项目文档

# Functional Requirement

# Chapter 1: Functional Requirements  
  
## 1.1 Asset Registration Function   
\*\*Function ID:\*\* FR-01   
\*\*Description:\*\* Allows users with proper permissions to register new assets in the system.   
\*\*Input:\*\* Asset details (Name, Description, CategoryID, Location, PurchaseDate).   
\*\*Output:\*\* A new Asset record in the database with an assigned AssetID.  
  
## 1.2 View Asset Information Function   
\*\*Function ID:\*\* FR-02   
\*\*Description:\*\* Allows users with proper permissions to view detailed information about a specific asset.   
\*\*Input:\*\* Asset identifier (e.g., Name, AssetID, CategoryID).   
\*\*Output:\*\* Displayed asset details (Name, Description, CategoryID, Status, Location, PurchaseDate, Usage History).  
  
## 1.3 Modify Asset Details Function   
\*\*Function ID:\*\* FR-03   
\*\*Description:\*\* Enables users with proper permissions to update the information of an existing asset.   
\*\*Input:\*\* Asset identifier and updated details (e.g., Name, Description, CategoryID, Location).   
\*\*Output:\*\* Updated Asset record in the database, including a new AssetModification entry.  
  
## 1.4 Remove Asset Function   
\*\*Function ID:\*\* FR-04   
\*\*Description:\*\* Allows users with proper permissions to remove an asset from the system.   
\*\*Input:\*\* Asset identifier and confirmation of removal.   
\*\*Output:\*\* Asset is deleted from the database, and a new AssetDeletion record is created.  
  
## 1.5 User Registration Function   
\*\*Function ID:\*\* FR-05   
\*\*Description:\*\* Enables administrators to create new user accounts.   
\*\*Input:\*\* New user details (Name, Email, DepartmentID, Role).   
\*\*Output:\*\* A new User record in the database with a UserID and associated UserRegistration entry.  
  
## 1.6 Assign User Permissions Function   
\*\*Function ID:\*\* FR-06   
\*\*Description:\*\* Allows administrators to assign specific permissions to users based on their role or department.   
\*\*Input:\*\* User identifier and selected Permission(s).   
\*\*Output:\*\* Updated User record in the database and a new PermissionAssignment entry.  
  
## 1.7 Modify User Information Function   
\*\*Function ID:\*\* FR-07   
\*\*Description:\*\* Enables administrators to update the details of an existing user.   
\*\*Input:\*\* User identifier and updated details (Name, Email, DepartmentID, Role).   
\*\*Output:\*\* Updated User record in the database, including a new UserModification entry.  
  
## 1.8 Remove User Function   
\*\*Function ID:\*\* FR-08   
\*\*Description:\*\* Allows administrators to delete a user from the system.   
\*\*Input:\*\* User identifier and confirmation of removal.   
\*\*Output:\*\* User is deleted from the database, and a new UserDeletion record is created.  
  
## 1.9 Administrator Login Function   
\*\*Function ID:\*\* FR-09   
\*\*Description:\*\* Authenticates administrators and grants access to system management functions based on their assigned permissions.   
\*\*Input:\*\* Admin username and password.   
\*\*Output:\*\* Administrator login status and display of the main interface/dashboard.  
  
## 1.10 Manage Departments Function   
\*\*Function ID:\*\* FR-10   
\*\*Description:\*\* Enables administrators to create, update, or remove departments.   
\*\*Input:\*\* Department identifier and updated or new details (Name, Description).   
\*\*Output:\*\* Updated or deleted Department record in the database, including DepartmentMembership updates if necessary.  
  
## 1.11 Add Department Function   
\*\*Function ID:\*\* FR-11   
\*\*Description:\*\* Allows administrators to create a new department.   
\*\*Input:\*\* Department name and description.   
\*\*Output:\*\* A new Department record in the database with an assigned DepartmentID.  
  
## 1.12 Remove Department Function   
\*\*Function ID:\*\* FR-12   
\*\*Description:\*\* Allows administrators to delete a department and reassign or remove associated users and assets.   
\*\*Input:\*\* Department identifier and confirmation of removal.   
\*\*Output:\*\* Department record is deleted from the database, and DepartmentMembership entries are updated.  
  
## 1.13 Create Asset Category Function   
\*\*Function ID:\*\* FR-13   
\*\*Description:\*\* Enables administrators to define new asset categories.   
\*\*Input:\*\* Category name, description, and parent category identifier (if applicable).   
\*\*Output:\*\* A new AssetCategory record in the database with an assigned CategoryID.  
  
## 1.14 Modify Asset Category Function   
\*\*Function ID:\*\* FR-14   
\*\*Description:\*\* Allows administrators to update the details of an existing asset category.   
\*\*Input:\*\* Asset category identifier and updated details (Name, Description).   
\*\*Output:\*\* Updated AssetCategory record in the database and a new CategoryManagement entry.  
  
## 1.15 Remove Asset Category Function   
\*\*Function ID:\*\* FR-15   
\*\*Description:\*\* Enables administrators to delete an asset category and reassign or remove associated assets.   
\*\*Input:\*\* Asset category identifier and confirmation of removal.   
\*\*Output:\*\* AssetCategory record is deleted from the database, and Asset records are updated accordingly.  
  
## 1.16 View Asset Category Function   
\*\*Function ID:\*\* FR-16   
\*\*Description:\*\* Allows users or administrators to view details of an asset category.   
\*\*Input:\*\* Asset category identifier.   
\*\*Output:\*\* Displayed category details (Name, Description, ParentCategoryID, associated Assets).  
  
## 1.17 Manage Permission Assignment Function   
\*\*Function ID:\*\* FR-17   
\*\*Description:\*\* Enables administrators to assign, modify, or revoke permissions for a user.   
\*\*Input:\*\* User identifier and Permission(s) to be assigned, modified, or revoked.   
\*\*Output:\*\* Updated PermissionAssignment record in the database and associated AuditLog entry.  
  
## 1.18 Record Asset Usage Function   
\*\*Function ID:\*\* FR-18   
\*\*Description:\*\* Allows users or administrators to log the usage of an asset.   
\*\*Input:\*\* Asset identifier and usage details (UsageDate, UsageDuration, Purpose).   
\*\*Output:\*\* A new UsageRecord in the database and an AuditLog entry for the usage action.  
  
