项目文档

# Functional Requirement

1.1 Asset Registration Function   
 Function ID: FR-01   
 Description: Users can register new assets by entering required information. The system must validate the data, create a new asset record, and initiate the approval workflow.   
 Input: Asset details (Name, Description, Category, Status, Location, PurchaseDate, Value).   
 Output: A new asset record in the Asset entity, an updated AssetUsageRecord, initiation of an AssetApprovalWorkflow, and an email notification sent to the Administrator.  
  
1.2 View Asset Information Function   
 Function ID: FR-02   
 Description: Users can view the details of a specific asset. The system retrieves the asset record and optionally the associated usage record.   
 Input: Asset ID or selection from the asset list.   
 Output: Displayed asset information (Name, Description, Category, Status, Location, PurchaseDate, Value), and optionally the associated AssetUsageRecord.  
  
1.3 Modify Asset Details Function   
 Function ID: FR-03   
 Description: Users can modify the details of an existing asset. The system must validate the updated data, update the asset record, and initiate an approval workflow.   
 Input: Asset ID or selection from the asset list, updated asset details (Name, Description, Category, Status, Location, PurchaseDate, Value).   
 Output: Updated asset record in the Asset entity, updated AssetUsageRecord if necessary, initiation of an AssetApprovalWorkflow, and an email notification sent to the Administrator.  
  
1.4 Delete Asset Record Function   
 Function ID: FR-04   
 Description: Users can delete an asset record. The system must confirm the deletion, remove the asset record, update the usage record, and initiate an approval workflow.   
 Input: Asset ID or selection from the asset list, confirmation of deletion.   
 Output: Deleted asset record from the Asset entity, updated or deleted AssetUsageRecord, initiation of an AssetApprovalWorkflow, and an email notification sent to the Administrator.  
  
1.5 Initiate Asset Approval Function   
 Function ID: FR-05   
 Description: Users can initiate the approval workflow for an asset. The system creates a new approval workflow and sends a notification to the administrator.   
 Input: Asset ID or selection from the asset list, confirmation to initiate approval.   
 Output: A new AssetApprovalWorkflow record, email notification to the Administrator, and audit log entry.  
  
1.6 View Asset Approval Function   
 Function ID: FR-06   
 Description: Users can view the approval status and details of a specific asset. The system retrieves and displays the approval workflow information.   
 Input: Asset ID or selection from the asset list.   
 Output: Displayed approval status, current step, and any relevant comments or actions from the AssetApprovalWorkflow entity.  
  
1.7 Create Asset Usage Record Function   
 Function ID: FR-07   
 Description: Users can create a new asset usage record for a specific asset. The system must validate the usage details, create the record, and initiate an approval workflow.   
 Input: Asset ID or selection from the asset list, usage details (UsageDate, UsageDetails, Status).   
 Output: A new AssetUsageRecord linked to the selected Asset, initiation of an AssetApprovalWorkflow, and an email notification sent to the Administrator.  
  
1.8 View Asset Usage History Function   
 Function ID: FR-08   
 Description: Users can view the usage history of a specific asset. The system retrieves and displays all AssetUsageRecords associated with the asset.   
 Input: Asset ID or selection from the asset list.   
 Output: Displayed usage history (UsageDate, UsageDetails, Status), and audit log entry.  
  
1.9 Update Asset Usage Status Function   
 Function ID: FR-09   
 Description: Users can update the status of an existing asset usage record. The system must validate the new status, update the record, and initiate an approval workflow.   
 Input: AssetUsageRecord ID or selection from the usage record list, new status (e.g., "In Use", "Available", "Maintenance").   
 Output: Updated AssetUsageRecord, initiation of an AssetApprovalWorkflow, and an email notification sent to the Administrator.  
  
1.10 Delete Usage Record Function   
 Function ID: FR-10   
 Description: Users can delete an asset usage record. The system must confirm the deletion, remove the record, and send a notification to the administrator.   
 Input: AssetUsageRecord ID or selection from the usage record list, confirmation of deletion.   
 Output: Deleted AssetUsageRecord, email notification to the Administrator, and audit log entry.  
  
1.11 User Login Function   
 Function ID: FR-11   
 Description: Users can authenticate and log in to the system. The system validates the credentials, initiates a session, and logs the login activity.   
 Input: Username and password.   
 Output: Initiated session, redirected to the appropriate interface based on user role, and audit log entry.  
  
1.12 User Registration Function   
 Function ID: FR-12   
 Description: Administrators can register new users by entering their details. The system must validate the data, create the user record, assign permissions, and send a confirmation email.   
 Input: User details (Name, Email, Role).   
 Output: A new User record, assigned Permission, email notification to the new user, and audit log entry.  
  
1.13 Manage User Permissions Function   
 Function ID: FR-13   
 Description: Administrators can assign, modify, or revoke permissions for users. The system updates the user's permissions and logs the activity.   
 Input: UserID, PermissionID, new permission settings.   
 Output: Updated PermissionAssignment record, email notification to the user and/or administrator, and audit log entry.  
  
1.14 View User List Function   
 Function ID: FR-14   
 Description: Administrators can view the list of all registered users. The system retrieves and displays the user data, and logs the activity.   
 Input: None (system retrieves all users).   
 Output: Displayed list of users (UserID, Name, Email, Role, RegistrationDate, LastLogin), and audit log entry.  
  
1.15 Manage Administrator Account Function   
 Function ID: FR-15   
 Description: Administrators can manage other administrator accounts by creating, modifying, or deleting them. The system validates the action and logs the activity.   
 Input: Admin details (Name, Email, Role), action (create, modify, delete).   
 Output: Updated Administrator record, email notification to the administrator, and audit log entry.  
  
1.16 Generate Asset Report Function   
 Function ID: FR-16   
 Description: Administrators can generate reports based on asset and usage data. The system must aggregate the data and provide the report in a user-friendly format.   
 Input: Report type, filters (e.g., asset type, location, date range).   
 Output: Generated ReportAnalysis with aggregated data, display in table/chart format, and audit log entry.  
  
1.17 View Report Analysis Function   
 Function ID: FR-17   
 Description: Users or administrators can view detailed analysis reports. The system retrieves and displays the report data, and logs the activity.   
 Input: Report ID or selection from the report list.   
 Output: Displayed report content (Title, Description, GenerationDate, Content), and audit log entry.  
  
1.18 Export Asset Data Function   
 Function ID: FR-18   
 Description: Administrators can export asset data in a selected format. The system must retrieve the data, format it, and make it available for download.   
 Input: Export type (e.g., all assets, specific types), filters (e.g., location, status), export format (e.g., PDF, Excel, CSV).   
 Output: Exported file ready for download, audit log entry, and email notification to the Administrator.  
  
1.19 Import Asset Data Function   
 Function ID: FR-19   
 Description: Administrators can import asset data from a file. The system must validate the file format and structure, and import the data into the system.   
 Input: Data file (e.g., CSV or Excel), type of data to import (e.g., asset records).   
 Output: Imported asset records stored in the database, audit log entry, and email notification to the Administrator.  
  
