Authentication Requirements

Session Expirty: Accounts that are not used after a certain period of time should be automatically removed from the active session list.

Session Management: Upon successful authentication, the module should generate a session ID for the user.Each session should have an expiration time to ensure security and prevent unauthorized access.

User Authentication: The module should allow users to authenticate by providing a email and password. User credentials (email and password) should be checked against a known list of valid credentials.

Scability and Performance: The module should be designed to handle a large number of Authentication requests efficiently. It should be scalable to accommodate future growth in user base and system load.

Functinotaly Blocking: The module should provide functionality to block certain features that require authentication. Unauthorized users or users with expired sessions should be blocked from accessing these features.

Security: User passwords should be securely stored and managed. Session IDs should be unique and not predictable.

Error Handling and Reporting: Proper error handling should be implemented to handle invalid authentication attempts, session expirations, and other potential errors.

Testing: Comprehensive unit tests should be developed to ensure the correctness and reliability of the authentication module. Unit Test

Authentication Module Requirements

- ● User Authentication
- ● Session Management
- ● Session Expiry
- ● Functinotaly Blocking
- ● Security
- ● Scalability and Performance
- ● Error Handling and Reporting
- ● Testing