项目文档

# Functional Requirement

1. Functional Requirements   
  
1.1 Asset Registration Function   
 Function ID: FR-01   
 Description: Allow authenticated users to register new assets with necessary details, which requires administrator approval before being stored in the database.   
 Input: Asset information (e.g., asset name, type, description, location, owner, and other relevant details).   
 Output: Asset record stored in the database and an audit log entry created.   
  
1.2 Asset Validation Function   
 Function ID: FR-02   
 Description: Validate the input data for completeness and correctness during asset registration or modification.   
 Input: User-submitted asset data.   
 Output: Validation result (success or error message with details to correct).   
  
1.3 Asset Approval Request Function   
 Function ID: FR-03   
 Description: Automatically request administrator approval for asset registration or modification if the system requires it.   
 Input: Validated asset data and action type (register or modify).   
 Output: Approval request sent to the administrator for review.   
  
1.4 Administrator Approval Function   
 Function ID: FR-04   
 Description: Allow administrators to approve or reject asset registration or modification requests.   
 Input: Pending approval request details.   
 Output: Updated approval status in the database.   
  
1.5 Asset Storage Function   
 Function ID: FR-05   
 Description: Store approved asset data in the database and maintain the integrity of the asset records.   
 Input: Approved asset data and its associated metadata.   
 Output: Asset record stored in the database.   
  
1.6 Asset Retrieval Function   
 Function ID: FR-06   
 Description: Retrieve asset records from the database for viewing or modifying.   
 Input: Asset identifier (e.g., asset ID, name, or search criteria).   
 Output: Retrieved asset record with its associated details.   
  
1.7 Asset Modification Function   
 Function ID: FR-07   
 Description: Allow authenticated users to modify existing asset records, which requires administrator approval.   
 Input: Asset identifier and updated asset data.   
 Output: Updated asset record in the database and audit log entry.   
  
1.8 Asset Deletion Function   
 Function ID: FR-08   
 Description: Allow authenticated users to request the deletion of an asset record, which requires administrator approval.   
 Input: Asset identifier and confirmation of deletion.   
 Output: Deleted asset record from the database and audit log entry.   
  
1.9 Asset Usage Recording Function   
 Function ID: FR-09   
 Description: Allow users to record usage of an asset, including time, purpose, and other details, which may require approval depending on configuration.   
 Input: Asset identifier, usage details (start time, end time, quantity, purpose).   
 Output: Usage record stored in the database and audit log entry.   
  
1.10 Usage Approval Request Function   
 Function ID: FR-10   
 Description: Automatically request administrator approval for asset usage if the permission approval workflow is enabled.   
 Input: Usage details and asset identifier.   
 Output: Usage approval request sent to the administrator.   
  
1.11 Usage Approval Decision Function   
 Function ID: FR-11   
 Description: Allow administrators to approve or reject asset usage requests.   
 Input: Pending usage request details.   
 Output: Updated usage record status in the database.   
  
1.12 Asset Report Generation Function   
 Function ID: FR-12   
 Description: Allow authenticated users to generate reports based on asset data, including filters and time ranges.   
 Input: Report type, time range, and optional filters (e.g., asset category, location, status).   
 Output: Generated report in the selected format (e.g., PDF, Excel).   
  
1.13 Report Validation Function   
 Function ID: FR-13   
 Description: Validate the report request to ensure the required data is available and the user has the appropriate permissions.   
 Input: Report request parameters.   
 Output: Validation result (success or error message with details to correct).   
  
1.14 Report Export Function   
 Function ID: FR-14   
 Description: Export the generated report in the selected format for download or email delivery.   
 Input: Generated report data and export format.   
 Output: Export file available for download or sent via email.   
  
1.15 Audit Log Recording Function   
 Function ID: FR-15   
 Description: Log all system actions (e.g., asset registration, modification, deletion, and report generation) in the audit log for traceability.   
 Input: Action details (actor, action type, timestamp, asset identifier, etc.).   
 Output: Audit log entry stored in the database.   
  
1.16 Authentication Log Recording Function   
 Function ID: FR-16   
 Description: Log all authentication-related events (e.g., login, unauthorized access attempts) for security monitoring.   
 Input: Authentication event details (actor, action type, timestamp, status).   
 Output: Authentication log entry stored in the database.   
  
1.17 Email Notification Function   
 Function ID: FR-17   
 Description: Send email notifications to users and administrators for various system events, such as asset registration, approval decisions, and report readiness.   
 Input: Recipient’s email address, message content, and event details.   
 Output: Email notification sent to the recipient or logged as a failure in the audit log.   
  
1.18 Permission Assignment Function   
 Function ID: FR-18   
 Description: Allow administrators to assign or modify user permissions for accessing and managing asset data.   
 Input: User identifier and permission details (e.g., view, modify, delete, report generation).   
 Output: Updated permission record in the database and audit log entry.   
  
1.19 Permission Approval Request Function   
 Function ID: FR-19   
 Description: Automatically request approval for permission assignment or modification if the permission approval workflow is enabled.   
 Input: Permission request details and user identifier.   
 Output: Approval request sent to the administrator for review.   
  
1.20 Permission Approval Decision Function   
 Function ID: FR-20   
 Description: Allow administrators to approve or reject permission assignment or modification requests.   
 Input: Pending permission request details.   
 Output: Updated permission status in the database.   
  
1.21 User Registration Function   
 Function ID: FR-21   
 Description: Allow administrators to register new users in the system with required details such as username, password, and role.   
 Input: User information (e.g., username, password, role, contact details).   
 Output: New user record stored in the database and audit log entry.   
  
1.22 User Account Management Function   
 Function ID: FR-22   
 Description: Allow administrators to create, modify, or delete user accounts in the system.   
 Input: User identifier and account action (create, modify, or delete).   
 Output: Updated user account status in the database and audit log entry.   
  
1.23 Data Import Function   
 Function ID: FR-23   
 Description: Allow users to import asset data from external files (e.g., CSV, Excel) into the system, which may require administrator approval.   
 Input: Source file (e.g., CSV, Excel) with asset data.   
 Output: Asset records stored in the database and audit log entry.   
  
1.24 Data Export Function   
 Function ID: FR-24   
 Description: Allow users to export asset data in various formats (e.g., CSV, Excel, PDF) based on specified criteria.   
 Input: Export format and optional filters (e.g., asset type, location, status).   
 Output: Export file generated and available for download or email delivery.   
  
1.25 Asset Category Management Function   
 Function ID: FR-25   
 Description: Allow administrators to manage asset categories, including creating, modifying, and deleting categories.   
 Input: Asset category identifier and action (create, modify, delete).   
 Output: Updated asset category record in the database and audit log entry.   
  
1.26 Location Management Function   
 Function ID: FR-26   
 Description: Allow administrators to manage asset locations, including creating, modifying, and deleting locations.   
 Input: Location identifier and action (create, modify, delete).   
 Output: Updated location record in the database and audit log entry.   
  