1.20 Send Email Notification Function   
 Function ID: FR-20   
 Description: The system can send email notifications for various events (e.g., asset registration, approval, or permission changes).   
 Input: Event details (AssetID, UserID, action type), recipient (Administrator), email content.   
 Output: EmailNotification sent to the recipient, audit log entry, and confirmation of delivery.  
  
1.21 View Email Notification History Function   
 Function ID: FR-21   
 Description: Users or administrators can view the history of sent and failed email notifications. The system retrieves and displays the notifications, and logs the activity.   
 Input: Filters (e.g., date, recipient, event type).   
 Output: Displayed EmailNotification records (Subject, Content, SendDate, Status), and audit log entry.  
  
1.22 Audit System Logs Function   
 Function ID: FR-22   
 Description: Administrators can view and filter audit logs to monitor system activities. The system retrieves and displays the logs, and logs the access activity.   
 Input: Filters (e.g., date, user, action type).   
 Output: Displayed AuditLog entries (UserID, Action, Timestamp, Details), and audit log entry for the access.  
  
1.23 Manage Login Record Function   
 Function ID: FR-23   
 Description: Administrators can manage login records, including viewing, filtering, and deleting them. The system logs the management activity.   
 Input: Action (view, filter, delete), filters (e.g., user, date, login status).   
 Output: Displayed LoginRecord entries (UserID, Timestamp, Status), and audit log entry for the management action.  
  
1.24 Manage User Registration Function   
 Function ID: FR-24   
 Description: Administrators can manage the user registration process, including enabling/disabling self-registration and setting validation rules.   
 Input: Configuration settings (e.g., enable/disable self-registration, validation rules, default roles).   
 Output: Updated UserRegistration configuration, audit log entry, and email notification to the Administrator.  
  
1.25 Manage Permission Assignment Function   
 Function ID: FR-25   
 Description: Administrators can assign or modify permissions for users or roles. The system validates the permissions and logs the assignment activity.   
 Input: UserID or Role, PermissionID, new permission settings.   
 Output: Updated PermissionAssignment record, audit log entry, and email notification to the Administrator.  
  
1.26 Manage Report Analysis Function   
 Function ID: FR-26   
 Description: Administrators can configure and manage report analysis settings, including report templates and data aggregation rules.   
 Input: Report analysis settings (e.g., templates, rules, schedules).   
 Output: Updated ReportAnalysis configuration, audit log entry, and email notification to the Administrator.

# External Description

2. External Interfaces  
  
2.1 User Interface Output   
The system interacts with users through a graphical user interface (GUI) that provides the following features:   
- \*\*Asset Management Screens\*\*: Allow users to register, modify, delete, and view asset records, including Name, Description, Category, Status, Location, PurchaseDate, and Value.   
- \*\*Usage Record Screens\*\*: Enable users to create, update, and delete asset usage records, displaying UsageDate, UsageDetails, and Status.   
- \*\*Approval Workflow Screens\*\*: Show the approval status and details of an asset, including the current step and any relevant comments or actions.   
- \*\*User Management Screens\*\*: Provide administrators with the ability to register new users, manage permissions, view user lists, and manage administrator accounts.   
- \*\*Report Generation and Analysis Screens\*\*: Allow administrators to generate and view reports based on aggregated asset and usage data, with options to display in table or chart formats.   
- \*\*Login and Registration Screens\*\*: Support user authentication and new user registration, with fields for Username, Password, Name, Email, and Role.   
- \*\*Email Notification History Screen\*\*: Displays a list of sent and failed email notifications, including Subject, Content, SendDate, and Status.   
- \*\*Audit Log Screen\*\*: Enables administrators to view and filter audit logs, displaying UserID, Action, Timestamp, and Details.   
- \*\*Export and Import Screens\*\*: Allow administrators to export asset data in formats such as PDF, Excel, or CSV, and import data from files like CSV or Excel.   
- \*\*Configuration Screens\*\*: Provide administrators with the ability to manage system settings, including user registration rules, permission assignments, and report analysis templates.   
- \*\*Email Notification Settings Screen\*\*: Enables administrators to configure email notification templates and delivery rules.   
- \*\*Data Input Forms\*\*: Used for capturing and validating asset and usage details, ensuring data integrity before processing.   
- \*\*Confirmation Dialogs\*\*: Prompt users to confirm actions such as asset or usage record deletion.   
- \*\*Notification Panels\*\*: Display system-generated messages or alerts, such as successful asset registration or workflow initiation.   
- \*\*Dashboard Views\*\*: Provide an overview of asset status, usage trends, and user activity for quick access to critical information.   
  
These interfaces are designed to be intuitive and user-friendly, allowing users to perform actions and receive feedback efficiently.  
  
2.2 Hardware Interface Output   
This system does not have direct hardware interfaces. However, it may be accessed via various hardware devices such as desktop computers, laptops, tablets, and mobile phones. The system is designed to be compatible with standard input/output devices, including keyboards, mice, touchscreens, and printers, to support asset data export and report printing.   
The system does not require any specialized hardware for its core operations and relies on standard computing hardware for execution.  
  
2.3 Software Interface Output   
The system interacts with several software components and external data sources, which are described as follows:   
  
- \*\*Asset Database (Asset Entity)\*\*:   
 \*\*Role\*\*: Stores all asset records, including Name, Description, Category, Status, Location, PurchaseDate, and Value.   
 \*\*Interaction Method\*\*: The system writes and reads data from this database when assets are registered, modified, or deleted.   
 \*\*Input/Output\*\*:   
 - Input: Asset details for registration or modification.   
 - Output: Updated or newly created asset records, and audit log entries.   
  
- \*\*AssetUsageRecord Database\*\*   
 \*\*Role\*\*: Tracks the usage history of assets, including UsageDate, UsageDetails, and Status.   
 \*\*Interaction Method\*\*: The system reads and updates this database when viewing, creating, modifying, or deleting usage records.   
 \*\*Input/Output\*\*:   
 - Input: Usage details and asset ID for new usage records.   
 - Output: Updated or newly created usage records, and audit log entries.   
  
- \*\*AssetApprovalWorkflow Database\*\*   
 \*\*Role\*\*: Manages the approval workflow for asset-related actions, including the current step, comments, and status.   
 \*\*Interaction Method\*\*: The system creates, updates, and retrieves workflow records when initiating or viewing approval workflows.   
 \*\*Input/Output\*\*:   
 - Input: Asset or usage record ID and confirmation to initiate approval.   
 - Output: Updated or newly created workflow records, and audit log entries.   
  
- \*\*User Database (User Entity)\*\*   
 \*\*Role\*\*: Stores user information, including UserID, Name, Email, Role, RegistrationDate, and LastLogin.   
 \*\*Interaction Method\*\*: The system reads and writes user data during login, registration, and management functions.   
 \*\*Input/Output\*\*:   
 - Input: User details for registration or modification.   
 - Output: Updated or newly created user records, and audit log entries.   
  
- \*\*PermissionAssignment Database\*\*   
 \*\*Role\*\*: Manages user or role-based permissions, including PermissionID and assigned settings.   
 \*\*Interaction Method\*\*: The system updates this database when permissions are assigned, modified, or revoked.   
 \*\*Input/Output\*\*:   
 - Input: UserID or Role, PermissionID, and new permission settings.   
 - Output: Updated permission assignments and audit log entries.   
  
