Core Components Requirements

Security

Authentication

Purpose:

A mechanism for identifying a valid user of the system

Scope:

Any user attempting to use the system

Requirements:

- The user must provide a valid security credentials whenever attempting to authenticate with the system
- Valid security credentials consist of a valid username and valid time-based one-time password (OTP)
  - Valid usernames will consist of the following:
    i. a-z
    ii. 0-9
    iii. .,@!
  - OTP is defined in NIST SP 800-63b section 5.1.4.1
    i. OTP is changed upon every successful use
    ii. OTP expires every 2 minutes
    iii. OTP must be at minimum 8 characters
    iv. Valid characters will consist of the following:
      a. a-z
      b. A-Z
      c. 0-9
- A maximum of 5 failed authentication attempts within 24 hours for the same account before account is disabled
  - 24 hour timer begins on the first failed authentication. If the account was not disabled after 24 hours, then the the fail count resets to 0.
  - Account is locked until a valid account recovery is performed by user or by system admin. Upon successful account recovery, the failed count resets to 0.
  - For each failed attempt, the account undergoing authentication and the IP address that initiated the authentication request will be recorded.
- System failures from this feature must not result in the system going offline

Use Cases:

- Pre-conditions
  - User must not already have an active authenticated session with the system on the current device, otherwise authentication is not possible.
  - User must be on login view or attempting to access to a protected resource as defined in Authorization
- Success
  1. User submits valid security credentials. The user is automatically navigated to the user's home view.

- Failure Cases
    1. User submits valid security credentials. Automatic navigation does not take place.
    2. User submits valid security credentials. The user is automatically navigated to a view other than the user's home view.
    3. User submits invalid username. A system message displays "Invalid username or password provided. Retry again or contact system administrator".
    4. User submits invalid OTP. A system message displays "Invalid username or password provided. Retry again or contact system administrator if issue persists".
    5. User submits invalid security credentials. A system message displays "Invalid username or password provided. Retry again or contact system admin".
    6. User submits valid security credentials for a disabled account. A system message displays "Account disabled. Perform account recovery or contact system admin". The failure attempt is recorded accurately.
    7. User submits valid security credentials for a disabled account. A system message displays "Account disabled. Perform account recovery or contact system admin". The failure attempt is not recorded accurately. The system attempts to log that the failure attempt did not complete successfully.

Authorization

Purpose:

A mechanism for restricting access to protected resources (e.g. functionalities, data, and views) to only valid users

Scope:

Any user attempting to use the system

Requirements:

- By default, unauthenticated users will only be given access to resources or functionalities that does not require knowledge of user's identity
- The operation and timestamp of each unauthorized access will be recorded by the system
- The system must prevent unauthorized users from viewing, modifying or deleting any protected data (scalar or aggregate data)
- The system must prevent unauthorized users from executing any protected functionality
- The system must prevent unauthorized users from viewing or interacting with any protected views
- Any user access modifications should be active upon the next successful authentication by user
- System failures from this feature must not result in the system going offline

Use Cases:

- Pre-conditions
    - User must be authenticated to enforce user-specific restrictions
    - User account must be active

- Success
    1. User attempts to access a protected functionality within authorization scope. Access is granted to perform functionality.
    2. User attempts to access protected data within authorization scope. Access is granted to perform read operations.
    3. User attempts to modify protected data within authorization scope. Access is granted to perform write operations.
    4. User attempts to access protected views within authorization scope. Access is granted to the view. User is automatically navigated to view.
- Failure Cases
    1. Unauthorized access is not recorded by system when authorization fails. A system log of failure is attempted.
    2. User attempts to access a protected functionality outside of authorization scope. Access is denied and a system message displays “Unauthorized access”.
    3. User attempts to access protected data outside of authorization scope. Access is denied and a system message displays “Unauthorized access to data”.
    4. User attempts to modify protected data outside of authorization scope. Access is denied and a system message displays “Unauthorized access to data”.
    5. User attempts to access protected views outside of authorization scope. Access is denied and a system message displays “Unauthorized access to view”.
    6. User attempts to access protected views within authorization scope, but contains protected data that is not within read scope. Access is granted to the view. Upon completion of automatic navigation to view, a system message displays “Unauthorized access to data” with protected data not visible within the view.
    7. User attempts to access protected views within authorization scope, but contains protected data that is not within write scope. Access is granted to the view. Upon completion of automatic navigation to view, protected data is visible within the view. Attempts to modify the data will result in a system message that displays “Unauthorized access to data”

Logout

Purpose:

A mechanism for ending an active authenticated session

Scope:

Any active authenticated user

Requirements:

- The current active session on the device will end within 5 seconds upon invocation
- The user will be navigated to the home view of the system upon successful completion
- System failures from this feature must not result in the system going offline