## 1.19 View Usage Records Function   
\*\*Function ID:\*\* FR-19   
\*\*Description:\*\* Enables users or administrators to view the usage history of a specific asset.   
\*\*Input:\*\* Asset identifier.   
\*\*Output:\*\* Displayed usage records (UsageDate, UsageDuration, Purpose, UserID).  
  
## 1.20 Modify Usage Records Function   
\*\*Function ID:\*\* FR-20   
\*\*Description:\*\* Allows users or administrators to update existing asset usage records.   
\*\*Input:\*\* UsageRecord identifier and updated details (UsageDate, UsageDuration, Purpose).   
\*\*Output:\*\* Updated UsageRecord in the database and an AuditLog entry for the modification.  
  
## 1.21 Delete Usage Records Function   
\*\*Function ID:\*\* FR-21   
\*\*Description:\*\* Enables administrators or users with permissions to delete a specific usage record.   
\*\*Input:\*\* UsageRecord identifier and confirmation of deletion.   
\*\*Output:\*\* UsageRecord is removed from the database and an AuditLog entry is created.  
  
## 1.22 View Audit Log Function   
\*\*Function ID:\*\* FR-22   
\*\*Description:\*\* Allows users or administrators with proper permissions to view audit logs.   
\*\*Input:\*\* Filtering criteria (e.g., timestamp range, affected entity, action type).   
\*\*Output:\*\* Displayed audit log entries (LogID, UserID, AssetID, RecordID, Action, Timestamp, Details).  
  
## 1.23 Generate Audit Report Function   
\*\*Function ID:\*\* FR-23   
\*\*Description:\*\* Enables administrators to generate and optionally send audit reports.   
\*\*Input:\*\* Report generation parameters (e.g., time range, action type).   
\*\*Output:\*\* A structured audit report and an AuditLog entry for the report generation.  
  
## 1.24 Send Email Notification Function   
\*\*Function ID:\*\* FR-24   
\*\*Description:\*\* Allows users or administrators to send email notifications to other users for various system events.   
\*\*Input:\*\* Recipient identifier, email content or template, and event details.   
\*\*Output:\*\* EmailNotification record in the database and an AuditLog entry for the email action.

# External Description

# Chapter 2: External Interfaces  
  
## 2.1 User Interface Output  
  
The system interacts with users through a graphical user interface (GUI), allowing for the input and display of asset, user, and department information, as well as the execution of administrative actions. The following user interface outputs are defined for the system:  
  
- \*\*Asset Registration Interface (FR-01):\*\*   
 Displays a form for entering asset details such as Name, Description, CategoryID, Location, and PurchaseDate. After submission, the system confirms the successful creation of a new asset with an assigned AssetID.  
  
- \*\*View Asset Information Interface (FR-02):\*\*   
 Provides a detailed view of an asset's information, including Name, Description, CategoryID, Status, Location, PurchaseDate, and Usage History. Users can search for an asset using its Name, AssetID, or CategoryID.  
  
- \*\*Modify Asset Details Interface (FR-03):\*\*   
 Allows users to edit asset fields such as Name, Description, CategoryID, and Location. Upon saving, the system updates the Asset record and creates a new AssetModification entry.  
  
- \*\*Remove Asset Interface (FR-04):\*\*   
 Presents a confirmation dialog for asset removal. After confirmation, the system deletes the asset and logs the deletion with an AssetDeletion record.  
  
- \*\*User Registration Interface (FR-05):\*\*   
 Offers a form for administrators to input new user details (Name, Email, DepartmentID, Role). A success message is displayed once a new user is created, including a UserID.  
  
- \*\*Assign User Permissions Interface (FR-06):\*\*   
 Enables administrators to select a user and assign specific permissions. The system updates the User record and logs the permission assignment in the PermissionAssignment table.  
  
- \*\*Modify User Information Interface (FR-07):\*\*   
 Provides fields for administrators to update user details such as Name, Email, DepartmentID, and Role. The system reflects these changes in the User record and logs the modification in a UserModification entry.  
  
- \*\*Remove User Interface (FR-08):\*\*   
 Displays a confirmation prompt for user deletion. Once confirmed, the system removes the user and logs the action in a UserDeletion record.  
  
- \*\*Administrator Login Interface (FR-09):\*\*   
 Presents a login form for administrators, accepting a username and password. Upon successful authentication, the system grants access to the main dashboard or interface.  
  
- \*\*Department Management Interface (FR-10, FR-11, FR-12):\*\*   
 Includes functionality for creating, updating, and deleting departments. The system reflects these changes in the Department record and updates DepartmentMembership as necessary.  
  
- \*\*Asset Category Management Interface (FR-13, FR-14, FR-15, FR-16):\*\*   
 Enables administrators to define, modify, or delete asset categories. The system updates the AssetCategory record and logs the action in a CategoryManagement entry.  
  
- \*\*Permission Assignment Management Interface (FR-17):\*\*   
 Provides a mechanism for administrators to assign, modify, or revoke permissions for a user. The system updates the PermissionAssignment record and logs the change in an AuditLog.  
  
- \*\*Asset Usage Logging Interface (FR-18):\*\*   
 Allows users or administrators to log the usage of an asset by entering UsageDate, UsageDuration, and Purpose. The system creates a new UsageRecord and logs the action in the AuditLog.  
  
- \*\*View Usage Records Interface (FR-19):\*\*   
 Displays a list of all usage records for a given asset, including UsageDate, UsageDuration, Purpose, and the associated UserID.  
  
- \*\*Modify Usage Records Interface (FR-20):\*\*   
 Provides a form for users or administrators to update an existing usage record. The system modifies the UsageRecord and logs the change in the AuditLog.  
  
- \*\*Delete Usage Records Interface (FR-21):\*\*   
 Presents a confirmation prompt for deleting a usage record. After confirmation, the system removes the record and logs the deletion in the AuditLog.  
  
- \*\*Audit Log Interface (FR-22):\*\*   
 Enables users or administrators to view audit logs with filtering options such as timestamp range, affected entity, and action type. The system displays a list of audit log entries including LogID, UserID, AssetID, RecordID, Action, Timestamp, and Details.  
  
- \*\*Audit Report Generation Interface (FR-23):\*\*   
 Provides a form for administrators to specify report generation parameters such as time range and action type. The system generates a structured audit report and logs the report generation in the AuditLog.  
  