- \*\*Email Notification System\*\*   
 \*\*Role\*\*: Sends and logs email notifications for various events such as asset registration, approval, and permission changes.   
 \*\*Interaction Method\*\*: The system sends emails to designated recipients (e.g., Administrators) and logs the status of each notification.   
 \*\*Input/Output\*\*:   
 - Input: Event details (AssetID, UserID, action type), recipient (Administrator), and email content.   
 - Output: EmailNotification records (Subject, Content, SendDate, Status) and audit log entries.   
  
- \*\*AuditLog Database\*\*   
 \*\*Role\*\*: Logs all system activities for audit purposes, including UserID, Action, Timestamp, and Details.   
 \*\*Interaction Method\*\*: The system writes to this database whenever an action is performed, including login, asset management, usage record management, and configuration changes.   
 \*\*Input/Output\*\*:   
 - Input: Action details (e.g., "Asset Modified", "User Registered").   
 - Output: AuditLog entries and additional logs for access and management actions.   
  
- \*\*ReportAnalysis Database\*\*   
 \*\*Role\*\*: Stores generated reports and their aggregated data for viewing and analysis.   
 \*\*Interaction Method\*\*: The system writes to this database when reports are generated and reads from it when reports are viewed.   
 \*\*Input/Output\*\*:   
 - Input: Report type, filters (e.g., asset type, location, date range), and export format.   
 - Output: Generated ReportAnalysis records and audit log entries.   
  
- \*\*LoginRecord Database\*\*   
 \*\*Role\*\*: Stores login records, including UserID, Timestamp, and Status.   
 \*\*Interaction Method\*\*: The system writes login activity to this database and allows administrators to view and manage these records.   
 \*\*Input/Output\*\*:   
 - Input: Action (view, filter, delete) and filters (e.g., user, date, login status).   
 - Output: Displayed LoginRecord entries and audit log entries for management actions.   
  
- \*\*UserRegistration Configuration Database\*\*   
 \*\*Role\*\*: Stores system-wide configuration settings for user registration, such as enable/disable self-registration and validation rules.   
 \*\*Interaction Method\*\*: The system updates this configuration when administrators change user registration settings.   
 \*\*Input/Output\*\*:   
 - Input: Configuration settings (e.g., enable/disable self-registration, validation rules, default roles).   
 - Output: Updated UserRegistration configuration and audit log entries.   
  
- \*\*ReportAnalysis Configuration Database\*\*   
 \*\*Role\*\*: Stores report analysis settings, including templates, data aggregation rules, and schedules.   
 \*\*Interaction Method\*\*: The system updates this configuration when administrators modify report analysis settings.   
 \*\*Input/Output\*\*:   
 - Input: Report analysis settings (e.g., templates, rules, schedules).   
 - Output: Updated ReportAnalysis configuration and audit log entries.   
  
2.4 Communication Interface Output   
The system communicates with external entities through the following interfaces:   
  
- \*\*Email Communication Interface\*\*   
 \*\*Role\*\*: Sends email notifications to administrators and users for events such as asset registration, approval, permission changes, and data export/import.   
 \*\*Interaction Method\*\*: The system uses this interface to send emails and log their status.   
 \*\*Input/Output\*\*:   
 - Input: Recipient (Administrator), email content (Subject and Content), and event details (AssetID, UserID, action type).   
 - Output: Confirmation of email delivery, and audit log entries for email notifications.   
  
- \*\*Web Communication Interface\*\*   
 \*\*Role\*\*: Supports access to the system via web browsers, allowing users to interact with the GUI and perform asset and user management tasks.   
 \*\*Interaction Method\*\*: The system communicates through HTTP/HTTPS protocols to serve web pages and process user inputs.   
 \*\*Input/Output\*\*:   
 - Input: Web requests from users or administrators.   
 - Output: Web responses, including HTML, JSON, or file downloads (e.g., PDF, Excel, CSV).   
  
- \*\*File Import/Export Interface\*\*   
 \*\*Role\*\*: Enables administrators to import asset data from files (e.g., CSV, Excel) and export data in selected formats (e.g., PDF, Excel, CSV).   
 \*\*Interaction Method\*\*: The system processes file uploads, validates the format and structure, and exports data in the specified format.   
 \*\*Input/Output\*\*:   
 - Input: File (CSV or Excel), data type (e.g., asset records), and export format.   
 - Output: Imported asset records, exported files ready for download, and audit log entries.   
  
- \*\*System Audit Log Communication Interface\*\*   
 \*\*Role\*\*: Logs system activities for monitoring and auditing, including user actions, login events, and configuration changes.   
 \*\*Interaction Method\*\*: The system writes audit logs to this interface whenever an action is performed.   
 \*\*Input/Output\*\*:   
 - Input: Action details (e.g., "User Permission Modified", "Asset Deleted").   
 - Output: Audit log entries and additional logs for access to the audit system.   
  
These communication interfaces ensure that the system can send notifications, interact with users via the web, and exchange data with external files and systems. They are designed to be secure, reliable, and scalable to support the system's functional requirements.

# Use Case

Use Case Name: Asset Registration   
Use Case ID: UC-01   
Actors: User, Administrator   
Preconditions:   
- The user must be authenticated and have access to the asset registration module.   
- The system must be connected to the asset database.   
- The user must have the necessary permissions to register new assets.   
  
Postconditions:   
- A new asset is successfully registered in the system.   
- The asset usage record is updated.   
- An approval workflow is initiated for the asset.   
- An email notification is sent to the administrator for review.   
- An audit log is created to document the registration activity.   
  
Main Flow:   
1. The user navigates to the asset registration interface.   
2. The user fills in the required asset details (e.g., name, type, location, and description).   
3. The user submits the asset registration request.   
4. The system validates the input data and checks for completeness.   
5. If valid, the system creates a new asset record and updates the asset usage record.   
6. The system initiates the approval workflow and sends an email notification to the administrator.   
7. The system logs the registration activity in the audit log.   
8. The system displays a confirmation message to the user indicating successful registration.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the user to correct the information.   
2. If the system cannot connect to the asset database, the asset registration is paused, and the user is notified of the issue.   
3. If the approval workflow fails, the system logs the error and sends an alert to the administrator for troubleshooting.   
4. If the email notification fails to send, the system logs the failure and provides a manual option for the user to notify the administrator.  
  
Use Case Name: View Asset Information   
Use Case ID: UC-02   
Actors: User, Administrator   
Preconditions:   
- The user must be authenticated and logged into the system.   
- The system must be connected to the asset database.   
- The user must have the necessary permissions to view asset details.   
  
Postconditions:   
- The asset information is displayed to the user.   
- The asset usage record is accessed and shown if applicable.   
- The system logs the viewing activity in the audit log.   
  
Main Flow:   
1. The user navigates to the asset information viewing interface.   
2. The user selects an asset from the list or enters an asset ID for search.   
3. The system retrieves the asset information from the asset database.   
4. The system displays the asset details (e.g., name, type, location, status, and description) to the user.   
5. If the asset has an associated usage record, the system retrieves and displays it.   
6. The system logs the viewing activity in the audit log.   
  