Use Cases:

- Pre-conditions
  - User must have an active authenticated session on the device, otherwise the user is unable to perform the operation
  - User must be on view with Logout option
- Success
  1. User performs logout request. The active session ends. The user is automatically navigated to the default home view of the system with the default culture settings. A system message displays “Logout successfully” upon completion of automatic navigation to home view. The logout process completes within 5 seconds upon invocation.
- Failure Cases
  1. User performs logout request. The active session has ended. The user is not automatically navigated to the default home view. A system message displays “Logout operation error” or no message is shown
  2. User performs logout request. The active session has ended. The user is automatically navigated to the default home view, but not set to the default culture settings. A system message displays “Logout operation error” or no message is shown
  3. The logout process takes longer than 5 seconds.

User Administration

Account Creation (Registration)

Purpose:

A mechanism for creating new user accounts within the system

Scope:

Any user attempting to use the system

Requirements:

- System administrators cannot be created using Account Creation feature
- All user accounts must be stored in a persistent data store
- The user provides a valid email address that belongs to the user.
- The user provides a secret passphrase for requesting OTP
  - Secret passphrase must be a minimum of 8 characters
  - Valid characters will consist of the following:
    i. blank space
    ii. a-z
    iii. A-Z
    iv. 0-9
    v. .,@!
- The user is given a system-wide unique username upon validation of email
  - Valid characters will consist of the following:
    i. a-z
    ii. 0-9
    iii. .,@!

- A unique URL link is provided for every account creation request
- The URL link is valid for only 24 hours from date of account creation request
- System failures from this feature must not result in the system going offline

Use Cases:

- Pre-conditions
  - User must not have an active authenticated session
  - User must be on account creation view
- Success
  1. User registers with a valid email and valid passphrase. A system message displays “Email confirmation pending”. The user receives a confirmation email within 15 seconds upon invocation of system message. The user completes email confirmation within 24 hours. User is notified of username. A system message displays “Account created successfully”
- Failure Cases
  1. User registers with an invalid email or invalid passphrase. A system message displays “Account creation error. Retry again or contact system administrator” or no system message.
  2. User registers with a valid email and valid passphrase. A system message displays “Email confirmation pending”. The user does not receives a confirmation email at all or an email within 15 seconds upon invocation of system message.
  3. User registers with a valid email and valid passphrase. A system message displays “Email confirmation pending”. The user receives an email confirmation within 15 seconds upon invocation of system message. The user does not complete email confirmation within 24 hours.
  4. User registers with a valid email and valid passphrase. A system message displays “Email confirmation pending”. The user receives an email confirmation within 15 seconds upon invocation of system message. The user completes email confirmation within 24 hours. User is not notified of username
  5. User registers with a valid email and valid passphrase. A system message displays “Email confirmation pending”. The user receives an email confirmation within 15 seconds upon invocation of system message. The user completes email confirmation within 24 hours. User is notified of username. A system message does not display
  6. User registers with a valid email and valid passphrase. A system message displays “Email confirmation pending”. The user receives an email confirmation within 15 seconds upon invocation of system message. The user completes email confirmation within 24 hours. User is notified of username. A system message displays “Account created successfully”, but account is not created and stored in the data store

Account Recovery

Purpose:

A mechanism for regaining access to an active or disabled account

Scope:

Any registered user

Requirements:

- The user must provide a valid username and associated email to receive a system email containing a recovery URL link
- The user must receive recovery email within 15 seconds upon invocation
- Recovery URL link must be navigated to and completed within 24 hours, otherwise a new recovery request must be started
- A maximum of 5 recovery requests can be made per account per calendar month.
- Recovery request limit resets every 00:00:00AM local time on the 1st of the month.
- System failures from this feature must not result in the system going offline

Use Cases:

- Pre-conditions
  - User must not have an active authenticated session on the device, otherwise the user is unable to perform the operation
  - User must be on account recovery view
- Success
  1. User provides valid username and associated email. User receives recovery email within 15 seconds. User completes recovery request within 24 hours. A system message displays “Account recovery completed successfully” within 5 seconds of completion.
- Failure Cases
  1. User provides invalid username. A system message displays “Account recovery error” or no system message
  2. User provides valid username, but invalid email. A system message displays “Account recovery error” or no system message
  3. User provides valid username and email. User does not receive recovery email.
  4. User provides valid username and email. User does not receive recovery email within 15 seconds.
  5. User provides valid username and associated email. User receives recovery email within 15 seconds. User does not complete recovery request within 24 hours.
  6. User provides valid username and associated email. User receives recovery email within 15 seconds. User completes recovery request within 24 hours. A system message does not show or a system message displays “Account recovery error”

Account Deletion

Purpose:

A mechanism for deleting a user account

Scope:

Any registered user of the system

Requirements:

