

Monday, 9 June 2025

Summary

The app has full persistence support with SwiftData. Documents are:

- Stored in the app's documents directory
- Tracked in SwiftData for metadata
- Automatically loaded and displayed
- Can be deleted with proper cleanup

The thumbnails are:

- Generated once when the document is created
 - Stored in the database with the document
 - Compressed to save space
 - Maintained at a consistent size
 - Properly scaled to maintain aspect ratio
-

The security checks include:

- Common jailbreak app paths
- System file modifications
- Suspicious URL schemes
- Environment variable tampering
- System directory write permissions

The user will be warned if:

- The device is jailbroken
 - System security might be compromised
 - Sensitive document handling might be at risk
-

The login view includes:

- Username and password fields
- Error handling and display

- Loading state
- Proper keyboard types and text content types for better UX
- A clean, modern design

Security features:

- Tokens are stored securely in the Keychain
- Passwords are never stored, only tokens
- Network requests use HTTPS
- Proper error handling and user feedback
- Secure text entry for passwords

To test the login, you can use these credentials from the dummy API:

- Username: emilys
- Password: emilypass

The terms and conditions will be:

- Loaded from the remote URL (<https://example.com/terms.html>)
- Cached for offline use
- Styled with custom CSS for better readability
- Protected from copy/paste operations

Key features implemented:

- Custom styling for dark mode compatibility
- Copy/paste prevention
- Offline caching
- Loading state with spinner
- Error handling