Alternative Flow:   
1. If the asset ID entered is invalid or not found, the system displays an error message and prompts the user to try again.   
2. If the system cannot connect to the asset database, the viewing request is paused, and the user is notified of the issue.   
3. If the user does not have permission to view the asset information, the system denies access and logs the unauthorized attempt.   
4. If an error occurs during the retrieval of asset usage records, the system displays a warning message and continues with the asset information display.  
  
Use Case Name: Modify Asset Details   
Use Case ID: UC-03   
Actors: User, Administrator   
Preconditions:   
- The user must be authenticated and logged into the system.   
- The system must be connected to the asset database.   
- The user must have the necessary permissions to modify asset details.   
- The asset to be modified must already exist in the system.   
  
Postconditions:   
- The asset details are successfully updated in the system.   
- The asset usage record is updated if necessary.   
- An approval workflow is initiated for the modified asset.   
- An email notification is sent to the administrator for review.   
- An audit log is created to document the modification activity.   
  
Main Flow:   
1. The user navigates to the asset modification interface.   
2. The user selects an asset from the list or enters an asset ID for search.   
3. The system retrieves the asset information from the asset database.   
4. The user edits the relevant asset details (e.g., name, type, location, or description).   
5. The user submits the modified asset details.   
6. The system validates the updated data and checks for completeness.   
7. If valid, the system updates the asset record and modifies the asset usage record if needed.   
8. The system initiates the approval workflow and sends an email notification to the administrator.   
9. The system logs the modification activity in the audit log.   
10. The system displays a confirmation message to the user indicating successful modification.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the user to correct the information.   
2. If the system cannot connect to the asset database, the modification request is paused, and the user is notified of the issue.   
3. If the approval workflow fails, the system logs the error and sends an alert to the administrator for troubleshooting.   
4. If the email notification fails to send, the system logs the failure and provides a manual option for the user to notify the administrator.   
5. If the user does not have permission to modify the asset details, the system denies the request and logs the unauthorized attempt.   
6. If the asset ID entered is invalid or not found, the system displays an error message and prompts the user to try again.  
  
Use Case Name: Delete Asset Record   
Use Case ID: UC-04   
Actors: User, Administrator   
Preconditions:   
- The user must be authenticated and logged into the system.   
- The system must be connected to the asset database.   
- The user must have the necessary permissions to delete asset records.   
- The asset to be deleted must exist in the system.   
  
Postconditions:   
- The selected asset record is successfully deleted from the system.   
- The asset usage record is updated or removed accordingly.   
- An approval workflow is initiated for the deletion.   
- An email notification is sent to the administrator for review.   
- An audit log is created to document the deletion activity.   
  
Main Flow:   
1. The user navigates to the asset deletion interface.   
2. The user selects an asset from the list or enters an asset ID for search.   
3. The system retrieves the asset information from the asset database.   
4. The user confirms the deletion of the selected asset.   
5. The system validates the deletion request and checks user permissions.   
6. If valid, the system deletes the asset record and updates the asset usage record.   
7. The system initiates the approval workflow and sends an email notification to the administrator.   
8. The system logs the deletion activity in the audit log.   
9. The system displays a confirmation message to the user indicating successful deletion.   
  
Alternative Flow:   
1. If the asset ID entered is invalid or not found, the system displays an error message and prompts the user to try again.   
2. If the system cannot connect to the asset database, the deletion request is paused, and the user is notified of the issue.   
3. If the user does not have permission to delete the asset record, the system denies the request and logs the unauthorized attempt.   
4. If the approval workflow fails, the system logs the error and sends an alert to the administrator for troubleshooting.   
5. If the email notification fails to send, the system logs the failure and provides a manual option for the user to notify the administrator.  
  
Use Case Name: User Login   
Use Case ID: UC-00   
Actors: User, Administrator   
Preconditions:   
- The system must be operational and accessible.   
- The user must have a valid account with a username and password.   
- The authentication database must be connected and available.   
  
Postconditions:   
- The user is successfully authenticated and logged into the system.   
- The user's session is initiated.   
- The system logs the login activity in the audit log.   
- The user is redirected to the appropriate interface based on their role.   
  
Main Flow:   
1. The user opens the login interface of the system.   
2. The user enters their username and password.   
3. The system verifies the credentials against the authentication database.   
4. If valid, the system initiates a user session and logs the login activity.   
5. The system determines the user's role (User or Administrator).   
6. The system redirects the user to the appropriate interface based on their role.   
7. The user is now able to access and perform actions within the system.   
  
Alternative Flow:   
1. If the entered username or password is incorrect, the system displays an error message and prompts the user to try again.   
2. If the authentication database is unavailable, the system displays a connectivity error and prevents login.   
3. If the user account is locked or disabled, the system denies access and logs the failed attempt.   
4. If the system fails to log the activity in the audit log, it displays a warning and allows the login to proceed.   
5. If the session initialization fails, the system displays an error and requires the user to reattempt login.  
  
Use Case Name: User Registration   
Use Case ID: UC-05   
Actors: Administrator   
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the authentication database.   
- The administrator must have the necessary permissions to register new users.   
  
Postconditions:   
- A new user is successfully registered in the system.   
- The user's access permissions are assigned accordingly.   
- An email notification is sent to the new user for confirmation.   
- The system logs the registration activity in the audit log.   
  
Main Flow:   
1. The administrator navigates to the user registration interface.   
2. The administrator fills in the required user details (e.g., username, password, full name, and role).   
3. The administrator submits the user registration request.   
4. The system validates the input data and checks for completeness.   
5. If valid, the system creates a new user record and assigns appropriate permissions.   
6. The system sends an email notification to the new user for confirmation.   
7. The system logs the registration activity in the audit log.   
8. The system displays a confirmation message to the administrator indicating successful registration.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the information.   
2. If the system cannot connect to the authentication database, the registration request is paused, and the administrator is notified of the issue.   
3. If the email notification fails to send, the system logs the failure and provides a manual option for the administrator to notify the user.   
4. If the system fails to log the activity in the audit log, it displays a warning and proceeds with the registration.   
5. If the username is already taken, the system displays an error message and prompts the administrator to choose a different username.  
  
Use Case Name: Manage User Permissions   
Use Case ID: UC-06   
Actors: Administrator   
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the authentication and asset databases.   
- The administrator must have the necessary permissions to manage user roles and access levels.   
  
Postconditions:   
- The user's permissions are updated in the system.   
- The system logs the permission change activity in the audit log.   
- An email notification is sent to the user and/or administrator for confirmation.   
  
Main Flow:   
1. The administrator navigates to the user permission management interface.   
2. The administrator selects a user from the list or searches for a user by ID or name.   
3. The system retrieves the user's current role and permissions.   
4. The administrator modifies the user's permissions or role as needed.   
5. The administrator submits the updated permission settings.   
6. The system validates the changes and confirms that the administrator has the authority to make them.   
7. The system updates the user's permissions in the database.   
8. The system sends an email notification to the user and logs the activity in the audit log.   
9. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the user ID is invalid or not found, the system displays an error message and prompts the administrator to try again.   
2. If the system cannot connect to the authentication database, the permission update is paused, and the administrator is notified of the issue.   
3. If the administrator does not have permission to modify the selected user’s access, the system denies the request and logs the unauthorized attempt.   
4. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the information.   
5. If the email notification fails to send, the system logs the failure and provides a manual option for the administrator to notify the user.   
6. If the audit log cannot be updated, the system displays a warning message but allows the permission change to proceed.  
  