1.27 Asset Transfer Record Management Function   
 Function ID: FR-27   
 Description: Allow administrators or authorized users to create, modify, or delete asset transfer records.   
 Input: Transfer record identifier and action (create, modify, delete).   
 Output: Updated asset transfer record in the database and audit log entry.   
  
1.28 Asset Maintenance Record Management Function   
 Function ID: FR-28   
 Description: Allow administrators or authorized users to create, modify, or delete asset maintenance records.   
 Input: Maintenance record identifier and action (create, modify, delete).   
 Output: Updated asset maintenance record in the database and audit log entry.

# External Description

2. External Interfaces   
This chapter describes the external interfaces of the system, including user interfaces, hardware interfaces, software interfaces, and communication interfaces. These interfaces define how the system interacts with external entities such as users, hardware devices, other software systems, and communication protocols.   
  
2.1 User Interface   
The system provides a graphical user interface (GUI) for users to interact with asset management functionalities. The interface is designed to be intuitive and user-friendly, supporting the following interactions:   
- \*\*Asset Registration Screen\*\*: Users can input asset details such as asset name, type, description, location, and owner.   
- \*\*Asset Validation Feedback\*\*: Displays success or error messages to inform users about the validation results of their input data.   
- \*\*Approval Request Screen\*\*: Provides administrators with a screen to review and approve or reject asset registration, modification, or usage requests.   
- \*\*Asset Retrieval Interface\*\*: Allows users to search and view asset records using asset identifiers or filters.   
- \*\*Asset Modification Screen\*\*: Enables users to update existing asset information after retrieving the asset record.   
- \*\*Asset Deletion Request Interface\*\*: Users can request the deletion of an asset record and confirm the action.   
- \*\*Asset Usage Recording Screen\*\*: Users can input usage details such as start time, end time, quantity, and purpose for an asset.   
- \*\*Report Generation Interface\*\*: Users can select report types, time ranges, and filters to generate reports based on asset data.   
- \*\*Report Export Interface\*\*: Displays options for exporting generated reports in formats such as PDF or Excel.   
- \*\*User Account Management Interface\*\*: Administrators can manage user accounts by creating, modifying, or deleting user records.   
- \*\*Permission Assignment Interface\*\*: Administrators can assign or modify user permissions for asset-related operations.   
- \*\*Data Import/Export Interface\*\*: Users can import asset data from external files (e.g., CSV, Excel) and export asset data in various formats.   
- \*\*Asset Category Management Interface\*\*: Administrators can manage asset categories by creating, modifying, or deleting categories.   
- \*\*Location Management Interface\*\*: Administrators can manage asset locations by creating, modifying, or deleting location records.   
- \*\*Asset Transfer Record Management Interface\*\*: Administrators or authorized users can manage asset transfer records.   
- \*\*Asset Maintenance Record Management Interface\*\*: Administrators or authorized users can manage asset maintenance records.   
- \*\*Audit Log View Interface\*\*: Users can view system actions and authentication events for traceability and security monitoring.   
  
2.2 Hardware Interface   
The system does not directly interact with specific hardware devices. However, it may be deployed on servers or workstations that require standard hardware interfaces such as:   
- \*\*Server Hardware\*\*: The system requires a server with sufficient processing power, memory, and storage to handle asset data and user requests.   
- \*\*Input Devices\*\*: Standard input devices like keyboards and mice are used by users to interact with the system.   
- \*\*Output Devices\*\*: Monitors and printers are used to display or print asset records, reports, and audit logs.   
  
2.3 Software Interface   
The system interacts with the following software components and data sources:   
- \*\*Database System\*\*:   
 - \*\*Role\*\*: Stores and retrieves asset records, audit logs, authentication logs, permission records, user accounts, asset categories, locations, usage records, transfer records, and maintenance records.   
 - \*\*Interaction Method\*\*: The system uses SQL queries to interact with the database for CRUD (Create, Read, Update, Delete) operations.   
 - \*\*Inputs/Outputs\*\*:   
 - Input: Asset data, audit log entries, authentication events, permission assignments, user account details, asset categories, locations, usage records, transfer records, and maintenance records.   
 - Output: Asset records, audit logs, authentication logs, permission records, user accounts, asset categories, locations, usage records, transfer records, and maintenance records.   
  
- \*\*Email Notification Service\*\*:   
 - \*\*Role\*\*: Sends email notifications to users and administrators for system events such as asset registration, approval decisions, and report readiness.   
 - \*\*Interaction Method\*\*: The system uses an email API to send emails.   
 - \*\*Inputs/Outputs\*\*:   
 - Input: Recipient’s email address, message content, and event details.   
 - Output: Email notification sent to the recipient or logged as a failure in the audit log.   
  
- \*\*Data Export Tools\*\*:   
 - \*\*Role\*\*: Exports data in formats such as CSV, Excel, or PDF.   
 - \*\*Interaction Method\*\*: The system uses libraries or tools to generate export files.   
 - \*\*Inputs/Outputs\*\*:   
 - Input: Export format and optional filters (e.g., asset type, location, status).   
 - Output: Export file generated and available for download or email delivery.   
  
- \*\*Data Import Tools\*\*:   
 - \*\*Role\*\*: Imports asset data from external files (e.g., CSV, Excel) into the system.   
 - \*\*Interaction Method\*\*: The system uses file parsing libraries to read and process imported data.   
 - \*\*Inputs/Outputs\*\*:   
 - Input: Source file (e.g., CSV, Excel) with asset data.   
 - Output: Asset records stored in the database and audit log entry.   
  
2.4 Communication Interface   
The system communicates with external entities via the following means:   
- \*\*Email Notifications\*\*:   
 - \*\*Role\*\*: Sends and receives email notifications for system events.   
 - \*\*Interaction Method\*\*: Uses SMTP (Simple Mail Transfer Protocol) to send emails and possibly IMAP/POP3 to handle failed delivery logs.   
 - \*\*Inputs/Outputs\*\*:   
 - Input: Recipient’s email address, message content, and event details.   
 - Output: Email notification sent to the recipient or logged as a failure in the audit log.   
  
- \*\*Web Browsing\*\*:   
 - \*\*Role\*\*: Allows users to access the system through web browsers.   
 - \*\*Interaction Method\*\*: The system is accessible via HTTP/HTTPS protocols and supports standard web technologies such as HTML, CSS, and JavaScript.   
 - \*\*Inputs/Outputs\*\*:   
 - Input: User input through web forms and navigation actions.   
 - Output: Dynamic web pages and user feedback (e.g., success or error messages).   
  
- \*\*API Communication\*\*:   
 - \*\*Role\*\*: The system may expose APIs for integration with other internal or external systems.   
 - \*\*Interaction Method\*\*: RESTful APIs are used to allow external systems to interact with the asset management system.   
 - \*\*Inputs/Outputs\*\*:   
 - Input: External requests for asset data, usage records, or report generation.   
 - Output: Structured data responses (e.g., JSON or XML) containing the requested information.   
  