- \*\*Email Notification Interface (FR-24):\*\*   
 Allows users or administrators to compose and send email notifications for system events. The system logs the email action in the AuditLog and stores the details in the EmailNotification table.  
  
## 2.2 Hardware Interface Output  
  
This system does not directly interact with external hardware devices. There are no hardware interface outputs defined at this stage. However, if future integration with hardware (e.g., asset tracking devices or scanners) is required, it will be specified in a subsequent revision of this document.  
  
## 2.3 Software Interface Output  
  
The system interacts with external software through its database and potentially via API calls for audit logging and email notifications. The following software interfaces are defined:  
  
- \*\*Database Interface:\*\*   
 The system communicates with a relational database to store and retrieve data. The database contains the following tables:   
 - \*\*Asset:\*\* Stores asset information (Name, Description, CategoryID, Location, PurchaseDate, Status).   
 - \*\*User:\*\* Maintains user data (Name, Email, DepartmentID, Role, UserID).   
 - \*\*Department:\*\* Holds department details (Name, Description, DepartmentID).   
 - \*\*AssetCategory:\*\* Defines asset categories (Name, Description, ParentCategoryID, CategoryID).   
 - \*\*PermissionAssignment:\*\* Tracks permissions assigned to users.   
 - \*\*UsageRecord:\*\* Logs asset usage (UsageDate, UsageDuration, Purpose, UserID, AssetID).   
 - \*\*AuditLog:\*\* Records system actions and changes (LogID, UserID, AssetID, RecordID, Action, Timestamp, Details).   
 - \*\*EmailNotification:\*\* Stores information about sent email notifications (RecipientID, Content, Timestamp, EventType).  
  
 The system performs operations such as inserting, updating, and deleting records in these tables. Developers must ensure that the database schema aligns with the functional requirements.  
  
- \*\*Email Notification Software Interface (FR-24):\*\*   
 The system sends email notifications via an external email service. The interface requires the following inputs:   
 - Recipient identifier (e.g., UserID or Email)   
 - Email content or template   
 - Event details (e.g., action performed, timestamp)   
 The system outputs an email message with the specified content and logs the action in the AuditLog and EmailNotification tables.  
  
- \*\*Audit Log Software Interface (FR-22, FR-23):\*\*   
 The system maintains an AuditLog table to record all actions and changes. The AuditLog entry includes:   
 - LogID   
 - UserID   
 - AssetID (if applicable)   
 - RecordID (if applicable)   
 - Action (e.g., register, modify, delete)   
 - Timestamp   
 - Details (description of the action)   
 This interface is used for internal tracking and reporting.  
  
- \*\*External API Interface (for Audit Report Generation, FR-23):\*\*   
 If the system is to generate reports in a structured format (e.g., PDF, Excel), it may interact with a third-party API or library for report generation. The system provides the data to be included in the report and receives a file output from the API. The interface must support input parameters such as time range and action type.  
  
## 2.4 Communication Interface Output  
  
The system communicates with external entities via network-based protocols for audit logging, email notifications, and potential remote access.  
  
- \*\*Email Communication Interface (FR-24):\*\*   
 The system sends email notifications using a configured SMTP server or email service. The communication interface handles the transmission of email content, recipient information, and event details. The system must ensure secure and reliable email delivery and log the communication in the AuditLog and EmailNotification tables.  
  
- \*\*Web Communication Interface (for Audit Report Generation, FR-23):\*\*   
 If the system is to generate reports in a structured format (e.g., PDF, Excel), it may communicate with a web service or API to perform the report generation. The system sends the required data and formatting instructions to the service and receives the completed report file as a response.  
  
- \*\*Audit Log Communication Interface (FR-22, FR-23):\*\*   
 The system logs all actions in the AuditLog table, which can be accessed via a web-based interface or API. Users or administrators can query the AuditLog using filtering criteria such as timestamp range, affected entity, and action type. This allows for remote auditing and monitoring of system activities.  
  
- \*\*Remote Access Communication Interface (FR-09):\*\*   
 The system supports remote access via web or mobile interfaces, allowing administrators to log in and perform system management functions. The interface must be secure, using encryption and authentication protocols to protect user credentials and data integrity.  
  
---  
  
This chapter provides a comprehensive overview of the external interfaces the system must support. Each interface is clearly defined and described in terms of its role, input/output, and interaction method. Developers should use this information to ensure the system integrates seamlessly with its environment and meets all functional and non-functional requirements.

# Use Case

Use Case Name: Asset Registration   
Use Case ID: UC-01   
Actors: User, Administrator, Department, Asset Category, Permission, Asset, Usage Record, Audit Log, Email Notification, Database Record   
Preconditions:   
1. The user must have valid login credentials and appropriate permissions to register assets.   
2. The asset must not already exist in the system.   
3. The system must be connected to the database and email notification service.   
  
Postconditions:   
1. The asset is successfully registered and stored in the database.   
2. An audit log entry is created to record the registration event.   
3. The user receives a confirmation email notification.   
4. The asset is available for use and tracking in the system.   
  
Main Flow:   
1. The user logs into the system with valid credentials.   
2. The user navigates to the asset registration page.   
3. The user selects the appropriate department and asset category for the new asset.   
4. The user enters the required asset details (e.g., name, description, serial number, location).   
5. The system validates the input data and checks if the asset already exists.   
6. The system creates a new asset record in the database.   
7. The system logs the registration event in the audit log.   
8. The system sends an email notification to the user confirming the asset registration.   
9. The system displays a confirmation message to the user.   
  
Alternative Flow:   
1. If the user does not have sufficient permissions, the system denies access and displays an error message.   
2. If the asset already exists in the database, the system displays a warning message and does not create a new record.   
3. If the input data is invalid, the system displays an error message and prompts the user to correct the information.   
4. If the system fails to connect to the database or email service, the system displays an error message and logs the issue for troubleshooting.  
  
Use Case Name: View Asset Information   
Use Case ID: UC-02   
Actors: User, Administrator, Department, Asset Category, Permission, Asset, Usage Record, Audit Log, Email Notification, Database Record   
Preconditions:   
1. The user must be logged in and have valid permissions to view asset information.   
2. The asset must exist in the system and be associated with a department or category.   
3. The system must have access to the database to retrieve asset records.   
  