Use Case Name: View User List   
Use Case ID: UC-07   
Actors: Administrator   
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the authentication database.   
- The administrator must have the necessary permissions to view user information.   
  
Postconditions:   
- The list of users is displayed to the administrator.   
- The system logs the viewing activity in the audit log.   
  
Main Flow:   
1. The administrator navigates to the user list interface.   
2. The system retrieves the list of all registered users from the authentication database.   
3. The system displays the user list (e.g., usernames, full names, roles, and status).   
4. The system logs the viewing activity in the audit log.   
  
Alternative Flow:   
1. If the system cannot connect to the authentication database, the request is paused, and the administrator is notified of the issue.   
2. If the administrator does not have permission to view the user list, the system denies access and logs the unauthorized attempt.   
3. If an error occurs while retrieving user data, the system displays a warning message and continues to display available user information.  
  
Use Case Name: Create Asset Usage Record   
Use Case ID: UC-08   
Actors: User, Administrator   
Preconditions:   
- The user must be authenticated and logged into the system.   
- The system must be connected to the asset database.   
- The user must have the necessary permissions to create asset usage records.   
- The asset for which the usage record is being created must already exist in the system.   
  
Postconditions:   
- A new asset usage record is successfully created in the system.   
- The asset usage record is linked to the corresponding asset.   
- An approval workflow is initiated for the usage record.   
- An email notification is sent to the administrator for review.   
- An audit log is created to document the creation activity.   
  
Main Flow:   
1. The user navigates to the asset usage record creation interface.   
2. The user selects an asset from the list or enters an asset ID for reference.   
3. The user inputs the usage details (e.g., usage date, duration, purpose, and user involved).   
4. The user submits the asset usage record request.   
5. The system validates the input data and checks for completeness.   
6. If valid, the system creates a new asset usage record and links it to the selected asset.   
7. The system initiates the approval workflow and sends an email notification to the administrator.   
8. The system logs the creation activity in the audit log.   
9. The system displays a confirmation message to the user indicating successful record creation.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the user to correct the information.   
2. If the system cannot connect to the asset database, the record creation is paused, and the user is notified of the issue.   
3. If the approval workflow fails, the system logs the error and sends an alert to the administrator for troubleshooting.   
4. If the email notification fails to send, the system logs the failure and provides a manual option for the user to notify the administrator.   
5. If the user does not have permission to create a usage record, the system denies the request and logs the unauthorized attempt.   
6. If the selected asset ID is invalid or not found, the system displays an error message and prompts the user to try again.  
  
Use Case Name: View Asset Usage History   
Use Case ID: UC-09   
Actors: User, Administrator   
Preconditions:   
- The user must be authenticated and logged into the system.   
- The system must be connected to the asset database.   
- The user must have the necessary permissions to view asset usage history.   
- The asset for which the usage history is being viewed must already exist in the system.   
  
Postconditions:   
- The asset usage history is displayed to the user.   
- The system logs the viewing activity in the audit log.   
  
Main Flow:   
1. The user navigates to the asset usage history viewing interface.   
2. The user selects an asset from the list or enters an asset ID for search.   
3. The system retrieves the asset usage history from the asset usage record database.   
4. The system displays the asset usage history (e.g., usage dates, duration, purpose, and users involved) to the user.   
5. The system logs the viewing activity in the audit log.   
  
Alternative Flow:   
1. If the asset ID is invalid or not found, the system displays an error message and prompts the user to try again.   
2. If the system cannot connect to the asset usage record database, the request is paused, and the user is notified of the issue.   
3. If the user does not have permission to view the asset usage history, the system denies access and logs the unauthorized attempt.   
4. If an error occurs while retrieving the usage history, the system displays a warning message and continues to display available data.  
  
Use Case Name: Update Asset Usage Status   
Use Case ID: UC-10   
Actors: User, Administrator   
Preconditions:   
- The user must be authenticated and logged into the system.   
- The system must be connected to the asset and asset usage record databases.   
- The user must have the necessary permissions to update asset usage status.   
- The asset usage record to be updated must already exist in the system.   
  
Postconditions:   
- The asset usage status is successfully updated in the system.   
- The asset usage record is modified accordingly.   
- An approval workflow is initiated for the updated usage record.   
- An email notification is sent to the administrator for review.   
- An audit log is created to document the status update activity.   
  
Main Flow:   
1. The user navigates to the asset usage status update interface.   
2. The user selects an asset usage record from the list or enters a usage record ID for search.   
3. The system retrieves the selected asset usage record.   
4. The user modifies the usage status (e.g., "In Use," "Available," "Maintenance").   
5. The user submits the updated usage status.   
6. The system validates the input data and confirms the status is valid.   
7. If valid, the system updates the asset usage record and initiates the approval workflow.   
8. The system sends an email notification to the administrator for review.   
9. The system logs the status update activity in the audit log.   
10. The system displays a confirmation message to the user indicating the status has been updated.   
  
Alternative Flow:   
1. If the input status is invalid or not recognized, the system displays an error message and prompts the user to select a valid status.   
2. If the system cannot connect to the asset usage record database, the update request is paused, and the user is notified of the issue.   
3. If the approval workflow fails, the system logs the error and sends an alert to the administrator for troubleshooting.   
4. If the email notification fails to send, the system logs the failure and provides a manual option for the user to notify the administrator.   
5. If the user does not have permission to update the asset usage status, the system denies the request and logs the unauthorized attempt.   
6. If the selected usage record ID is invalid or not found, the system displays an error message and prompts the user to try again.  
  
Use Case Name: Delete Usage Record   
Use Case ID: UC-11   
Actors: User, Administrator   
Preconditions:   
- The user must be authenticated and logged into the system.   
- The system must be connected to the asset usage record database.   
- The user must have the necessary permissions to delete usage records.   
- The asset usage record to be deleted must already exist in the system.   
  
Postconditions:   
- The selected asset usage record is successfully deleted from the system.   
- The system logs the deletion activity in the audit log.   
- An email notification is sent to the administrator for confirmation.   
  
Main Flow:   
1. The user navigates to the asset usage record deletion interface.   
2. The user selects an asset usage record from the list or enters a usage record ID for search.   
3. The system retrieves the asset usage record from the database.   
4. The user confirms the deletion of the selected usage record.   
5. The system validates the deletion request and checks user permissions.   
6. If valid, the system deletes the asset usage record.   
7. The system sends an email notification to the administrator for confirmation.   
8. The system logs the deletion activity in the audit log.   
9. The system displays a confirmation message to the user indicating successful deletion.   
  
Alternative Flow:   
1. If the usage record ID is invalid or not found, the system displays an error message and prompts the user to try again.   
2. If the system cannot connect to the asset usage record database, the deletion request is paused, and the user is notified of the issue.   
3. If the user does not have permission to delete the usage record, the system denies the request and logs the unauthorized attempt.   
4. If the email notification fails to send, the system logs the failure and provides a manual option for the user to notify the administrator.   
5. If the audit log cannot be updated, the system displays a warning message but allows the deletion to proceed.  
  