- Only a system administrator account can delete another system administrator account
- All personal identifiable information (PII) along with the user account data is permanently deleted from the system
- Account deletion is irreversible
- System failures from this feature must not result in the system going offline

Use Cases:

- Pre-conditions
  - User must have an active authenticated session
  - User must be on account deletion view
  - User has permission to delete account
- Success
  1. User choses to delete account and confirms action. All PII data and user account data is permanently deleted from the system. A system message displays “Account deletion successful”. Upon acknowledgment of system message, the user is automatically navigated to the home view with default language and culture settings.
- Failure Cases
  1. User choses to delete account and confirms action, but system does not delete both PII data or user account data.
  2. Data is not permanently deleted from the system.
  3. A system message is not shown or the wrong message is shown after all PII data and user account data is permanently deleted from the system
  4. The user is unable to acknowledge the system message “Account deletion successful” after the successful data deletion.
  5. The user user is not automatically redirected to the default home view of the system.
  6. The user is automatically redirected to the default home view, but the default language and culture setting is not shown.

User Management

Purpose:

A mechanism for administration of any user account

Scope:

Any system administrator user

Requirements:

- All operations are applied to a persistent data store
- Only system administrator have access to the User Management view
- The system administrator will have access to view and modify all accounts and their associated user profile data within the system
- Single Operation
  - Create Account
  - Update Account
  - Delete Account
  - Disable Account
  - Enable Account

    - Operation should be completed within 5 seconds upon invocation
  - Bulk Operation
    - Multiple operations (e.g. all the same or mixed) within the same request
    - Maximum of 10K operations per request
    - Requests can be made through an uploaded file extract
    - File extract cannot be greater than 2GB in size
    - Operation should be completed within 60 seconds
  - All single and bulk operations must be able to affect any user account/profile attribute within the system
  - Only a system administrator account can create other system administrator accounts
  - The system must have at least one system administrator account with total system access at all times
  - System failures from this feature must not result in the system going offline

Use Cases:

  - Pre-conditions
    - User must have an active authenticated session
    - User must be on user management view
    - User must be a system administrator
  - Success
    1. User is able to perform any single UM operation within 5 seconds upon invocation. A system message displays “UM operation was successful”
    2. User is able to perform less than 10K UM operations in bulk within 60 seconds. A system message displays “Bulk UM operation was successful”
    3. User is able to perform 10K UM operations in bulk within 60 seconds. A system message displays “Bulk UM operation was successful”
  - Failure Cases
    1. Single UM operation takes longer than 5 seconds
    2. Bulk UM operations takes longer than 60 seconds
    3. Single UM operation completes within 5 seconds, but no system message is shown or inaccurate system message is shown
    4. Bulk UM operations completes within 60 seconds, but no system message is shown or inaccurate system message is shown
    5. Single UM operation completes within 5 seconds, with system message “UM operation was successful” shown, but latest data is not written to data store
    6. Bulk UM operations completes within 60 seconds, with system message “Bulk UM operation was successful” shown, but latest data is not written to data store
    7. 10K Bulk UM operations completes takes longer than 60 seconds
    8. 10K Bulk UM operations completes within 60s seconds, but no system message is shown or inaccurate system message is shown
    9. 10K Bulk UM operations completes within 60 seconds, with system message “Bulk UM operation was successful” shown, but latest data is not written to data store

System Observability

Usage Analysis Dashboard

Purpose:

A visualization mechanism for gaining insight on user behavior within system

Scope:

Any system administrator account of the system

Requirements:

- All data must be fetched from a persistent data store
- Key Performance Indicators (KPIs)
  - The top 5 most visited view of all time (bar chart)
  - The top 5 average duration per view of all time (bar chart)
  - The number of logins per day within the span of 3 months (trend chart)
  - The number of registrations per day within the span of 3 month (trend chart)
  - Two application specific feature metric
- All KPI data must be automatically refreshed in intervals of 60 seconds
- The view must load within 15 seconds upon completion of navigation.
- System failures from this feature must not result in the system going offline

Use Cases:

- Pre-conditions
  - Persistent data store must be active
  - Persistent data store must accessible by the system
  - User must have an active authenticated session on the device
  - User must be on Usage Analysis Dashboard view
  - User must be a system administrator
- Success
  1. User is able to navigate to the view. The view loads within 15 seconds. All KPIs automatically refreshes data within 60 seconds.
- Failure Cases
  1. User is unable to navigate to the page, but is a system administrator
  2. User is able to navigate to the page, but view does not load within 15 seconds upon navigation completion.
  3. User is able to navigate to the page, view loads within 15 seconds, but no KPI data is refreshed.
  4. User is able to navigate to the page, view loads within 15 seconds, but not all KPI data is refreshed.
  5. User is able to navigate to the page, view loads within 15 seconds, but all KPI refresh takes longer than 60 seconds.