Postconditions:   
1. The user is presented with the asset information.   
2. The system logs the viewing action in the audit log.   
3. The asset data is retrieved from the database without modification.   
4. The user may optionally receive an email notification with the asset details.   
  
Main Flow:   
1. The user logs into the system with valid credentials.   
2. The user selects the "View Asset Information" option from the asset management menu.   
3. The user searches for the asset using identifiers such as asset name, serial number, or category.   
4. The system retrieves the asset record from the database.   
5. The system displays the asset details (e.g., name, category, department, location, usage history).   
6. The system logs the viewing action in the audit log.   
7. The user reviews the asset information.   
8. The user may choose to request an email notification with the asset details.   
9. The system sends the email notification if requested.   
  
Alternative Flow:   
1. If the user does not have sufficient permissions, the system denies access and displays an error message.   
2. If the asset is not found in the database, the system displays a message indicating that the asset does not exist.   
3. If the system fails to retrieve asset information, an error message is displayed and the issue is logged for troubleshooting.   
4. If the user requests an email notification and the system cannot send it, an error message is shown, and the issue is logged.  
  
Use Case Name: Modify Asset Details   
Use Case ID: UC-03   
Actors: User, Administrator, Department, Asset Category, Permission, Asset, Usage Record, Audit Log, Email Notification, Database Record   
  
Preconditions:   
1. The user must be logged in and have valid permissions to modify asset details.   
2. The asset must exist in the system and be associated with a department or category.   
3. The system must have access to the database to retrieve and update asset records.   
  
Postconditions:   
1. The asset details are successfully updated in the database.   
2. An audit log entry is created to record the modification event.   
3. The user receives a confirmation email notification.   
4. The updated asset information is available for use and tracking in the system.   
  
Main Flow:   
1. The user logs into the system with valid credentials.   
2. The user navigates to the asset modification page.   
3. The user searches for the asset using identifiers such as asset name, serial number, or category.   
4. The system retrieves the asset record from the database.   
5. The user edits the asset details (e.g., name, description, location, or category).   
6. The system validates the updated input data.   
7. The system updates the asset record in the database.   
8. The system logs the modification event in the audit log.   
9. The system sends an email notification to the user confirming the asset modification.   
10. The system displays a confirmation message to the user.   
  
Alternative Flow:   
1. If the user does not have sufficient permissions, the system denies access and displays an error message.   
2. If the asset is not found in the database, the system displays a message indicating that the asset does not exist.   
3. If the input data is invalid, the system displays an error message and prompts the user to correct the information.   
4. If the system fails to update the asset record, an error message is displayed and the issue is logged for troubleshooting.   
5. If the system fails to connect to the database or email service, the system displays an error message and logs the issue for troubleshooting.  
  
Use Case Name: Remove Asset   
Use Case ID: UC-04   
Actors: User, Administrator, Department, Asset Category, Permission, Asset, Usage Record, Audit Log, Email Notification, Database Record   
  
Preconditions:   
1. The user must be logged in and have valid permissions to remove assets.   
2. The asset must exist in the system and be associated with a department or category.   
3. The system must have access to the database to retrieve and delete asset records.   
  
Postconditions:   
1. The asset is successfully removed from the database.   
2. An audit log entry is created to record the removal event.   
3. The user receives a confirmation email notification.   
4. The asset is no longer available for use or tracking in the system.   
  
Main Flow:   
1. The user logs into the system with valid credentials.   
2. The user navigates to the asset removal page.   
3. The user searches for the asset using identifiers such as asset name, serial number, or category.   
4. The system retrieves the asset record from the database.   
5. The system displays a confirmation prompt to ensure the user wants to remove the asset.   
6. The user confirms the removal of the asset.   
7. The system deletes the asset record from the database.   
8. The system logs the removal event in the audit log.   
9. The system sends an email notification to the user confirming the asset removal.   
10. The system displays a confirmation message to the user.   
  
Alternative Flow:   
1. If the user does not have sufficient permissions, the system denies access and displays an error message.   
2. If the asset is not found in the database, the system displays a message indicating that the asset does not exist.   
3. If the user cancels the removal, the system does not delete the asset and returns to the asset list.   
4. If the system fails to delete the asset record, an error message is displayed, and the issue is logged for troubleshooting.   
5. If the system fails to connect to the database or email service, the system displays an error message and logs the issue for troubleshooting.  
  
Use Case Name: User Registration   
Use Case ID: UC-05   
Actors: User, Administrator, Department, Permission, Database Record, Email Notification, Audit Log   
  
Preconditions:   
1. The system must be accessible to new users.   
2. The Administrator must have the ability to create new user accounts.   
3. The system must have access to the database to store user records.   
4. The system must be connected to the email notification service.   
  
Postconditions:   
1. The new user is successfully registered and stored in the database.   
2. An audit log entry is created to record the registration event.   
3. The user receives a confirmation email notification.   
4. The user can now log in and access the system based on assigned permissions.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the user registration page.   
3. The Administrator enters the new user's details (e.g., name, email, department, role).   
4. The system validates the input data and checks for duplicate email or user records.   
5. The system creates a new user record in the database and assigns appropriate permissions.   
6. The system logs the user registration event in the audit log.   
7. The system sends an email notification to the user confirming the registration and including login instructions.   
8. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the email is already associated with an existing user, the system displays a warning message and does not create a new record.   
3. If the input data is invalid, the system displays an error message and prompts the Administrator to correct the information.   
4. If the system fails to connect to the database or email service, an error message is displayed, and the issue is logged for troubleshooting.  
  
Use Case Name: Assign User Permissions   
Use Case ID: UC-06   
Actors: User, Administrator, Department, Permission, Database Record, Audit Log, Email Notification   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to assign user permissions.   
2. The target user must exist in the system.   
3. The system must have access to the database to update user records and permission assignments.   
4. The system must be connected to the email notification service to send confirmation emails.   
  