Use Case Name: Initiate Asset Approval   
Use Case ID: UC-12   
Actors: User, Administrator   
Preconditions:   
- The user must be authenticated and logged into the system.   
- The system must be connected to the asset and approval workflow databases.   
- The user must have the necessary permissions to initiate asset approval.   
- The asset to be approved must already exist in the system.   
  
Postconditions:   
- The asset approval workflow is initiated.   
- The system sends an email notification to the administrator.   
- The system logs the approval initiation in the audit log.   
  
Main Flow:   
1. The user navigates to the asset approval initiation interface.   
2. The user selects an asset from the list or enters an asset ID for reference.   
3. The system retrieves the asset details from the asset database.   
4. The user confirms the request to initiate approval for the asset.   
5. The system initiates the approval workflow for the selected asset.   
6. The system sends an email notification to the administrator for review.   
7. The system logs the initiation of the approval workflow in the audit log.   
8. The system displays a confirmation message to the user indicating that the approval process has been initiated.   
  
Alternative Flow:   
1. If the asset ID is invalid or not found, the system displays an error message and prompts the user to try again.   
2. If the system cannot connect to the asset or approval workflow database, the request is paused, and the user is notified of the issue.   
3. If the user does not have permission to initiate asset approval, the system denies the request and logs the unauthorized attempt.   
4. If the approval workflow fails to start, the system logs the error and sends an alert to the administrator for troubleshooting.   
5. If the email notification fails to send, the system logs the failure and provides a manual option for the user to notify the administrator.  
  
Use Case Name: View Asset Approval   
Use Case ID: UC-13   
Actors: User, Administrator   
Preconditions:   
- The user must be authenticated and logged into the system.   
- The system must be connected to the approval workflow database.   
- The user must have the necessary permissions to view asset approval status.   
- The asset for which the approval is being viewed must already exist in the system.   
  
Postconditions:   
- The asset approval status and details are displayed to the user.   
- The system logs the viewing activity in the audit log.   
  
Main Flow:   
1. The user navigates to the asset approval viewing interface.   
2. The user selects an asset from the list or enters an asset ID for search.   
3. The system retrieves the asset approval workflow details from the approval workflow database.   
4. The system displays the approval status, current step, and any relevant comments or actions.   
5. The system logs the viewing activity in the audit log.   
  
Alternative Flow:   
1. If the asset ID is invalid or not found, the system displays an error message and prompts the user to try again.   
2. If the system cannot connect to the approval workflow database, the request is paused, and the user is notified of the issue.   
3. If the user does not have permission to view the asset approval details, the system denies access and logs the unauthorized attempt.   
4. If an error occurs while retrieving the approval workflow data, the system displays a warning message and continues to display available approval details.  
  
Use Case Name: Manage Permission Levels   
Use Case ID: UC-14   
Actors: Administrator   
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the authentication database.   
- The administrator must have the necessary permissions to manage permission levels.   
  
Postconditions:   
- Permission levels are successfully created, modified, or deleted in the system.   
- The system logs the permission level changes in the audit log.   
- An email notification is sent to the administrator for confirmation or alert purposes.   
  
Main Flow:   
1. The administrator navigates to the permission level management interface.   
2. The administrator selects an action: create a new permission level, modify an existing one, or delete a permission level.   
3. The system retrieves the current permission levels from the authentication database.   
4. The administrator inputs or selects the relevant permission details (e.g., level name, access rights, and associated roles).   
5. The administrator submits the permission level request.   
6. The system validates the input and checks if the action is allowed based on the administrator's privileges.   
7. If valid, the system updates the permission level in the database.   
8. The system sends an email notification to the administrator for confirmation.   
9. The system logs the permission level change in the audit log.   
10. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the information.   
2. If the system cannot connect to the authentication database, the request is paused, and the administrator is notified of the issue.   
3. If the administrator does not have permission to manage the selected permission level, the system denies the request and logs the unauthorized attempt.   
4. If the email notification fails to send, the system logs the failure and provides a manual option for the administrator to confirm or troubleshoot.   
5. If the audit log cannot be updated, the system displays a warning message but allows the permission level change to proceed.  
  
Use Case Name: Generate Asset Report   
Use Case ID: UC-15   
Actors: Administrator   
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the asset and asset usage record databases.   
- The administrator must have the necessary permissions to generate asset reports.   
- The report analysis module must be available and functional.   
  
Postconditions:   
- A comprehensive asset report is generated and displayed or exported.   
- The system logs the report generation activity in the audit log.   
- The report includes aggregated data from asset records and usage history.   
  
Main Flow:   
1. The administrator navigates to the asset report generation interface.   
2. The administrator selects the report type (e.g., usage summary, asset status report, or full asset inventory).   
3. The administrator specifies the date range or filters for the report (e.g., asset type, location, or usage status).   
4. The system retrieves the relevant asset and asset usage data based on the filters.   
5. The system processes and aggregates the data for the selected report type.   
6. The system generates the asset report and displays it in a user-friendly format (e.g., table or chart).   
7. The system logs the report generation activity in the audit log.   
8. The administrator has the option to export the report in a specified format (e.g., PDF, Excel, or CSV).   
9. The system confirms the report is ready for viewing or download.   
  
Alternative Flow:   
1. If the system cannot connect to the asset or asset usage record database, the report generation is paused, and the administrator is notified of the issue.   
2. If the specified filters do not return any data, the system displays a message indicating no results were found and allows the administrator to adjust the filters.   
3. If the report analysis module is not available, the system displays an error and prevents report generation.   
4. If the export format is invalid or not supported, the system displays an error message and prompts the administrator to select a valid format.   
5. If the audit log cannot be updated, the system displays a warning message but allows the report to be generated.  
  
Use Case Name: View Report Analysis   
Use Case ID: UC-16   
Actors: User, Administrator   
Preconditions:   
- The user must be authenticated and logged into the system.   
- The system must be connected to the report analysis and asset usage record databases.   
- The user must have the necessary permissions to view report analysis.   
- The report analysis module must be available and functional.   
  
Postconditions:   
- The selected report analysis is displayed to the user.   
- The system logs the viewing activity in the audit log.   
- The report includes relevant data from asset records and usage history.   
  
Main Flow:   
1. The user navigates to the report analysis viewing interface.   
2. The user selects a specific report or enters a report ID for search.   
3. The system retrieves the selected report analysis from the report analysis database.   
4. The system displays the report data (e.g., charts, summaries, and detailed statistics).   
5. The system logs the viewing activity in the audit log.   
6. The user can optionally download or print the report.   
  
Alternative Flow:   
1. If the report ID is invalid or not found, the system displays an error message and prompts the user to try again.   
2. If the system cannot connect to the report analysis database, the request is paused, and the user is notified of the issue.   
3. If the user does not have permission to view the report analysis, the system denies access and logs the unauthorized attempt.   
4. If an error occurs while retrieving the report data, the system displays a warning message and continues to display available data.  
  
Use Case Name: Export Asset Data   
Use Case ID: UC-17   
Actors: Administrator   
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the asset and asset usage record databases.   
- The administrator must have the necessary permissions to export asset data.   
- The data export module must be available and functional.   
  
Postconditions:   
- The asset data is successfully exported in the selected format.   
- The system logs the export activity in the audit log.   
- The exported file is ready for download or transfer.   
  