- \*\*Internal Messaging (for Approval Workflows)\*\*:   
 - \*\*Role\*\*: Facilitates the approval workflow by sending internal messages or notifications to administrators.   
 - \*\*Interaction Method\*\*: Uses in-system notifications or message queues to inform administrators of pending approval requests.   
 - \*\*Inputs/Outputs\*\*:   
 - Input: Approval request details and user identifiers.   
 - Output: Notification to administrators for review and decision-making.   
  
This section ensures that all external data sources and interaction methods are clearly defined and aligned with the functional requirements, providing developers with a comprehensive understanding of the system's external dependencies and communication protocols.

# Use Case

Use Case Name: Asset Registration   
Use Case ID: UC-01   
Actors: User, Administrator, Database   
Preconditions:   
- The user is authenticated and has the necessary permissions for asset registration.   
- The asset data to be registered is available and valid.   
- The system is connected to the database.   
  
Postconditions:   
- The asset information is successfully stored in the database.   
- An audit log is created to record the registration event.   
- The user is notified of the successful registration via an email notification.   
  
Main Flow:   
1. The user initiates the asset registration process by selecting the "Register Asset" option in the system.   
2. The user fills out the asset registration form with the required information (e.g., asset name, type, description, etc.).   
3. The system validates the input data and checks for completeness.   
4. The system requests approval from the administrator for the asset registration.   
5. The administrator reviews the asset registration request and approves it.   
6. The system saves the asset record into the database.   
7. The system generates an audit log entry for the asset registration.   
8. The system sends an email notification to the user confirming the 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 data.   
2. If the administrator rejects the asset registration request, the system informs the user of the rejection and provides the reason.   
3. If the system fails to connect to the database during asset registration, the system displays an error message and logs the failure in the authentication log.  
  
Use Case Name: View Asset Details   
Use Case ID: UC-05   
Actors: User, Administrator, Database, Authentication Log, Email Notification   
  
Preconditions:   
- The user is authenticated and has the necessary permissions to view asset details.   
- The asset record exists in the database.   
- The system is connected to the database.   
  
Postconditions:   
- The user is able to view detailed information about the selected asset.   
- The system logs the access event in the audit log.   
- If required, the user is notified via email about any changes or updates to the asset.   
  
Main Flow:   
1. The user selects an asset from the asset list or searches for an asset using a specific identifier.   
2. The system retrieves the asset record from the database.   
3. The system displays the asset details on the user interface (e.g., name, type, status, owner, location, etc.).   
4. The system logs the view action in the audit log.   
5. If configured, the system checks for any pending notifications related to the asset and sends an email to the user if applicable.   
  
Alternative Flow:   
1. If the asset record does not exist, the system displays an error message indicating that the asset could not be found.   
2. If the user does not have permission to view the asset, the system denies access and logs the unauthorized attempt in the authentication log.   
3. If the system fails to connect to the database, the system displays an error message and logs the failure in the authentication log.  
  
Use Case Name: Modify Asset Information   
Use Case ID: UC-02   
Actors: User, Administrator, Database, Audit Log, Email Notification   
  
Preconditions:   
- The user is authenticated and has the necessary permissions for asset modification.   
- The asset record to be modified exists in the database.   
- The system is connected to the database.   
  
Postconditions:   
- The asset information is successfully updated in the database.   
- An audit log is created to record the modification event.   
- The administrator is notified of the modification request via an email notification.   
- If approved, the user is notified of the successful modification via an email notification.   
  
Main Flow:   
1. The user selects an asset from the asset list or searches for an asset using a specific identifier.   
2. The system retrieves the asset record from the database.   
3. The user modifies the asset information as needed.   
4. The system validates the updated data and checks for completeness.   
5. The system submits the modification request for administrator approval.   
6. The administrator reviews the modification request and approves it.   
7. The system updates the asset record in the database.   
8. The system generates an audit log entry for the modification.   
9. The system sends an email notification to the user confirming the 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 data.   
2. If the administrator rejects the modification request, the system informs the user of the rejection and provides the reason.   
3. If the asset record does not exist, the system displays an error message indicating that the asset could not be found.   
4. If the user does not have permission to modify the asset, the system denies the request and logs the unauthorized attempt in the authentication log.   
5. If the system fails to connect to the database during modification, the system displays an error message and logs the failure in the authentication log.  
  
Use Case Name: Delete Asset   
Use Case ID: UC-03   
Actors: User, Administrator, Database, Audit Log, Email Notification   
  
Preconditions:   
- The user is authenticated and has the necessary permissions for asset deletion.   
- The asset record to be deleted exists in the database.   
- The system is connected to the database.   
  
Postconditions:   
- The asset record is successfully removed from the database.   
- An audit log is created to record the deletion event.   
- The administrator is notified of the deletion request via email.   
- If approved, the user is notified of the successful deletion via email.   
  
Main Flow:   
1. The user selects an asset from the asset list or searches for an asset using a specific identifier.   
2. The user initiates the deletion process by selecting the "Delete Asset" option.   
3. The system confirms the deletion with the user to prevent accidental removal.   
4. The system submits the deletion request for administrator approval.   
5. The administrator reviews the deletion request and approves it.   
6. The system deletes the asset record from the database.   
7. The system logs the deletion event in the audit log.   
8. The system sends an email notification to the user confirming the deletion.   
  
Alternative Flow:   
1. If the user cancels the deletion confirmation, the system terminates the process and returns to the asset list.   
2. If the administrator rejects the deletion request, the system informs the user and logs the rejection reason in the audit log.   
3. If the asset record does not exist, the system displays an error message indicating that the asset could not be found.   
4. If the user does not have permission to delete the asset, the system denies the request and logs the unauthorized attempt in the authentication log.   
5. If the system fails to connect to the database during deletion, the system displays an error message and logs the failure in the authentication log.  
  
Use Case Name: View Asset Usage Records   
Use Case ID: UC-06   
Actors: User, Administrator, Database, Audit Log, Email Notification   
  
Preconditions:   
- The user is authenticated and has the necessary permissions to view asset usage records.   
- The asset record and its associated usage records exist in the database.   
- The system is connected to the database.   
  
Postconditions:   
- The user is able to view the usage history of the selected asset.   
- The system logs the access event in the audit log.   
- If configured, the system sends an email notification to the user summarizing the usage records.   
  
Main Flow:   
1. The user selects an asset from the asset list or searches for an asset using a specific identifier.   
2. The user clicks the "View Usage Records" option for the selected asset.   
3. The system retrieves the asset usage records from the database.   
4. The system displays the usage records on the user interface (e.g., user who used the asset, date, duration, purpose).   
5. The system logs the view action in the audit log.   
6. If configured, the system sends an email notification to the user with a summary of the usage records.   
  