Postconditions:   
1. The user's permissions are successfully updated and stored in the database.   
2. An audit log entry is created to record the permission assignment event.   
3. The user receives a confirmation email notification with details of the assigned permissions.   
4. The user can now access system functionalities based on the new permissions.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the user permissions management page.   
3. The Administrator selects the user for whom permissions need to be assigned.   
4. The system retrieves the user's current permissions from the database.   
5. The Administrator chooses the appropriate permissions from the available options.   
6. The system validates the selected permissions and ensures they are applicable to the user's role or department.   
7. The system updates the user's permission record in the database.   
8. The system logs the permission assignment event in the audit log.   
9. The system sends an email notification to the user confirming the assigned permissions.   
10. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the selected user does not exist in the database, the system displays a warning message.   
3. If the selected permissions are invalid or not applicable, the system displays an error message and prompts the Administrator to select valid permissions.   
4. If the system fails to update the user's permission record in the database, an error message is displayed and the issue is logged for troubleshooting.   
5. If the system fails to send the email notification, an error message is shown, and the issue is logged for troubleshooting.  
  
Use Case Name: Modify User Information   
Use Case ID: UC-07   
Actors: User, Administrator, Department, Permission, Database Record, Email Notification, Audit Log   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to modify user information.   
2. The target user must exist in the system.   
3. The system must have access to the database to retrieve and update user records.   
4. The system must be connected to the email notification service.   
  
Postconditions:   
1. The user's information is successfully updated and stored in the database.   
2. An audit log entry is created to record the modification event.   
3. The user receives an email notification confirming the updated information.   
4. The modified user information is reflected in the system and available for future use.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the user modification page.   
3. The Administrator searches for the user using identifiers such as username, email, or department.   
4. The system retrieves the user's current information from the database.   
5. The Administrator edits the user's details (e.g., name, email, department, or role).   
6. The system validates the updated input data and checks for duplicate emails.   
7. The system updates the user's record in the database.   
8. The system logs the modification event in the audit log.   
9. The system sends an email notification to the user confirming the modification.   
10. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the user is not found in the database, the system displays a message indicating that the user does not exist.   
3. If the updated email is already associated with another user, the system displays a warning message and does not proceed with the update.   
4. If the input data is invalid, the system displays an error message and prompts the Administrator to correct the information.   
5. If the system fails to update the user's record in the database, an error message is displayed and the issue is logged for troubleshooting.   
6. If the system fails to send the email notification, an error message is shown, and the issue is logged for troubleshooting.  
  
Use Case Name: Remove User   
Use Case ID: UC-08   
Actors: User, Administrator, Department, Permission, Database Record, Email Notification, Audit Log   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to remove users.   
2. The target user must exist in the system.   
3. The system must have access to the database to retrieve and delete user records.   
4. The system must be connected to the email notification service.   
  
Postconditions:   
1. The target user is successfully removed from the database.   
2. An audit log entry is created to record the removal event.   
3. The user receives a confirmation email notification.   
4. The user can no longer access the system.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the user removal page.   
3. The Administrator searches for the user using identifiers such as username, email, or department.   
4. The system retrieves the user's record from the database.   
5. The system displays a confirmation prompt to ensure the Administrator wants to remove the user.   
6. The Administrator confirms the removal of the user.   
7. The system deletes the user's record from the database.   
8. The system logs the removal event in the audit log.   
9. The system sends an email notification to the user confirming the removal.   
10. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the user is not found in the database, the system displays a message indicating that the user does not exist.   
3. If the Administrator cancels the removal, the system does not delete the user and returns to the user list.   
4. If the system fails to delete the user's record, an error message is displayed, and the issue is logged for troubleshooting.   
5. If the system fails to connect to the database or email service, the system displays an error message and logs the issue for troubleshooting.  
  
Use Case Name: Administrator Login   
Use Case ID: UC-09   
Actors: Administrator, Permission, Database Record, Audit Log   
  
Preconditions:   
1. The Administrator must have a valid account in the system with login credentials.   
2. The system must have access to the database to verify the Administrator’s credentials.   
3. The system must be able to log the login event in the audit log.   
  
Postconditions:   
1. The Administrator is successfully authenticated and logged into the system.   
2. The login event is recorded in the audit log.   
3. The Administrator is granted access to the system based on their assigned permissions.   
4. The system displays the Administrator’s dashboard or main interface.   
  
Main Flow:   
1. The Administrator enters their username and password on the login page.   
2. The system validates the input credentials against the database records.   
3. If the credentials are valid, the system authenticates the Administrator.   
4. The system retrieves the Administrator’s permissions from the database.   
5. The system logs the login event in the audit log.   
6. The system displays the Administrator’s main interface or dashboard.   
  
Alternative Flow:   
1. If the credentials are invalid, the system displays an error message and denies access.   
2. If the system fails to connect to the database, the login is blocked, and an error message is displayed.   
3. If the login attempt is unauthorized due to insufficient permissions, the system denies access and logs the event.   
4. If the system fails to log the login event in the audit log, an error message is displayed, and the issue is logged for troubleshooting.  
  
Use Case Name: Manage Departments   
Use Case ID: UC-10   
Actors: Administrator, Department, Permission, Database Record, Audit Log   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to manage departments.   
2. The system must have access to the database to retrieve and update department records.   
3. The system must be able to log the department management actions in the audit log.   
  
Postconditions:   
1. The department is successfully created, updated, or removed in the database.   
2. An audit log entry is created for each department management action.   
3. The system reflects the current department structure based on the changes made.   
4. Users are assigned to or removed from departments as needed.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the department management page.   
3. The Administrator selects an action: "Create Department," "Update Department," or "Remove Department."   
4. If creating a department, the Administrator enters the department name and description.   
5. If updating a department, the Administrator selects the department and modifies its details.   
6. If removing a department, the Administrator selects the department and confirms the removal.   
7. The system validates the input data and checks for existing department records (if creating).   
8. The system updates the department record in the database.   
9. The system logs the department management action in the audit log.   
10. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the department name is already in use when creating, the system displays a warning and does not proceed.   
3. If the input data is invalid, the system displays an error message and prompts the Administrator to correct it.   
4. If the system fails to update or delete the department record, an error message is displayed and the issue is logged.   
5. If the system fails to log the action in the audit log, an error message is shown, and the issue is logged for troubleshooting.  
  
Use Case Name: Add Department   
Use Case ID: UC-11   
Actors: Administrator, Department, Permission, Database Record, Audit Log   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to add departments.   
2. The system must have access to the database to store department records.   
3. The system must be able to log the department creation event in the audit log.   
  