Main Flow:   
1. The administrator navigates to the asset data export interface.   
2. The administrator selects the type of data to export (e.g., all assets, specific asset types, or asset usage records).   
3. The administrator specifies filters (e.g., date range, location, or asset status).   
4. The administrator selects the export format (e.g., PDF, Excel, or CSV).   
5. The system retrieves the relevant asset data based on the selected filters.   
6. The system processes and formats the data for export.   
7. The system generates the export file and makes it available for download.   
8. The system logs the export activity in the audit log.   
9. The administrator is notified that the export is complete and can download the file.   
  
Alternative Flow:   
1. If the system cannot connect to the asset or asset usage record database, the export is paused, and the administrator is notified of the issue.   
2. If the selected filters do not return any data, the system displays a message indicating no results were found and allows the administrator to adjust the filters.   
3. If the data export module is not available, the system displays an error and prevents the export.   
4. If the export format is invalid or not supported, the system displays an error message and prompts the administrator to select a valid format.   
5. If the system fails to log the activity in the audit log, it displays a warning message but allows the export to proceed.  
  
Use Case Name: Import Asset Data   
Use Case ID: UC-18   
Actors: Administrator   
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the asset database.   
- The administrator must have the necessary permissions to import asset data.   
- A valid data file (e.g., CSV, Excel) containing asset information must be prepared.   
  
Postconditions:   
- The asset data from the file is successfully imported into the system.   
- The system validates and processes each record, creating new asset entries.   
- An audit log is created to document the import activity.   
- An email notification is sent to the administrator confirming the import.   
  
Main Flow:   
1. The administrator navigates to the data import interface.   
2. The administrator selects the type of data to import (e.g., asset records).   
3. The administrator uploads the data file (e.g., CSV or Excel).   
4. The system validates the file format and structure.   
5. The system processes the file and maps the data to the corresponding asset fields.   
6. The system imports valid asset data into the asset database.   
7. The system logs the import activity in the audit log.   
8. The system sends an email notification to the administrator confirming the import.   
9. The system displays a confirmation message to the administrator indicating successful import.   
  
Alternative Flow:   
1. If the file format is invalid or unsupported, the system displays an error message and prompts the administrator to upload a valid file.   
2. If the file structure does not match the required format, the system displays an error and provides a template for reference.   
3. If the system cannot connect to the asset database, the import is paused, and the administrator is notified of the issue.   
4. If the administrator does not have permission to import data, the system denies the request and logs the unauthorized attempt.   
5. If the email notification fails to send, the system logs the failure and provides a manual option for the administrator to confirm the import.   
6. If the audit log cannot be updated, the system displays a warning message but allows the import to proceed.  
  
Use Case Name: Send Email Notification   
Use Case ID: UC-19   
Actors: System, Administrator   
Preconditions:   
- The system must be connected to the email notification service.   
- The recipient administrator must have a valid email address registered in the system.   
- The system must have an event or action that requires sending an email notification (e.g., asset registration, approval workflow, or permission change).   
- The email notification module must be enabled and functional.   
  
Postconditions:   
- The email notification is successfully sent to the administrator.   
- The system logs the notification activity in the audit log.   
- The administrator receives the notification with relevant details about the event.   
  
Main Flow:   
1. The system detects an event that requires sending an email notification (e.g., asset registration, approval request, or user permission change).   
2. The system prepares the email content, including the event type, relevant asset or user information, and next steps for the administrator.   
3. The system verifies the email address of the recipient administrator from the authentication database.   
4. The system sends the email notification through the configured email service.   
5. The system logs the email notification activity in the audit log, including the timestamp and details of the event.   
6. The system confirms the notification was sent and continues with the main process.   
  
Alternative Flow:   
1. If the email address is invalid or missing, the system logs the failure and provides a manual option for the administrator to review and send the notification.   
2. If the email service is unavailable, the system logs the failure and notifies the administrator to retry later.   
3. If the audit log cannot be updated, the system displays a warning but proceeds with sending the email notification.   
4. If the system fails to send the email notification, it logs the error and provides an option to send it manually via the system interface.  
  
Use Case Name: View Email Notification History   
Use Case ID: UC-20   
Actors: Administrator, User   
Preconditions:   
- The user or administrator must be authenticated and logged into the system.   
- The system must be connected to the email notification database.   
- The user or administrator must have the necessary permissions to view email notification history.   
- The email notification module must be enabled and functional.   
  
Postconditions:   
- The history of email notifications is displayed to the user or administrator.   
- The system logs the viewing activity in the audit log.   
- The email notification records are retrieved and shown in a clear format.   
  
Main Flow:   
1. The user or administrator navigates to the email notification history interface.   
2. The system retrieves all email notification records from the email notification database.   
3. The system filters and displays the email notification history based on criteria such as date, recipient, or event type.   
4. The user or administrator can view details of each notification, such as subject, content, timestamp, and status.   
5. The system logs the viewing activity in the audit log.   
  
Alternative Flow:   
1. If the system cannot connect to the email notification database, the request is paused, and the user or administrator is notified of the issue.   
2. If the email notification database is empty or no notifications match the filters, the system displays a message indicating no data is available.   
3. If the user or administrator does not have permission to view the email notification history, the system denies access and logs the unauthorized attempt.   
4. If an error occurs while retrieving the email notification records, the system displays a warning message and continues to display available data.  
  
Use Case Name: Audit System Logs   
Use Case ID: UC-21   
Actors: Administrator   
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the audit log database.   
- The administrator must have the necessary permissions to access the audit logs.   
  
Postconditions:   
- The system logs are retrieved and displayed to the administrator.   
- The system logs the viewing activity in the audit log.   
- The administrator can filter and search the logs as needed.   
  
Main Flow:   
1. The administrator navigates to the audit log interface.   
2. The system retrieves the audit log entries from the audit log database.   
3. The system displays the logs in a structured format, including details such as user, action, timestamp, and status.   
4. The administrator can apply filters (e.g., by date, user, or action type) to narrow the results.   
5. The system updates the displayed logs based on the applied filters.   
6. The system logs the administrator's access to the audit logs.   
  
Alternative Flow:   
1. If the system cannot connect to the audit log database, the request is paused, and the administrator is notified of the issue.   
2. If the administrator does not have permission to view the audit logs, the system denies access and logs the unauthorized attempt.   
3. If no logs match the applied filters, the system displays a message indicating no results were found and allows the administrator to adjust the filters.   
4. If an error occurs during log retrieval, the system displays a warning message and continues to display available data.  
  
Use Case Name: Manage Administrator Account   
Use Case ID: UC-22   
Actors: Administrator   
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the authentication database.   
- The administrator must have the necessary permissions to manage administrator accounts.   
  
Postconditions:   
- The administrator account is successfully created, modified, or deleted.   
- The system logs the account management activity in the audit log.   
- An email notification is sent to the administrator for confirmation or alert purposes.   
  