Alternative Flow:   
1. If the asset usage records do not exist, the system displays a message indicating no usage records are available.   
2. If the user does not have permission to view the usage records, the system denies access and logs the unauthorized attempt in the authentication log.   
3. If the system fails to connect to the database, it displays an error message and logs the failure in the authentication log.  
  
Use Case Name: Record Asset Usage   
Use Case ID: UC-04   
Actors: User, Administrator, Database, Audit Log, Email Notification, Permission Approval Workflow   
  
Preconditions:   
- The user is authenticated and has the necessary permissions to record asset usage.   
- The asset record exists in the database.   
- The system is connected to the database.   
- The permission approval workflow is enabled for asset usage tracking.   
  
Postconditions:   
- The asset usage record is successfully stored in the database.   
- An audit log is created to record the usage event.   
- If approval is required, the administrator is notified via email and approves the usage.   
- The user is notified via email of the successful recording of the usage.   
  
Main Flow:   
1. The user selects an asset from the asset list or searches for an asset using a specific identifier.   
2. The user initiates the asset usage recording process by selecting the "Record Usage" option.   
3. The user enters the required usage details (e.g., start time, end time, purpose, quantity used).   
4. The system validates the input data and checks for completeness.   
5. If permission is required, the system submits the usage request for administrator approval.   
6. The administrator reviews the usage request and approves it.   
7. The system saves the usage record into the database.   
8. The system logs the usage event in the audit log.   
9. The system sends an email notification to the user confirming the successful recording of the usage.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the user to correct the data.   
2. If the asset record does not exist, the system displays an error message indicating that the asset could not be found.   
3. If the user does not have permission to record asset usage, the system denies the request and logs the unauthorized attempt in the authentication log.   
4. If the administrator rejects the usage request, the system informs the user of the rejection and logs the reason in the audit log.   
5. If the system fails to connect to the database during usage recording, it displays an error message and logs the failure in the authentication log.  
  
Use Case Name: Generate Asset Reports   
Use Case ID: UC-07   
Actors: User, Administrator, Database, Report, Audit Log, Email Notification   
  
Preconditions:   
- The user is authenticated and has the necessary permissions to generate asset reports.   
- The system is connected to the database.   
- The required asset data is available in the database.   
  
Postconditions:   
- The asset report is generated and made available for download or viewing.   
- The system logs the report generation event in the audit log.   
- The user is notified via email about the report availability.   
  
Main Flow:   
1. The user selects the "Generate Asset Report" option from the system menu.   
2. The user chooses the report type (e.g., asset inventory, usage summary, depreciation report).   
3. The user specifies the time range and any filters (e.g., asset category, location, status).   
4. The system retrieves the relevant asset data from the database.   
5. The system processes the data and generates the report in the selected format (e.g., PDF, Excel).   
6. The system logs the report generation in the audit log.   
7. The system provides the report for download or viewing by the user.   
8. The system sends an email notification to the user confirming the report is ready.   
  
Alternative Flow:   
1. If the user does not have permission to generate the report, the system denies the request and logs the unauthorized attempt in the authentication log.   
2. If the system fails to retrieve data from the database, it displays an error message and logs the failure in the authentication log.   
3. If no asset data matches the report criteria, the system generates a report with a message indicating no data was found.   
4. If the system fails to generate the report, it displays an error message and logs the failure in the audit log.   
5. If the email notification fails to send, the system logs the failure in the audit log and informs the user.  
  
Use Case Name: View Report Data   
Use Case ID: UC-08   
Actors: User, Administrator, Database, Report, Audit Log, Email Notification   
  
Preconditions:   
- The user is authenticated and has the necessary permissions to view report data.   
- The report data exists in the database.   
- The system is connected to the database.   
  
Postconditions:   
- The user is able to view the requested report data.   
- The system logs the report data access event in the audit log.   
- If configured, the user is notified via email of any report-related updates or alerts.   
  
Main Flow:   
1. The user selects the "View Report Data" option from the system menu.   
2. The user chooses the specific report to view (e.g., asset usage, inventory status, maintenance history).   
3. The system retrieves the report data from the database.   
4. The system displays the report data in a structured and user-friendly format.   
5. The system logs the view action in the audit log.   
6. If configured, the system checks for any pending notifications related to the report and sends an email to the user if applicable.   
  
Alternative Flow:   
1. If the requested report data does not exist, the system displays a message indicating no data is available.   
2. If the user does not have permission to view the report, the system denies access and logs the unauthorized attempt in the authentication log.   
3. If the system fails to connect to the database during report data retrieval, it displays an error message and logs the failure in the authentication log.   
4. If the system encounters an error while displaying the report data, it logs the error in the audit log and informs the user.   
5. If the email notification fails to send, the system logs the failure in the audit log and informs the user.  
  
Use Case Name: Approve Asset Usage   
Use Case ID: UC-09   
Actors: Administrator, User, Permission Approval Workflow, Database, Audit Log, Email Notification   
  
Preconditions:   
- The user has submitted an asset usage request that requires approval.   
- The administrator is authenticated and has the necessary permissions to approve asset usage.   
- The system is connected to the database.   
- The permission approval workflow is enabled.   
  
Postconditions:   
- The asset usage request is approved or rejected by the administrator.   
- The system updates the usage record status in the database.   
- An audit log is created to record the approval or rejection event.   
- The user is notified via email of the approval or rejection decision.   
  
Main Flow:   
1. The administrator receives an email notification or system alert regarding a pending asset usage request.   
2. The administrator logs into the system and navigates to the "Pending Approvals" section.   
3. The administrator selects the asset usage request for review.   
4. The system displays the usage details (e.g., asset name, user, time, purpose).   
5. The administrator approves or rejects the request.   
6. The system updates the usage record in the database with the approval status.   
7. The system logs the approval or rejection action in the audit log.   
8. The system sends an email notification to the user informing them of the decision.   
  
Alternative Flow:   
1. If the system fails to update the usage record in the database, it displays an error message and logs the failure in the authentication log.   
2. If the user does not have permission to use the asset, the system automatically denies the request and logs the rejection reason.   
3. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.   
4. If the administrator does not respond within a configured time period, the system escalates the request to a higher-level administrator and logs the escalation.  
  
Use Case Name: Configure Workflow Rules   
Use Case ID: UC-10   
Actors: Administrator, Workflow Approval, Database, Audit Log, Email Notification   
  
Preconditions:   
- The administrator is authenticated and has the necessary permissions to configure workflow rules.   
- The system is connected to the database.   
- The workflow approval module is active and accessible.   
  
Postconditions:   
- The workflow rules are successfully updated or created in the system.   
- The changes are saved in the database.   
- An audit log is created to record the configuration event.   
- If configured, the administrator is notified via email about the successful configuration.   
  
Main Flow:   
1. The administrator navigates to the "Workflow Configuration" section of the system.   
2. The administrator selects the asset type or usage category to which the workflow rule applies.   
3. The administrator defines the workflow rule (e.g., approval level, conditions, notification settings).   
4. The system validates the rule configuration and checks for conflicts with existing rules.   
5. The system saves the workflow rule in the database.   
6. The system logs the configuration action in the audit log.   
7. The system sends an email notification to the administrator confirming the workflow rule is configured.   
  