Postconditions:   
1. The new department is successfully added and stored in the database.   
2. An audit log entry is created to record the department creation event.   
3. The Administrator receives a confirmation message.   
4. The department is available for assignment to users and assets in the system.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the department management page.   
3. The Administrator selects the "Create Department" option.   
4. The Administrator enters the department name and description.   
5. The system validates the input data and checks if the department name already exists.   
6. The system creates a new department record in the database.   
7. The system logs the creation event in the audit log.   
8. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the department name is already in use, the system displays a warning and does not create a new department.   
3. If the input data is invalid, the system displays an error message and prompts the Administrator to correct the information.   
4. If the system fails to connect to the database, an error message is displayed, and the issue is logged for troubleshooting.   
5. If the system fails to log the action in the audit log, an error message is shown, and the issue is logged for troubleshooting.  
  
Use Case Name: Remove Department   
Use Case ID: UC-12   
Actors: Administrator, Department, Permission, Database Record, Audit Log, Email Notification   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to remove departments.   
2. The department to be removed must exist in the system.   
3. The system must have access to the database to retrieve and delete department records.   
4. The system must be able to log the removal action in the audit log.   
5. The system must be connected to the email notification service to inform affected users.   
  
Postconditions:   
1. The department is successfully removed from the database.   
2. An audit log entry is created to record the removal event.   
3. The system updates references to ensure no assets or users are associated with the removed department.   
4. The Administrator receives a confirmation message.   
5. Affected users receive an email notification about the department removal.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the department management page.   
3. The Administrator selects the department to be removed.   
4. The system checks if the department has associated assets or users.   
5. The system displays a confirmation prompt to ensure the Administrator wants to proceed.   
6. The Administrator confirms the removal of the department.   
7. The system updates the associated assets and users to remove or reassign them from the department.   
8. The system deletes the department record from the database.   
9. The system logs the removal event in the audit log.   
10. The system sends an email notification to affected users.   
11. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the department is not found in the database, the system displays a message indicating that the department does not exist.   
3. If the department has associated assets or users and the system cannot reassign them, the system displays an error message and prevents removal.   
4. If the Administrator cancels the removal, the system does not delete the department and returns to the department list.   
5. If the system fails to delete the department record, an error message is displayed and the issue is logged for troubleshooting.   
6. If the system fails to send email notifications to affected users, an error message is shown, and the issue is logged for troubleshooting.  
  
Use Case Name: Create Asset Category   
Use Case ID: UC-13   
Actors: Administrator, Asset, Asset Category, Department, Permission, Database Record, Audit Log, Email Notification   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to create asset categories.   
2. The system must have access to the database to store asset category records.   
3. The system must be able to log the category creation event in the audit log.   
4. The system must be connected to the email notification service to send confirmation emails.   
  
Postconditions:   
1. The new asset category is successfully created and stored in the database.   
2. An audit log entry is created to record the category creation event.   
3. The Administrator receives a confirmation message.   
4. The asset category is available for use in asset registration and management.   
5. The user or Administrator may optionally receive an email notification about the new category.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the asset category management page.   
3. The Administrator selects the "Create Asset Category" option.   
4. The Administrator enters the category name, description, and any additional attributes.   
5. The system validates the input data and checks if the category name already exists.   
6. The system creates a new asset category record in the database.   
7. The system logs the creation event in the audit log.   
8. The system displays a confirmation message to the Administrator.   
9. The system may send an email notification to the Administrator or selected users to inform them of the new category.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the category name is already in use, the system displays a warning and does not create a new category.   
3. If the input data is invalid, the system displays an error message and prompts the Administrator to correct the information.   
4. If the system fails to connect to the database, an error message is displayed, and the issue is logged for troubleshooting.   
5. If the system fails to log the action in the audit log, an error message is shown, and the issue is logged for troubleshooting.   
6. If the system fails to send the email notification, an error message is displayed, and the issue is logged for troubleshooting.  
  
Use Case Name: Modify Asset Category   
Use Case ID: UC-14   
Actors: Administrator, Asset, Asset Category, Department, Permission, Database Record, Audit Log, Email Notification   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to modify asset categories.   
2. The target asset category must exist in the system.   
3. The system must have access to the database to retrieve and update asset category records.   
4. The system must be able to log the modification event in the audit log.   
5. The system must be connected to the email notification service to send updates if necessary.   
  
Postconditions:   
1. The asset category is successfully updated in the database.   
2. An audit log entry is created to record the modification event.   
3. The system reflects the updated asset category information.   
4. The Administrator receives a confirmation message.   
5. Users or Administrators may optionally receive an email notification about the category change.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the asset category management page.   
3. The Administrator selects the asset category to be modified.   
4. The system retrieves the current category details from the database.   
5. The Administrator edits the category information (e.g., name, description, or attributes).   
6. The system validates the updated input data and checks for duplicate category names.   
7. The system updates the asset category record in the database.   
8. The system logs the modification event in the audit log.   
9. The system displays a confirmation message to the Administrator.   
10. The system may send an email notification to the Administrator or selected users to inform them of the category modification.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the asset category is not found in the database, the system displays a message indicating that the category does not exist.   
3. If the updated category name already exists, the system displays a warning and does not proceed with the modification.   
4. If the input data is invalid, the system displays an error message and prompts the Administrator to correct the information.   
5. If the system fails to update the asset category record in the database, an error message is displayed, and the issue is logged for troubleshooting.   
6. If the system fails to log the action in the audit log, an error message is shown, and the issue is logged for troubleshooting.   
7. If the system fails to send the email notification, an error message is displayed, and the issue is logged for troubleshooting.  
  
Use Case Name: Remove Asset Category   
Use Case ID: UC-15   
Actors: Administrator, Asset, Asset Category, Department, Permission, Database Record, Audit Log, Email Notification   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to remove asset categories.   
2. The target asset category must exist in the system.   
3. The system must have access to the database to retrieve and delete asset category records.   
4. The system must be able to log the removal action in the audit log.   
5. The system must be connected to the email notification service to inform affected users.   
  
