TOTP)

```
{
  "requireTOTP": true,
  "message": "TOTP verification required"
}
```

POST /api/auth/login/totp

Xác thực mã TOTP (6 chữ số).

Request Body

```
{
  "email": "nam@example.com",
  "code": "123456"
}
```

Response (200 OK)

```
{
  "accessToken": "eyJhbGciOi...",
  "user": {
    "id": "550e8400-e29b-41d4-a716-446655440000",
    "username": "nam123"
  }
}
```

POST /api/auth/totp/setup

Bật hoặc reset TOTP.

Headers

- `Authorization: Bearer <token>`

Response (200 OK)

```
{
  "message": "TOTP secret generated",
  "totpSetup": {
    "secret": "NB2W45DFOIZA====",
    "qrCode": "..."
  }
}
```

POST /api/auth/totp/verify

Xác minh mã TOTP.

Headers

- `Authorization: Bearer <token>`

Request Body

```
{
  "code": "123456"
}
```

Response (200 OK)

```
{
  "message": "TOTP verified successfully",
  "totpEnabled": true
}
```

`POST /api/auth/logout`

Đăng xuất (client tự xóa token).

Response (200 OK)

```
{ "message": "User logged out" }
```

📁 2. File Management

`POST /api/files/upload`

Upload file mới và tạo share link.

Headers

```
Authorization: Bearer <token>  // optional - nếu không có thì anonymous upload
Content-Type: multipart/form-data
```

Form Data

Field	Type	Required	Description
file	binary	✅	File cần upload
isPublic	boolean	❌	Mặc định `true`
password	string	❌	Mật khẩu bảo vệ (min 6 ký tự)
availableFrom	ISO Date	❌	Thời điểm bắt đầu hiệu lực
availableTo	ISO Date	❌	Thời điểm kết thúc hiệu lực
sharedWith	JSON array	❌	Danh sách email `["user1@example.com"]`
enableTOTP	boolean	❌	Bật xác thực bằng TOTP khi tải file

⚡ **Logic thời gian hiệu lực (Validity Period)**

Trường hợp	Kết quả
Có FROM + TO	Hiệu lực từ FROM đến TO
Chỉ có TO	Hiệu lực từ hiện tại đến TO
Chỉ có FROM	Hiệu lực từ FROM đến FROM + 7 ngày

Không có gì	Hiệu lực từ hiện tại đến +7 ngày (default)

Response (201 Created)


```
{
  "success": true,
  "file": {
    "id": "550e8400-e29b-41d4-a716-446655440000",
    "fileName": "document.pdf",
    "fileSize": 2048576,
    "mimeType": "application/pdf",
    "shareToken": "a1b2c3d4e5f6g7h8",
    "shareLink": "https://example.com/f/a1b2c3d4e5f6g7h8",
    "isPublic": false,
    "hasPassword": true,
    "availableFrom": "2025-11-10T00:00:00Z",
    "availableTo": "2025-11-17T00:00:00Z",
    "validityDays": 7,
    "status": "pending",
    "sharedWith": ["user1@example.com", "user2@example.com"],
    "enableTOTP": false,
    "createdAt": "2025-11-04T12:00:00Z"
  },
  "message": "File uploaded successfully"
}
```

Validation Rules

- ✅ `availableFrom < availableTo` (nếu có cả hai)
- ✅ Khoảng cách tối thiểu: 1 giờ (`system_policy.min_validity_hours`)
- ✅ Khoảng cách tối đa: 30 ngày (`system_policy.max_validity_days`)
- ✅ Mặc định: 7 ngày (`system_policy.default_validity_days`)

Status Codes

Code	Mô tả
201	Upload thành công
400	Validation error
401	Unauthorized
413	File size exceeds limit

GET /api/files/:shareToken

Lấy thông tin file (sử dụng share token).

Response (200 OK)


```
{
  "file": {
    "id": "550e8400-e29b-41d4-a716-446655440000",
    "fileName": "document.pdf",
    "fileSize": 2048576,
    "mimeType": "application/pdf",
    "shareToken": "a1b2c3d4e5f6g7h8",
    "isPublic": false,
    "hasPassword": true,
    "availableFrom": "2025-11-10T00:00:00Z",
    "availableTo": "2025-11-17T00:00:00Z",
    "status": "active",
    "hoursRemaining": 120.5,
    "owner": {
      "id": "owner-uuid",
      "username": "nam123",
      "email": "nam@example.com"
    },
```

- `"sharedWith": ["user1@example.com", "user2@example.com"],`
- `"createdAt": "2025-11-04T12:00:00Z"`
- `}`
- `}`

File Status

Trạng thái	Mô tả
`pending`	Chưa đến `availableFrom`
`active`	Trong thời gian hiệu lực
`expired`	Đã hết hạn (`availableTo` đã qua)

-

`GET /api/files/:shareToken`

Lấy thông tin file (sử dụng share token).