Alternative Flow:   
1. If the workflow rule conflicts with an existing rule, the system displays a warning and prompts the administrator to resolve the conflict.   
2. If the system fails to validate the rule configuration, it displays an error message and prevents the rule from being saved.   
3. If the system fails to connect to the database during rule configuration, it displays an error message and logs the failure in the authentication log.   
4. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: Assign User Permissions   
Use Case ID: UC-11   
Actors: Administrator, User, Permission Approval Workflow, Database, Audit Log, Email Notification   
  
Preconditions:   
- The administrator is authenticated and has the necessary permissions to assign user permissions.   
- The user whose permissions are to be assigned exists in the system.   
- The system is connected to the database.   
- The permission approval workflow is enabled if required.   
  
Postconditions:   
- The user's permissions are updated in the database.   
- An audit log is created to record the permission assignment event.   
- If approval is required, the administrator receives confirmation of the approval or rejection via email.   
- The user is notified via email of the updated permissions.   
  
Main Flow:   
1. The administrator navigates to the "User Permissions" section of the system.   
2. The administrator selects a user from the user list or searches for a user using an identifier.   
3. The administrator chooses the permissions to assign (e.g., view, modify, delete, report generation).   
4. If the permission approval workflow is enabled, the system submits the permission assignment for approval.   
5. The system updates the user's permission record in the database.   
6. The system logs the permission assignment in the audit log.   
7. The system sends an email notification to the user confirming the updated permissions.   
  
Alternative Flow:   
1. If the selected user does not exist, the system displays an error message.   
2. If the system fails to connect to the database, it displays an error message and logs the failure in the authentication log.   
3. If the permission approval workflow is enabled and the request is rejected, the system updates the audit log with the rejection reason and informs the administrator.   
4. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.   
5. If the administrator does not have permission to assign permissions, the system denies the request and logs the unauthorized attempt in the authentication log.  
  
Use Case Name: Modify Permissions   
Use Case ID: UC-12   
Actors: Administrator, Permission Approval Workflow, Database, Audit Log, Email Notification   
  
Preconditions:   
- The administrator is authenticated and has the necessary permissions to modify permissions.   
- The permission to be modified exists in the system.   
- The system is connected to the database.   
- The permission approval workflow is enabled if required.   
  
Postconditions:   
- The permission is successfully updated in the database.   
- An audit log is created to record the modification event.   
- If approval is required, the administrator receives confirmation of the approval or rejection via email.   
- The user affected by the permission modification is notified via email.   
  
Main Flow:   
1. The administrator navigates to the "Permissions Management" section of the system.   
2. The administrator selects a specific permission or permission group to modify.   
3. The administrator updates the permission settings (e.g., grant or revoke access to certain functions or assets).   
4. If the permission approval workflow is enabled, the system submits the modification request for approval.   
5. The system updates the permission record in the database.   
6. The system logs the modification event in the audit log.   
7. The system sends an email notification to the affected user(s) confirming the updated permissions.   
  
Alternative Flow:   
1. If the selected permission does not exist, the system displays an error message.   
2. If the system fails to connect to the database, it displays an error message and logs the failure in the authentication log.   
3. If the permission approval workflow is enabled and the request is rejected, the system updates the audit log with the rejection reason and informs the administrator.   
4. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.   
5. If the administrator does not have permission to modify permissions, the system denies the request and logs the unauthorized attempt in the authentication log.  
  
Use Case Name: Register New Users   
Use Case ID: UC-13   
Actors: Administrator, User, Database, Authentication Log, Email Notification   
  
Preconditions:   
- The administrator is authenticated and has the necessary permissions to register new users.   
- The system is connected to the database.   
- The user registration form is accessible.   
  
Postconditions:   
- The new user information is successfully stored in the database.   
- An authentication log is created to record the registration event.   
- The new user is notified via email with a confirmation and login instructions.   
  
Main Flow:   
1. The administrator navigates to the "User Registration" section of the system.   
2. The administrator fills out the user registration form with the required information (e.g., username, password, role, contact details).   
3. The system validates the input data and checks for completeness.   
4. The system saves the new user record in the database.   
5. The system logs the user registration event in the authentication log.   
6. The system sends an email notification to the new user confirming the registration and providing login instructions.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the data.   
2. If the system fails to connect to the database during registration, it displays an error message and logs the failure in the authentication log.   
3. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.   
4. If the new user already exists in the database, the system displays a message indicating the user is already registered.  
  
Use Case Name: Manage User Accounts   
Use Case ID: UC-14   
Actors: Administrator, User, Database, Authentication Log, Email Notification   
  
Preconditions:   
- The administrator is authenticated and has the necessary permissions to manage user accounts.   
- The system is connected to the database.   
- The user account to be managed exists in the system (if applicable).   
  
Postconditions:   
- The user account is successfully created, updated, or deleted in the database.   
- An audit log is created to record the account management action.   
- The user is notified via email about account changes.   
- Any unauthorized access attempt is logged in the authentication log.   
  
Main Flow:   
1. The administrator navigates to the "User Account Management" section of the system.   
2. The administrator selects an action (e.g., "Create New User," "Edit User," "Delete User").   
3. If creating a new user, the administrator fills out the user registration form with the required information.   
4. If editing or deleting an existing user, the administrator selects the user from the user list or searches using an identifier.   
5. The system validates the input data and checks for completeness.   
6. The system performs the requested action (create, update, or delete) on the user account in the database.   
7. The system logs the account management action in the audit log.   
8. The system sends an email notification to the affected user(s) confirming the account change.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the data.   
2. If the system fails to connect to the database during account management, it displays an error message and logs the failure in the authentication log.   
3. If the user account does not exist (for update or delete actions), the system displays an error message.   
4. If the administrator does not have permission to manage user accounts, the system denies the request and logs the unauthorized attempt in the authentication log.   
5. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: Import Asset Data   
Use Case ID: UC-15   
Actors: User, Administrator, Database, Data Import/Export, Audit Log, Email Notification   
  
Preconditions:   
- The user is authenticated and has the necessary permissions to import asset data.   
- The system is connected to the database.   
- The data import/export module is enabled.   
- The source file (e.g., CSV, Excel) containing asset data is prepared and accessible.   
  
Postconditions:   
- The asset data is successfully imported into the database.   
- An audit log is created to record the import event.   
- If approval is required, the administrator is notified via email and approves the import.   
- The user is notified via email of the successful import or any errors encountered.   
  
Main Flow:   
1. The user navigates to the "Data Import/Export" section of the system.   
2. The user selects the "Import Asset Data" option and uploads the file containing asset data.   
3. The system validates the file format and checks for data consistency and completeness.   
4. If approval is required, the system submits the import request for administrator approval.   
5. The administrator reviews the import request and approves it.   
6. The system processes the file and imports the asset records into the database.   
7. The system logs the import event in the audit log.   
8. The system sends an email notification to the user confirming the successful import.   
  