Main Flow:   
1. The administrator navigates to the administrator account management interface.   
2. The administrator selects an action: create a new administrator account, modify an existing one, or delete an account.   
3. The system retrieves the current list of administrator accounts from the authentication database.   
4. The administrator inputs or selects the relevant account details (e.g., username, password, full name, and role).   
5. The administrator submits the account management request.   
6. The system validates the input and checks if the action is allowed based on the administrator's privileges.   
7. If valid, the system updates the administrator account in the database.   
8. The system sends an email notification to the administrator for confirmation or alert.   
9. The system logs the account management activity in the audit log.   
10. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the information.   
2. If the system cannot connect to the authentication database, the request is paused, and the administrator is notified of the issue.   
3. If the administrator does not have permission to manage the selected account, the system denies the request and logs the unauthorized attempt.   
4. If the email notification fails to send, the system logs the failure and provides a manual option for the administrator to notify or confirm.   
5. If the audit log cannot be updated, the system displays a warning message but allows the account management to proceed.  
  
Use Case Name: Manage Login Record   
Use Case ID: UC-23   
Actors: Administrator   
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the login record database.   
- The administrator must have the necessary permissions to manage login records.   
- The login record module must be available and functional.   
  
Postconditions:   
- The login record is successfully created, viewed, modified, or deleted in the system.   
- The system logs the management activity in the audit log.   
- The login record data is accessible for monitoring and analysis.   
  
Main Flow:   
1. The administrator navigates to the login record management interface.   
2. The administrator selects an action: view login records, filter by user, date, or status, or delete specific login records.   
3. The system retrieves the relevant login records from the login record database.   
4. The system displays the login record details (e.g., username, login time, status, and IP address).   
5. If the administrator chooses to delete a login record, the system validates the record's existence and confirms the deletion.   
6. The system performs the selected action (e.g., deletion of the login record).   
7. The system logs the login record management activity in the audit log.   
8. The system displays a confirmation message to the administrator indicating the action was completed.   
  
Alternative Flow:   
1. If the system cannot connect to the login record database, the request is paused, and the administrator is notified of the issue.   
2. If the selected login record is invalid or not found, the system displays an error message and prompts the administrator to try again.   
3. If the administrator does not have permission to manage login records, the system denies the request and logs the unauthorized attempt.   
4. If an error occurs during the deletion or modification of a login record, the system displays a warning message and provides a manual option for the administrator to troubleshoot.   
5. If the audit log cannot be updated, the system displays a warning message but allows the login record management to proceed.  
  
Use Case Name: Manage User Registration   
Use Case ID: UC-24   
Actors: Administrator   
  
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the authentication and user registration databases.   
- The administrator must have the necessary permissions to manage the user registration process.   
- The user registration module must be available and functional.   
  
Postconditions:   
- The user registration process is configured or modified in the system.   
- The system logs the management activity in the audit log.   
- The administrator is notified of the success or failure of the operation.   
  
Main Flow:   
1. The administrator navigates to the user registration management interface.   
2. The administrator selects an action: configure user registration settings (e.g., enable/disable self-registration, set validation rules, or assign default roles).   
3. The system retrieves the current configuration of the user registration process from the database.   
4. The administrator modifies the settings as required.   
5. The administrator submits the updated configuration.   
6. The system validates the input and checks if the action is allowed based on the administrator’s privileges.   
7. If valid, the system updates the user registration configuration in the database.   
8. The system logs the configuration change in the audit log.   
9. The system displays a confirmation message to the administrator indicating the settings have been successfully updated.   
  
Alternative Flow:   
1. If the system cannot connect to the authentication or user registration database, the request is paused, and the administrator is notified of the issue.   
2. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the information.   
3. If the administrator does not have permission to manage user registration settings, the system denies the request and logs the unauthorized attempt.   
4. If the audit log cannot be updated, the system displays a warning message but allows the configuration change to proceed.   
5. If the system fails to apply the configuration changes, it logs the error and provides an option for the administrator to retry or troubleshoot the issue.  
  
Use Case Name: Manage Permission Assignment   
Use Case ID: UC-25   
Actors: Administrator   
  
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the authentication and asset databases.   
- The administrator must have the necessary permissions to assign or modify permissions for users or roles.   
- The permission assignment module must be available and functional.   
  
Postconditions:   
- The permission assignments are successfully created, modified, or deleted in the system.   
- The system logs the permission assignment activity in the audit log.   
- The affected user or role has updated access rights.   
- An email notification is sent to the administrator for confirmation or alert purposes.   
  
Main Flow:   
1. The administrator navigates to the permission assignment management interface.   
2. The administrator selects a user or role to assign or modify permissions.   
3. The system retrieves the current permission assignments for the selected user or role.   
4. The administrator selects or inputs the new permissions to be assigned (e.g., access to specific modules, actions, or assets).   
5. The administrator submits the permission assignment request.   
6. The system validates the selected permissions and checks if the action is allowed based on the administrator’s privileges.   
7. If valid, the system updates the permission assignments in the authentication database.   
8. The system logs the permission assignment activity in the audit log.   
9. The system sends an email notification to the administrator confirming the permission changes.   
10. The system displays a confirmation message to the administrator indicating the permission assignment has been successfully updated.   
  
Alternative Flow:   
1. If the system cannot connect to the authentication or asset database, the request is paused, and the administrator is notified of the issue.   
2. If the selected user or role is invalid or not found, the system displays an error message and prompts the administrator to try again.   
3. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the information.   
4. If the administrator does not have permission to manage the selected permission assignment, the system denies the request and logs the unauthorized attempt.   
5. If the audit log cannot be updated, the system displays a warning message but allows the permission assignment change to proceed.   
6. If the email notification fails to send, the system logs the failure and provides a manual option for the administrator to confirm or troubleshoot.  
  
Use Case Name: Manage Report Analysis   
Use Case ID: UC-26   
Actors: Administrator   
  
Preconditions:   
- The administrator must be authenticated and logged into the system.   
- The system must be connected to the report analysis database.   
- The administrator must have the necessary permissions to manage report analysis settings and configurations.   
- The report analysis module must be available and functional.   
  
Postconditions:   
- The report analysis settings are successfully configured, modified, or deleted in the system.   
- The system logs the management activity in the audit log.   
- The report analysis module reflects the updated settings.   
- An email notification is sent to the administrator for confirmation or alert purposes.   
  
Main Flow:   
1. The administrator navigates to the report analysis management interface.   
2. The administrator selects an action: configure report analysis settings (e.g., set report templates, define data aggregation rules, or schedule automated report generation).   
3. The system retrieves the current report analysis configuration from the database.   
4. The administrator modifies or inputs the new settings for report analysis.   
5. The administrator submits the updated configuration.   
6. The system validates the input and confirms that the administrator has the authority to make the changes.   
7. If valid, the system updates the report analysis configuration in the database.   
8. The system logs the configuration change in the audit log.   
9. The system sends an email notification to the administrator confirming the report analysis settings have been updated.   
10. The system displays a confirmation message to the administrator indicating the settings have been successfully modified.   
  
Alternative Flow:   
1. If the system cannot connect to the report analysis database, the request is paused, and the administrator is notified of the issue.   
2. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the information.   
3. If the administrator does not have permission to manage report analysis settings, the system denies the request and logs the unauthorized attempt.   
4. If the audit log cannot be updated, the system displays a warning message but allows the configuration change to proceed.   
5. If the email notification fails to send, the system logs the failure and provides a manual option for the administrator to confirm or troubleshoot.