Postconditions:   
1. The asset category is successfully removed from the database.   
2. An audit log entry is created to record the removal event.   
3. The system updates references to ensure no assets are associated with the removed category.   
4. The Administrator receives a confirmation message.   
5. Affected users receive an email notification about the category removal.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the asset category management page.   
3. The Administrator selects the asset category to be removed.   
4. The system checks if the category has associated assets.   
5. The system displays a confirmation prompt to ensure the Administrator wants to proceed.   
6. The Administrator confirms the removal of the category.   
7. The system updates the associated assets to remove or reassign their category.   
8. The system deletes the asset category record from the database.   
9. The system logs the removal event in the audit log.   
10. The system sends an email notification to affected users.   
11. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the asset category is not found in the database, the system displays a message indicating that the category does not exist.   
3. If the category has associated assets and the system cannot reassign them, the system displays an error message and prevents removal.   
4. If the Administrator cancels the removal, the system does not delete the category and returns to the category list.   
5. If the system fails to delete the category record, an error message is displayed, and the issue is logged for troubleshooting.   
6. If the system fails to send email notifications to affected users, an error message is shown, and the issue is logged for troubleshooting.  
  
Use Case Name: View Asset Category   
Use Case ID: UC-16   
Actors: User, Administrator, Asset Category, Permission, Database Record, Audit Log   
  
Preconditions:   
1. The user or Administrator must be logged in with valid credentials and have the necessary permissions to view asset categories.   
2. The target asset category must exist in the system.   
3. The system must have access to the database to retrieve asset category records.   
4. The system must be able to log the viewing event in the audit log.   
  
Postconditions:   
1. The user or Administrator is presented with the details of the selected asset category.   
2. The system logs the viewing action in the audit log.   
3. The asset category data is retrieved from the database without modification.   
4. The user or Administrator may optionally receive an email notification with the category details.   
  
Main Flow:   
1. The user or Administrator logs into the system with valid credentials.   
2. The user or Administrator navigates to the asset category management or view page.   
3. The user or Administrator selects an asset category from the list or searches for it using a name or identifier.   
4. The system retrieves the selected asset category details from the database.   
5. The system displays the category information (e.g., name, description, associated assets).   
6. The system logs the viewing action in the audit log.   
7. The user or Administrator reviews the asset category details.   
8. The user or Administrator may request an email notification with the category details.   
9. The system sends the email notification if requested.   
  
Alternative Flow:   
1. If the user or Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the selected asset category is not found in the database, the system displays a message indicating that the category does not exist.   
3. If the system fails to retrieve the asset category information, an error message is displayed and the issue is logged for troubleshooting.   
4. If the system fails to send the email notification, an error message is shown, and the issue is logged for troubleshooting.  
  
Use Case Name: Manage Permissions   
Use Case ID: UC-17   
Actors: Administrator, User, Permission, Department, Database Record, Audit Log, Email Notification   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to manage permissions.   
2. The target user or permission must exist in the system.   
3. The system must have access to the database to retrieve and update permission records.   
4. The system must be able to log the permission management action in the audit log.   
5. The system must be connected to the email notification service to inform users of permission changes.   
  
Postconditions:   
1. The user's permissions are successfully assigned, modified, or revoked in the database.   
2. An audit log entry is created to record the permission management event.   
3. The user receives an email notification (if applicable) regarding the permission changes.   
4. The updated permissions take effect in the system immediately.   
5. The Administrator is informed of the success or failure of the operation.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the permission management page.   
3. The Administrator selects a user from the list or searches for them using identifiers such as username or department.   
4. The system retrieves the user's current permissions from the database.   
5. The Administrator modifies the user's permissions by adding, removing, or updating them.   
6. The system validates the new permission configuration and ensures it aligns with system rules.   
7. The system updates the user's permission record in the database.   
8. The system logs the permission management event in the audit log.   
9. The system sends an email notification to the user (if applicable) about the permission changes.   
10. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the selected user does not exist in the database, the system displays a message indicating that the user does not exist.   
3. If the permission configuration is invalid or violates system constraints, the system displays an error message and prompts the Administrator to correct the settings.   
4. If the system fails to update the user's permission record in the database, an error message is displayed and the issue is logged for troubleshooting.   
5. If the system fails to log the action in the audit log, an error message is shown, and the issue is logged for troubleshooting.   
6. If the system fails to send the email notification to the user, an error message is displayed, and the issue is logged for troubleshooting.  
  
Use Case Name: Assign Permissions   
Use Case ID: UC-18   
Actors: Administrator, User, Permission, Department, Database Record, Audit Log, Email Notification   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to assign permissions.   
2. The target user must exist in the system.   
3. The system must have access to the database to retrieve and update user and permission records.   
4. The system must be able to log permission assignment events in the audit log.   
5. The system must be connected to the email notification service to send confirmation emails.   
  
Postconditions:   
1. The user's permissions are successfully updated in the database.   
2. An audit log entry is created to record the permission assignment event.   
3. The user receives an email notification confirming the assigned permissions.   
4. The user can now access system functionalities based on the newly assigned permissions.   
5. The Administrator is informed of the success or failure of the operation.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the permission assignment page.   
3. The Administrator selects the user to whom permissions will be assigned.   
4. The system retrieves the user's current permissions and available permission options.   
5. The Administrator selects the appropriate permissions to assign.   
6. The system validates the selected permissions and ensures they are compatible with the user's role or department.   
7. The system updates the user's permission record in the database.   
8. The system logs the permission assignment in the audit log.   
9. The system sends an email notification to the user confirming the new permissions.   
10. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the selected user does not exist in the database, the system displays a message indicating that the user does not exist.   
3. If the selected permissions are invalid or not applicable, the system displays an error message and prompts the Administrator to choose valid permissions.   
4. If the system fails to update the user's permission record, an error message is displayed, and the issue is logged for troubleshooting.   
5. If the system fails to log the action in the audit log, an error message is shown, and the issue is logged for troubleshooting.   
6. If the system fails to send the email notification to the user, an error message is displayed, and the issue is logged for troubleshooting.  
  
Use Case Name: View Permission Details   
Use Case ID: UC-19   
Actors: Administrator, User, Permission, Department, Database Record, Audit Log   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to view permission details.   
2. The target user or permission must exist in the system.   
3. The system must have access to the database to retrieve permission records.   
4. The system must be able to log the viewing action in the audit log.   
  