Alternative Flow:   
1. If the file format is invalid or unsupported, the system displays an error message and prompts the user to upload a valid file.   
2. If the data is inconsistent or incomplete, the system logs the error and sends a notification to the user listing the issues.   
3. If the system fails to connect to the database during the import process, it displays an error message and logs the failure in the authentication log.   
4. If the administrator rejects the import request, the system logs the rejection in the audit log and informs the user of the reason.   
5. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: Export Asset Data   
Use Case ID: UC-16   
Actors: User, Administrator, Database, Data Import/Export, Audit Log, Email Notification   
  
Preconditions:   
- The user is authenticated and has the necessary permissions to export asset data.   
- The system is connected to the database.   
- The required asset data exists in the database.   
- The data import/export module is enabled.   
  
Postconditions:   
- The asset data is successfully exported in the selected format (e.g., CSV, Excel, PDF).   
- An audit log is created to record the export event.   
- If approval is required, the administrator is notified via email and approves the export.   
- The user is notified via email of the successful export or any errors encountered.   
  
Main Flow:   
1. The user navigates to the "Data Import/Export" section of the system.   
2. The user selects the "Export Asset Data" option and specifies the export format (e.g., CSV, Excel).   
3. The user chooses the asset criteria for the export (e.g., asset type, status, time range).   
4. The system validates the export request and checks for data availability.   
5. If approval is required, the system submits the export request for administrator approval.   
6. The administrator reviews the export request and approves it.   
7. The system retrieves the relevant asset data from the database.   
8. The system processes the data and generates the export file.   
9. The system logs the export event in the audit log.   
10. The system provides the export file for download or sends it to the user via email.   
11. The system sends an email notification to the user confirming the export is ready.   
  
Alternative Flow:   
1. If the export format is invalid or unsupported, the system displays an error message and prompts the user to select a valid format.   
2. If the system fails to retrieve data from the database, it displays an error message and logs the failure in the authentication log.   
3. If no asset data matches the export criteria, the system generates an export file with a message indicating no data was found.   
4. If the system fails to generate the export file, it displays an error message and logs the failure in the audit log.   
5. If the administrator rejects the export request, the system logs the rejection in the audit log and informs the user of the reason.   
6. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: View Audit Logs   
Use Case ID: UC-17   
Actors: User, Administrator, Database, Audit Log   
  
Preconditions:   
- The user is authenticated and has the necessary permissions to view audit logs.   
- The system is connected to the database.   
- Audit logs exist in the system.   
  
Postconditions:   
- The user is able to view the requested audit log entries.   
- The system logs the access to the audit log in the audit log.   
- If configured, the user is notified via email about any audit-related updates.   
  
Main Flow:   
1. The user navigates to the "Audit Logs" section of the system.   
2. The user selects a time range or filters the logs by actor, action, or asset.   
3. The system retrieves the relevant audit log entries from the database.   
4. The system displays the audit logs in a structured and user-friendly format.   
5. The system logs the view action in the audit log.   
6. If configured, the system sends an email notification to the user summarizing the audit logs.   
  
Alternative Flow:   
1. If the requested audit logs do not exist, the system displays a message indicating no data is available.   
2. If the user does not have permission to view the audit logs, the system denies access and logs the unauthorized attempt in the authentication log.   
3. If the system fails to connect to the database during audit log retrieval, it displays an error message and logs the failure in the authentication log.   
4. If the system encounters an error while displaying the audit logs, it logs the error in the audit log and informs the user.   
5. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: View Authentication Logs   
Use Case ID: UC-18   
Actors: User, Administrator, Authentication Log, Database, Email Notification   
  
Preconditions:   
- The user is authenticated and has the necessary permissions to view authentication logs.   
- The system is connected to the database.   
- Authentication log entries exist in the system.   
  
Postconditions:   
- The user is able to view the requested authentication log entries.   
- The system logs the access to the authentication logs in the audit log.   
- If configured, the user is notified via email about any authentication-related updates.   
  
Main Flow:   
1. The user navigates to the "Authentication Logs" section of the system.   
2. The user selects a time range or filters the logs by actor, action, or status.   
3. The system retrieves the relevant authentication log entries from the database.   
4. The system displays the authentication logs in a structured and user-friendly format.   
5. The system logs the view action in the audit log.   
6. If configured, the system sends an email notification to the user summarizing the logs.   
  
Alternative Flow:   
1. If the requested authentication logs do not exist, the system displays a message indicating no data is available.   
2. If the user does not have permission to view the authentication logs, the system denies access and logs the unauthorized attempt in the authentication log.   
3. If the system fails to connect to the database during log retrieval, it displays an error message and logs the failure in the authentication log.   
4. If the system encounters an error while displaying the logs, it logs the error in the audit log and informs the user.   
5. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: Send Email Notifications   
Use Case ID: UC-19   
Actors: System, User, Email Notification, Administrator, Audit Log   
  
Preconditions:   
- The system is configured to send email notifications.   
- The user or administrator has initiated an action that triggers an email notification.   
- The email notification module is active and accessible.   
- A valid email address is associated with the recipient.   
  
Postconditions:   
- The email notification is successfully sent to the intended recipient.   
- The system logs the email notification event in the audit log.   
- If the email fails to send, the system logs the failure in the audit log and alerts the administrator.   
  
Main Flow:   
1. The system identifies an event that requires an email notification (e.g., asset registration, usage approval, report generation).   
2. The system prepares the email content, including relevant details and a confirmation message.   
3. The system verifies the recipient's email address.   
4. The system sends the email notification to the designated recipient.   
5. The system logs the successful email notification in the audit log.   
  
Alternative Flow:   
1. If the recipient's email address is invalid, the system logs the error in the audit log and displays a warning to the administrator.   
2. If the email notification fails to send due to server issues or network errors, the system logs the failure in the audit log and alerts the administrator.   
3. If no email notification is configured for the event, the system does not send an email and proceeds with the action.   
4. If the email notification module is not active, the system logs the inactivity and displays a warning to the administrator.  
  
Use Case Name: Manage Email Templates   
Use Case ID: UC-20   
Actors: Administrator, Email Notification, Database, Audit Log   
  
Preconditions:   
- The administrator is authenticated and has the necessary permissions to manage email templates.   
- The system is connected to the database.   
- The email notification module is enabled.   
- The system contains a set of predefined or existing email templates.   
  
Postconditions:   
- The email template is successfully created, modified, or deleted in the database.   
- An audit log is created to record the email template management action.   
- The system updates the email notification module with the new template(s).   
- If an error occurs, it is logged in the audit log and the administrator is informed.   
  
