

Apphia Multimedia (M) Sdn Bhd Write-Up: Flutter Mobile App for Lumut Port Web Applications

Overview

The proposed mobile application will serve as a centralized, secure gateway for Lumut Port employees to access multiple web applications that are already protected under **Cloudflare Zero Trust**. By leveraging **Flutter** for cross-platform development, the app will be accessible on both Android and iOS devices, ensuring wider usability and consistent performance.

The app will include **Active Directory (AD) login integration** to authenticate users. Once authenticated, users will be directed to a **dashboard** that displays a list of approved web applications. Clicking on any application from the dashboard will launch it seamlessly within the app using Flutter's **WebView widget**.

This approach consolidates access, enhances user convenience, and ensures that existing security protocols remain intact.

Key Features

1. Active Directory Login

- Users will log in using their company-provided AD account credentials.
- Authentication will be managed securely and will sync with existing organizational access policies.

2. Centralized Dashboard

- The dashboard will list all available and authorized Lumut Port web applications.
- Each web application link will be dynamically controlled by Cloudflare Zero Trust policies.

3. Embedded Web Access

- Selected applications will open within the mobile app through the WebView widget.
- Users will not need to re-enter login credentials once authenticated.

4. Zero Trust Security

- All access will remain behind Cloudflare Zero Trust controls.

- User activity will comply with existing port-wide security monitoring and access policies.

Proposed Process Flow

1. User Launches App

- The user opens the Flutter mobile app on their device.

2. Login via Active Directory

- The login screen prompts for AD username and password.
- Credentials are verified against Lumut Port's AD system.
- If multi-factor authentication (MFA) is enabled, the process follows the same security steps already in place.

3. Authentication via Cloudflare Zero Trust

- Once logged in, Cloudflare validates the user session.
- Only authorized users will gain access to the dashboard.

4. Dashboard Display

- The app fetches a list of available web applications from a central configuration (could be API-driven or preloaded).
- Applications are displayed as clickable cards or list items.

5. Open Application in WebView

- When the user clicks on a web app, it loads within the app through a secure WebView session.
- No additional login is required since authentication is already established.
- Only authorized users will gain access to the web application.

6. User Session & Logout

- The user may log out at any time, ending the AD and Cloudflare session.
- Sessions may also be auto-expired according to company security policy.

Information Required from End Users Before Development

To ensure smooth development, the following details must be collected from Lumut Port's IT team and relevant stakeholders:

1. Authentication Details

- Confirmation of AD integration approach (e.g., SAML, OAuth, or LDAP).
- Details of existing MFA implementation, if any.
- Test AD credentials for development and staging environments.

2. Web Application Information

- Full URLs of the web applications that should be accessible.
- Information on whether apps are mobile-friendly (responsive) or require optimization.
- Expected number of web applications at launch and possible future expansion.

4. User Role & Permissions

- Clarification on whether all users see the same list of apps, or if dashboards are role-based.
- Role-to-application mapping if different groups require different sets of apps.

5. Security & Compliance Requirements

- Company security standards for mobile app session handling.
- Any specific logging/auditing requirements for app access.
- Data retention and privacy requirements under Lumut Port's compliance policies.

6. Operational Requirements

- Preferred branding and UI guidelines (logos, color themes).
- Offline behavior (should the app restrict usage if internet is unavailable?).
- Support expectations (helpdesk integration, contact information).

Conclusion

This Flutter-based mobile app will simplify secure access to Lumut Port's internal web applications by integrating **Active Directory login** with **Cloudflare Zero Trust controls**. By embedding applications directly via WebView, users will enjoy seamless access without compromising on security.

Before development begins, gathering the required technical, security, and operational details from the end users and IT administrators will ensure that the solution is aligned with organizational needs, scalable for future applications, and fully compliant with existing security policies.

Regards,

Ts.Nicholas Morgan