Response (200 OK)

```
{
 "file": {
  "id": "550e8400-e29b-41d4-a716-446655440000",
  "fileName": "document.pdf",
  "fileSize": 2048576,
  "mimeType": "application/pdf",
  "shareToken": "a1b2c3d4e5f6g7h8",
  "isPublic": false,
  "hasPassword": true,
  "availableFrom": "2025-11-10T00:00:00Z",
  "availableTo": "2025-11-17T00:00:00Z",
  "status": "active",
  "hoursRemaining": 120.5,
  "owner": {
```

```
    "id": "owner-uuid",
    "username": "nam123",
    "email": "nam@example.com"
   },
   "sharedWith": ["user1@example.com", "user2@example.com"],
   "createdAt": "2025-11-04T12:00:00Z"
  }
}
```


File Status:

- `pending`: Chưa đến thời gian `availableFrom`
- `active`: Đang trong thời gian hiệu lực
- `expired`: Đã hết hạn (`availableTo` đã qua)

Status Codes:

- `200`: OK
- `404`: File not found
- `410`: File expired (gone)

GET /api/files/:shareToken/download

Tải file về.

Query Parameters

?password=secret123 (nếu file có password)

Headers

Authorization: Bearer <token> (nếu file có sharedWith list)

Response (200 OK - File binary)

Content-Type: application/octet-stream
Content-Disposition: attachment; filename="document.pdf"
Content-Length: 2048576

[binary file data]

Response (403 Forbidden - Sai password)

```
{
  "error": "Incorrect password"
}
```

Response (403 Forbidden - Không trong sharedWith)

```
{
  "error": "Access denied. You don't have permission to download this file."
}
```

Response (423 Locked - Chưa đến thời gian)

```
{
  "error": "File not available yet",
  "availableFrom": "2025-11-10T00:00:00Z",
  "hoursUntilAvailable": 48.5
}
```

Response (410 Gone - Hết hạn)

```
{
  "error": "File expired",
  "expiredAt": "2025-11-17T00:00:00Z"
}
```

Access Control Logic:

1. ✅ Kiểm tra thời gian hiệu lực (FROM - TO)
2. ✅ Nếu có `password_hash` → yêu cầu password đúng
3. ✅ Nếu có `sharedWith` list → yêu cầu user trong danh sách
4. ✅ Nếu `is_public = true` → ai cũng tải được (trong thời gian hiệu lực)

Status Codes:

- `200`: Download success
- `401`: Unauthorized (cần login)
- `403`: Forbidden (sai password hoặc không có quyền)
- `404`: File not found
- `410`: File expired
- `423`: File locked (chưa đến thời gian)

`DELETE /api/files/:id`

Xóa file (chỉ owner hoặc anonymous uploader không thể xóa).

Headers

Authorization: Bearer <token>

Response (200 OK)

```
{
  "message": "File deleted successfully",
  "fileId": "550e8400-e29b-41d4-a716-446655440000"
}
```

Lưu ý:

- Anonymous upload (`owner_id = NULL`) **KHÔNG THỂ XÓA** file sau khi upload
- Chỉ user có `owner_id` mới có quyền xóa file của mình

Status Codes:

- `200`: Deleted successfully
- `403`: Forbidden (không phải owner hoặc anonymous upload)
- `404`: File not found

`GET /api/files/my`

Lấy danh sách file của user đã đăng nhập.

Headers

Authorization: Bearer <token>

Query Parameters

```
?status=active|expired|pending|all  (default: all)
&page=1
&limit=20
&sortBy=createdAt|fileName
&order=asc|desc
```

Response (200 OK)

```
{
```

```
 "files": [
  {
   "id": "file-uuid-1",
   "fileName": "photo.jpg",
   "fileSize": 1048576,
   "shareLink": "https://example.com/f/abc123",
   "shareToken": "abc123",
   "isPublic": true,
   "hasPassword": false,
   "availableFrom": "2025-11-04T00:00:00Z",
   "availableTo": "2025-11-11T00:00:00Z",
   "status": "active",
   "hoursRemaining": 72.5,
   "createdAt": "2025-11-04T00:00:00Z"
  }
 ],
 "pagination": {
  "currentPage": 1,
  "totalPages": 3,
  "totalFiles": 42,
  "limit": 20
 },
 "summary": {
  "activeFiles": 28,
  "pendingFiles": 5,
  "expiredFiles": 9
 }
}
```

POST /api/admin/cleanup

Xóa file hết hạn (Cron job hoặc Admin endpoint).