Main Flow:   
1. The administrator navigates to the "Email Templates" section of the system.   
2. The administrator selects an action: "Create New Template," "Edit Existing Template," or "Delete Template."   
3. If creating or editing a template, the administrator fills in the template details (e.g., subject, body, placeholders).   
4. The system validates the template content and checks for required fields.   
5. The system saves the template to the database.   
6. The system logs the action in the audit log.   
7. The system updates the email notification module with the new or modified template.   
  
Alternative Flow:   
1. If the template content is invalid or incomplete, the system displays an error message and prompts the administrator to correct the data.   
2. If the system fails to connect to the database, it displays an error message and logs the failure in the authentication log.   
3. If the selected template does not exist (for edit or delete actions), the system displays an error message.   
4. If the administrator does not have permission to manage email templates, the system denies the request and logs the unauthorized attempt in the authentication log.   
5. If the email notification module is not enabled, the system logs the inactivity and displays a warning to the administrator.  
  
Use Case Name: View Asset Category   
Use Case ID: UC-21   
Actors: User, Administrator, Database, Audit Log, Email Notification   
  
Preconditions:   
- The user is authenticated and has the necessary permissions to view asset categories.   
- The system is connected to the database.   
- Asset category records exist in the database.   
  
Postconditions:   
- The user is able to view the details of a specific asset category.   
- The system logs the access event in the audit log.   
- If configured, the user is notified via email about any changes or updates to the asset category.   
  
Main Flow:   
1. The user navigates to the "Asset Categories" section of the system.   
2. The user selects an asset category from the list or searches for it using a specific identifier.   
3. The system retrieves the selected asset category record from the database.   
4. The system displays the asset category details on the user interface (e.g., category name, description, associated assets, rules).   
5. The system logs the view action in the audit log.   
6. If configured, the system checks for any pending notifications related to the asset category and sends an email to the user if applicable.   
  
Alternative Flow:   
1. If the requested asset category does not exist, the system displays a message indicating no data is available.   
2. If the user does not have permission to view the asset category, the system denies access and logs the unauthorized attempt in the authentication log.   
3. If the system fails to connect to the database during asset category retrieval, it displays an error message and logs the failure in the authentication log.   
4. If the system encounters an error while displaying the asset category details, it logs the error in the audit log and informs the user.   
5. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: Manage Location   
Use Case ID: UC-22   
Actors: Administrator, Database, Audit Log, Email Notification   
  
Preconditions:   
- The administrator is authenticated and has the necessary permissions to manage locations.   
- The system is connected to the database.   
- The location data to be managed exists in the database (for update or delete actions).   
- The email notification module is enabled if email alerts are required.   
  
Postconditions:   
- The location information is successfully created, updated, or deleted in the database.   
- An audit log is created to record the location management event.   
- If configured, the system sends an email notification to relevant users about the location change.   
- Any unauthorized access attempt is logged in the authentication log.   
  
Main Flow:   
1. The administrator navigates to the "Location Management" section of the system.   
2. The administrator selects an action: "Create New Location," "Edit Location," or "Delete Location."   
3. For "Create New Location," the administrator fills in the required details (e.g., location name, address, department, capacity).   
4. For "Edit Location," the administrator selects an existing location and updates its information.   
5. For "Delete Location," the administrator selects an existing location and confirms the deletion.   
6. The system validates the input data and checks for completeness.   
7. The system performs the requested action (create, update, or delete) on the location record in the database.   
8. The system logs the location management action in the audit log.   
9. If configured, the system sends an email notification to relevant users (e.g., users associated with the location) about the change.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the data.   
2. If the system fails to connect to the database, it displays an error message and logs the failure in the authentication log.   
3. If the requested location does not exist (for update or delete actions), the system displays an error message.   
4. If the administrator does not have permission to manage locations, the system denies the request and logs the unauthorized attempt in the authentication log.   
5. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: Manage Department   
Use Case ID: UC-23   
Actors: Administrator, Database, Audit Log, Email Notification   
  
Preconditions:   
- The administrator is authenticated and has the necessary permissions to manage departments.   
- The system is connected to the database.   
- The department data to be managed exists in the database (for update or delete actions).   
- The email notification module is enabled if email alerts are required.   
  
Postconditions:   
- The department information is successfully created, updated, or deleted in the database.   
- An audit log is created to record the department management event.   
- If configured, the system sends an email notification to relevant users or administrators about the department change.   
- Any unauthorized access attempt is logged in the authentication log.   
  
Main Flow:   
1. The administrator navigates to the "Department Management" section of the system.   
2. The administrator selects an action: "Create New Department," "Edit Department," or "Delete Department."   
3. For "Create New Department," the administrator fills in the required details (e.g., department name, description, location, head of department).   
4. For "Edit Department," the administrator selects an existing department and updates its information.   
5. For "Delete Department," the administrator selects an existing department and confirms the deletion.   
6. The system validates the input data and checks for completeness.   
7. The system performs the requested action (create, update, or delete) on the department record in the database.   
8. The system logs the department management action in the audit log.   
9. If configured, the system sends an email notification to relevant users (e.g., users assigned to the department) about the change.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the data.   
2. If the system fails to connect to the database, it displays an error message and logs the failure in the authentication log.   
3. If the requested department does not exist (for update or delete actions), the system displays an error message.   
4. If the administrator does not have permission to manage departments, the system denies the request and logs the unauthorized attempt in the authentication log.   
5. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: View Asset Transfer Records   
Use Case ID: UC-24   
Actors: User, Administrator, Database, Audit Log, Email Notification   
  
Preconditions:   
- The user is authenticated and has the necessary permissions to view asset transfer records.   
- The asset transfer records exist in the database.   
- The system is connected to the database.   
  
Postconditions:   
- The user is able to view the transfer history of the selected asset.   
- The system logs the access event in the audit log.   
- If configured, the system sends an email notification to the user summarizing the transfer records.   
  
Main Flow:   
1. The user selects an asset from the asset list or searches for an asset using a specific identifier.   
2. The user clicks the "View Transfer Records" option for the selected asset.   
3. The system retrieves the asset transfer records from the database.   
4. The system displays the transfer records on the user interface (e.g., transfer date, source location, destination location, responsible administrator, reason for transfer).   
5. The system logs the view action in the audit log.   
6. If configured, the system sends an email notification to the user with a summary of the transfer records.   
  
Alternative Flow:   
1. If the requested asset transfer records do not exist, the system displays a message indicating no transfer records are available for the selected asset.   
2. If the user does not have permission to view asset transfer records, the system denies access and logs the unauthorized attempt in the authentication log.   
3. If the system fails to connect to the database during the retrieval process, it displays an error message and logs the failure in the authentication log.   
4. If the system encounters an error while displaying the transfer records, it logs the error in the audit log and informs the user.   
5. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: View Asset Maintenance Records   
Use Case ID: UC-25   
Actors: User, Administrator, Database, Audit Log, Email Notification   
  
Preconditions:   
- The user is authenticated and has the necessary permissions to view asset maintenance records.   
- The asset record and its associated maintenance records exist in the database.   
- The system is connected to the database.   
  