Logging

Purpose:

An internal mechanism for tracking all events of the system for auditing

Scope:

All system-initiated and user-initiated events within the system

Requirements:

- All log entries must be immutable
- All log entries must be saved to a persistent data store
- All log entries must contain a UTC timestamp, log level, user performing operation, a category and a description/message
- Valid Log Levels
    i. Info - for tracking flow of system
    ii. Debug - for tracking key information crucial to maintainers of the system
    iii. Warning - for tracking events that may lead to system failures
    iv. Error - for tracking system errors
- Valid Categories
    i. View
    ii. Business
    iii. Server
    iv. Data
    v. Data Store
- The logging process must not block any user from performing any interaction with the system
- The logging process must complete within 5 seconds upon invocation
- System failures from this feature must not result in the system going offline

Use Cases:

- Pre-conditions
    - Persistent data store must be active
    - Persistent data store must accessible by the system
    - Persistent data store must have storage capacity for log entry
- Success
    1. The system logs system success events
    2. The system logs system failure events
    3. The system logs user success events
    4. The system logs user failure events
- Failure Cases
    1. The logging process took longer than 5 seconds to complete upon invocation
    2. The logging process blocks a user from interacting with the system
    3. The logging process completes within 5 seconds, but did not save to a persistent date store
    4. The logging process completes within 5 seconds, but did not accurately save the event to the persistent data store (i.e. timestamp, log level, category, message, etc.)
    5. Previously saved log entries are modifiable

Archiving

Purpose:

An internal mechanism for offloading log entries to preserve system resources

Scope:

All log entries within the system

Requirements:

- Archival process must execute every 00:00:00AM (local time) on 1st of the month
- Archival process must only offload log entries that are older than 30 days
- Archival process must consolidate and compress entries being archived
- Archival process must offload entries to another location
- Archival process must remove offloaded entries from the system after successful archival
- Archival process must complete within 60 seconds upon invocation
- System failures from this feature must not result in the system going offline

Use Cases:

- Pre-conditions
  - Persistent data store must be active
  - Persistent data store must accessible by the system
  - Archival destination location must have storage capacity
- Success
  1. Archival process executes at 00:00:00AM (local time) on the 1st of the month. All log entries older than 30 days are consolidated, compressed and relocated to another location. All archived logs are removed from the system. The entire archival process completes within 60 seconds upon invocation.
- Failure Cases
  1. Archival process did not start at 00:00:00AM
  2. Archival process started at 00:00:00AM, but not local time
  3. Archival process started at 00:00:00AM (local time), but not on the 1st of the month
  4. Archival process started at 00:00:00AM (local time) on the 1st of the month, but did not archive any log entries even though there are logs older than 30 days
  5. Archival process started at 00:00:00AM (local time) on the 1st of the month, but did not archive all log entries older than 30 days
  6. Archival process started at 00:00:00AM (local time) on the 1st of the month. All log entries older than 30 days are not consolidated.
  7. Archival process started at 00:00:00AM (local time) on the 1st of the month. All log entries older than 30 days are consolidated, but are not compressed.
  8. Archival process started at 00:00:00AM (local time) on the 1st of the month. All log entries older than 30 days are consolidated and compressed, but is not relocated to another location
  9. Archival process started at 00:00:00AM (local time) on the 1st of the month. All log entries older than 30 days are consolidated, compressed and is relocated to another location, but archived logs are not removed from the system.
  10. Archival process took longer than 60 seconds to complete upon invocation.

Project Criteria Requirements

Universal Requirements

User Privacy
Purpose:
A mechanism to inform and protect user data from being used without consent
Scope:
All user related data within the system
Requirements:
- EULA per GDPR or California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)
- Opt-out of user data collection and selling of user data
- Explanation of use of data
- Deletion of user data / user account

Error Handling
Purpose:
A mechanism to prevent system failures from making the system go offline to any user
Scope:
Entire system
Requirements:
- Allowed System Failures:
    i. Web Server loses internet access
    ii. Cloud/Host Provider outage
- System failures from this feature must not result in the system going offline

UI / UX
Purpose:
To provide an intuitive interface for users to interact with the system
Scope:
All features that requires user interaction within the system
Requirements:
- All text must be in the selected language and culture setting
- All formats align with the selected unit of measurement
- All views must not require assistance from another human understand how to interact with the view

- All system messages to the user must be displayed in the default culture settings for non-Authenticated users and the selected culture settings for Authenticated users
- All system messages must appear within 5 seconds of the resolution of an operation
- System failures from this feature must not result in the system going offline

Documentation

Purpose:

To provide artifacts that describe the system in detail

Scope:

All features within the system

Requirements:

- Low-level design documents
- User Manuals
- FAQs