Headers

X-Cron-Secret: <secret_key>

hoặc

Authorization: Bearer <admin_token>

Response (200 OK)


```
{
 "message": "Cleanup completed",
```

"deletedFiles": 32,
"timestamp": "2025-11-08T00:00:00Z"
}

Logic xóa file:

- Xóa file có `availableTo < NOW`
- Xóa file chỉ có `availableFrom` và `availableFrom + 7 days < NOW`
- Xóa file không có gì và `created_at + 7 days < NOW`

⚙️ 3. Admin / System Management

`GET /api/admin/policy`

Lấy cấu hình hệ thống.

Headers

Authorization: Bearer <admin_token>

Response (200 OK)

{
"id": 1,
"maxFileSizeMB": 50,
"minValidityHours": 1,
"maxValidityDays": 30,
"defaultValidityDays": 7,
"requirePasswordMinLength": 6
}

`PATCH /api/admin/policy`

Cập nhật cấu hình hệ thống.

Headers

Authorization: Bearer <admin_token>

Request Body

```
{
 "maxFileSizeMB": 100,
 "maxValidityDays": 14,
 "defaultValidityDays": 5
}
```

Response (200 OK)

```
{
 "message": "System policy updated successfully",
 "policy": {
  "maxFileSizeMB": 100,
  "maxValidityDays": 14,
  "defaultValidityDays": 5
 }
}
```

🔐 4. Security & Validation

Thời gian hiệu lực (Validity Period)

Logic tính toán:

Input	Kết quả
`FROM=2025-11-10, TO=2025-11-17`	Hiệu lực từ 10/11 đến 17/11 (7 ngày)
`TO=2025-11-15`	Hiệu lực từ **bây giờ** đến 15/11
`FROM=2025-11-10`	Hiệu lực từ 10/11 đến **17/11** (FROM + 7 ngày default)
Không có gì	Hiệu lực từ **bây giờ** đến **7 ngày sau**

Validation rules:

- ✅ `FROM < TO` (nếu có cả hai)
- ✅ Thời gian tối thiểu: 1 giờ
- ✅ Thời gian tối đa: 30 ngày
- ✅ Mặc định: 7 ngày

File status:

```
NOW < FROM          → status: "pending"  (423 Locked)
FROM <= NOW <= TO   → status: "active"   (200 OK)
```

NOW > TO → status: "expired" (410 Gone)

Quyền hạn:

Scenario	Quyền truy cập
Public file (`is_public=true`)	Ai cũng tải được (trong thời gian hiệu lực)
File có password	Nhập đúng password → tải được
File có `sharedWith` list	Chỉ user trong list tải được
Private + password + sharedWith	Phải thỏa CẢ HAI điều kiện
Owner (`owner_id = user_id`)	Có thể xóa file bất kỳ lúc nào
Anonymous upload (`owner_id = NULL`)	**KHÔNG THỂ** quản lý sau khi upload

Anonymous Upload

Đặc điểm:

- `owner_id = NULL` → File không có chủ sở hữu
- Không cần đăng nhập để upload
- **KHÔNG THỂ XÓA** file sau khi upload
- **KHÔNG THỂ QUẢN LÝ** file (delete, etc.)
- File tự động xóa khi hết hạn

Use case:

- Share file tạm thời không cần tài khoản
- One-time file transfer
- Temporary file hosting

Password Protection

Implementation:

- Password được hash bằng **BCrypt** trước khi lưu vào `password_hash`
- Khi download, verify password bằng BCrypt
- Không trả về `password_hash` trong response

- Chỉ trả về `hasPassword: true/false`

Ví dụ:

```
-- Lưu password
UPDATE files
SET password_hash = crypt('secret123', gen_salt('bf'))
WHERE id = 'file-uuid';

-- Verify password
SELECT password_hash = crypt('secret123', password_hash)
FROM files
WHERE id = 'file-uuid';
```

Error Codes

Code	Message	Ý nghĩa
`200`	OK	Success
`201`	Created	Upload thành công
`400`	Bad Request	Validation error
`401`	Unauthorized	Cần đăng nhập
`403`	Forbidden	Sai password hoặc không có quyền
`404`	Not Found	File không tồn tại
`410`	Gone	File đã hết hạn
`413`	Payload Too Large	File quá lớn
`423`	Locked	File chưa đến thời gian hiệu lực

📝 Database Schema Reference

Tables:

1. **users** - User accounts với TOTP 2FA
2. **files** - File metadata với validity period
3. **shared_with** - M:N relationship giữa files và users
4. **system_policy** - Global configuration (singleton)

Key Concepts:

- `owner_id = NULL` → Anonymous upload
- `password_hash` → BCrypt password protection
- `available_from` / `available_to` → Validity period
- `is_public` → Public/Private access
- `share_token` → Unique share link identifier
- `totp_secret` / `totp_enabled` → 2FA authentication