Postconditions:   
- The user is able to view the maintenance history of the selected asset.   
- The system logs the access event in the audit log.   
- If configured, the system sends an email notification to the user summarizing the maintenance records.   
  
Main Flow:   
1. The user selects an asset from the asset list or searches for an asset using a specific identifier.   
2. The user clicks the "View Maintenance Records" option for the selected asset.   
3. The system retrieves the maintenance records associated with the asset from the database.   
4. The system displays the maintenance records on the user interface (e.g., date of maintenance, type of maintenance, responsible technician, cost, remarks).   
5. The system logs the view action in the audit log.   
6. If configured, the system sends an email notification to the user with a summary of the maintenance records.   
  
Alternative Flow:   
1. If the requested maintenance records do not exist, the system displays a message indicating no maintenance records are available for the selected asset.   
2. If the user does not have permission to view maintenance records, the system denies access and logs the unauthorized attempt in the authentication log.   
3. If the system fails to connect to the database during the retrieval process, it displays an error message and logs the failure in the authentication log.   
4. If the system encounters an error while displaying the maintenance records, it logs the error in the audit log and informs the user.   
5. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: Manage Asset Category   
Use Case ID: UC-26   
Actors: Administrator, Database, Audit Log, Email Notification   
  
Preconditions:   
- The administrator is authenticated and has the necessary permissions to manage asset categories.   
- The system is connected to the database.   
- The asset category data to be managed exists in the database (for update or delete actions).   
- The email notification module is enabled if email alerts are required.   
  
Postconditions:   
- The asset category information is successfully created, updated, or deleted in the database.   
- An audit log is created to record the asset category management event.   
- If configured, the system sends an email notification to relevant users or administrators about the asset category change.   
- Any unauthorized access attempt is logged in the authentication log.   
  
Main Flow:   
1. The administrator navigates to the "Asset Category Management" section of the system.   
2. The administrator selects an action: "Create New Asset Category," "Edit Asset Category," or "Delete Asset Category."   
3. For "Create New Asset Category," the administrator fills in the required details (e.g., category name, description, classification, associated rules).   
4. For "Edit Asset Category," the administrator selects an existing asset category and updates its information.   
5. For "Delete Asset Category," the administrator selects an existing asset category and confirms the deletion.   
6. The system validates the input data and checks for completeness.   
7. The system performs the requested action (create, update, or delete) on the asset category record in the database.   
8. The system logs the asset category management action in the audit log.   
9. If configured, the system sends an email notification to relevant users (e.g., users who interact with assets in the category) about the change.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the data.   
2. If the system fails to connect to the database, it displays an error message and logs the failure in the authentication log.   
3. If the requested asset category does not exist (for update or delete actions), the system displays an error message.   
4. If the administrator does not have permission to manage asset categories, the system denies the request and logs the unauthorized attempt in the authentication log.   
5. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: Manage Asset Transfer Records   
Use Case ID: UC-27   
Actors: Administrator, User, Database, Audit Log, Email Notification, Asset Transfer Record   
  
Preconditions:   
- The user or administrator is authenticated and has the necessary permissions to manage asset transfer records.   
- The system is connected to the database.   
- The asset transfer record to be managed exists in the database (for update or delete actions).   
- The email notification module is enabled if email alerts are required.   
  
Postconditions:   
- The asset transfer record is successfully created, updated, or deleted in the database.   
- An audit log is created to record the management action.   
- If configured, the system sends an email notification to relevant users or administrators about the asset transfer record change.   
- Any unauthorized access attempt is logged in the authentication log.   
  
Main Flow:   
1. The administrator or authorized user navigates to the "Asset Transfer Records" section of the system.   
2. The administrator or user selects an action: "Create Transfer Record," "Edit Transfer Record," or "Delete Transfer Record."   
3. For "Create Transfer Record," the user or administrator fills in the required transfer details (e.g., asset identifier, source location, destination location, transfer date, reason for transfer, responsible administrator).   
4. For "Edit Transfer Record," the user or administrator selects an existing transfer record and updates its information.   
5. For "Delete Transfer Record," the user or administrator selects an existing transfer record and confirms the deletion.   
6. The system validates the input data and checks for completeness.   
7. The system performs the requested action (create, update, or delete) on the asset transfer record in the database.   
8. The system logs the asset transfer record management action in the audit log.   
9. If configured, the system sends an email notification to relevant users (e.g., asset owner, destination department) about the transfer record change.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the user or administrator to correct the data.   
2. If the system fails to connect to the database, it displays an error message and logs the failure in the authentication log.   
3. If the requested asset transfer record does not exist (for update or delete actions), the system displays an error message.   
4. If the user or administrator does not have permission to manage asset transfer records, the system denies the request and logs the unauthorized attempt in the authentication log.   
5. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.  
  
Use Case Name: Manage Asset Maintenance Records   
Use Case ID: UC-28   
Actors: Administrator, User, Database, Audit Log, Email Notification, Asset Maintenance Record   
  
Preconditions:   
- The user or administrator is authenticated and has the necessary permissions to manage asset maintenance records.   
- The system is connected to the database.   
- The asset maintenance record to be managed exists in the database (for update or delete actions).   
- The email notification module is enabled if email alerts are required.   
  
Postconditions:   
- The asset maintenance record is successfully created, updated, or deleted in the database.   
- An audit log is created to record the maintenance record management event.   
- If configured, the system sends an email notification to relevant users or administrators about the maintenance record change.   
- Any unauthorized access attempt is logged in the authentication log.   
  
Main Flow:   
1. The administrator or authorized user navigates to the "Asset Maintenance Records" section of the system.   
2. The administrator or user selects an action: "Create Maintenance Record," "Edit Maintenance Record," or "Delete Maintenance Record."   
3. For "Create Maintenance Record," the user or administrator fills in the required maintenance details (e.g., asset identifier, maintenance date, type of maintenance, responsible technician, cost, remarks).   
4. For "Edit Maintenance Record," the user or administrator selects an existing maintenance record and updates its information.   
5. For "Delete Maintenance Record," the user or administrator selects an existing maintenance record and confirms the deletion.   
6. The system validates the input data and checks for completeness.   
7. The system performs the requested action (create, update, or delete) on the asset maintenance record in the database.   
8. The system logs the maintenance record management action in the audit log.   
9. If configured, the system sends an email notification to relevant users (e.g., asset owner, maintenance team) about the maintenance record change.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the user or administrator to correct the data.   
2. If the system fails to connect to the database, it displays an error message and logs the failure in the authentication log.   
3. If the requested asset maintenance record does not exist (for update or delete actions), the system displays an error message.   
4. If the user or administrator does not have permission to manage asset maintenance records, the system denies the request and logs the unauthorized attempt in the authentication log.   
5. If the email notification fails to send, the system logs the failure in the audit log and displays a warning to the administrator.