Postconditions:   
1. The Administrator is presented with the detailed permission information for the selected user.   
2. The system logs the viewing action in the audit log.   
3. The permission data is retrieved from the database without modification.   
4. The Administrator is informed of the success or failure of the operation.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the permission details page.   
3. The Administrator selects a user from the list or searches for them using identifiers such as username or department.   
4. The system retrieves the user's permission details from the database.   
5. The system displays the permission information (e.g., assigned roles, access levels, restrictions).   
6. The system logs the viewing action in the audit log.   
7. The Administrator reviews the permission details.   
8. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the selected user does not exist in the database, the system displays a message indicating that the user does not exist.   
3. If the system fails to retrieve the permission details, an error message is displayed and the issue is logged for troubleshooting.   
4. If the system fails to log the action in the audit log, an error message is shown, and the issue is logged for troubleshooting.  
  
Use Case Name: Record Asset Usage   
Use Case ID: UC-20   
Actors: User, Administrator, Asset, Asset Category, Department, Permission, Usage Record, Audit Log, Email Notification, Database Record   
  
Preconditions:   
1. The user or Administrator must be logged in with valid credentials and have the necessary permissions to record asset usage.   
2. The asset must exist in the system and be available for use.   
3. The system must have access to the database to create and store usage records.   
4. The system must be able to log the usage recording event in the audit log.   
5. The system must be connected to the email notification service to send updates if necessary.   
  
Postconditions:   
1. A new asset usage record is created and stored in the database.   
2. The usage event is logged in the audit log.   
3. The system reflects the updated usage history for the asset.   
4. The user or Administrator receives a confirmation message.   
5. If configured, the user or relevant stakeholders receive an email notification about the recorded usage.   
  
Main Flow:   
1. The user or Administrator logs into the system with valid credentials.   
2. The user or Administrator navigates to the asset usage recording page.   
3. The user or Administrator selects the asset for which usage is being recorded.   
4. The user or Administrator enters the usage details (e.g., start time, end time, user, activity description).   
5. The system validates the input data and checks the availability of the selected asset.   
6. The system creates a new usage record in the database.   
7. The system logs the usage recording event in the audit log.   
8. The system sends an email notification to the user or stakeholders (if applicable).   
9. The system displays a confirmation message to the user or Administrator.   
  
Alternative Flow:   
1. If the user or Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the selected asset is not found in the database, the system displays a message indicating that the asset does not exist.   
3. If the input data is invalid or incomplete, the system displays an error message and prompts the user or Administrator to correct the information.   
4. If the system fails to create the usage record in the database, an error message is displayed and the issue is logged for troubleshooting.   
5. If the system fails to log the action in the audit log, an error message is shown, and the issue is logged for troubleshooting.   
6. If the system fails to send the email notification, an error message is displayed, and the issue is logged for troubleshooting.  
  
Use Case Name: View Usage Records   
Use Case ID: UC-21   
Actors: User, Administrator, Asset, Usage Record, Audit Log, Email Notification, Database Record   
  
Preconditions:   
1. The user or Administrator must be logged in with valid credentials and have the necessary permissions to view usage records.   
2. The target asset must exist in the system and have associated usage records.   
3. The system must have access to the database to retrieve usage records.   
4. The system must be able to log the viewing action in the audit log.   
  
Postconditions:   
1. The user or Administrator is presented with the usage records for the selected asset.   
2. The system logs the viewing action in the audit log.   
3. The usage data is retrieved from the database without modification.   
4. The user or Administrator may optionally receive an email notification with the usage details.   
  
Main Flow:   
1. The user or Administrator logs into the system with valid credentials.   
2. The user or Administrator navigates to the usage record management or view page.   
3. The user or Administrator selects an asset from the list or searches for it using identifiers such as asset name, serial number, or category.   
4. The system retrieves the usage records associated with the selected asset from the database.   
5. The system displays the usage records (e.g., start and end times, activity description, user who used the asset).   
6. The system logs the viewing action in the audit log.   
7. The user or Administrator reviews the usage records.   
8. The user or Administrator may choose to request an email notification with the usage details.   
9. The system sends the email notification if requested.   
  
Alternative Flow:   
1. If the user or Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the selected asset is not found in the database, the system displays a message indicating that the asset does not exist.   
3. If the asset has no usage records, the system displays a message indicating that no usage history is available.   
4. If the system fails to retrieve the usage records, an error message is displayed and the issue is logged for troubleshooting.   
5. If the system fails to send the email notification, an error message is shown, and the issue is logged for troubleshooting.  
  
Use Case Name: Modify Usage Records   
Use Case ID: UC-22   
Actors: User, Administrator, Asset, Usage Record, Audit Log, Email Notification, Database Record   
  
Preconditions:   
1. The user or Administrator must be logged in with valid credentials and have the necessary permissions to modify usage records.   
2. The target asset must exist in the system and have associated usage records.   
3. The system must have access to the database to retrieve and update usage records.   
4. The system must be able to log the modification action in the audit log.   
5. The system must be connected to the email notification service to send confirmation emails if needed.   
  
Postconditions:   
1. The usage record is successfully modified and updated in the database.   
2. An audit log entry is created to record the modification event.   
3. The user or Administrator receives a confirmation message.   
4. If configured, an email notification is sent to inform relevant stakeholders of the changes.   
5. The modified usage record is reflected in the system for tracking and reporting.   
  
Main Flow:   
1. The user or Administrator logs into the system with valid credentials.   
2. The user or Administrator navigates to the usage record modification page.   
3. The user or Administrator searches for the asset or selects it from the list.   
4. The system retrieves the usage records associated with the selected asset.   
5. The user or Administrator selects the specific usage record to be modified.   
6. The user or Administrator updates the usage details (e.g., start time, end time, activity description).   
7. The system validates the updated data and checks for consistency with the asset's status and availability.   
8. The system updates the selected usage record in the database.   
9. The system logs the modification event in the audit log.   
10. The system displays a confirmation message to the user or Administrator.   
11. If configured, the system sends an email notification to relevant stakeholders.   
  
Alternative Flow:   
1. If the user or Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the selected asset is not found in the database, the system displays a message indicating that the asset does not exist.   
3. If the selected usage record is not found or is invalid, the system displays an error message.   
4. If the input data is invalid or inconsistent, the system displays an error message and prompts the user or Administrator to correct the information.   
5. If the system fails to update the usage record in the database, an error message is displayed, and the issue is logged for troubleshooting.   
6. If the system fails to log the action in the audit log, an error message is shown, and the issue is logged for troubleshooting.   
7. If the system fails to send the email notification, an error message is displayed, and the issue is logged for troubleshooting.  
  
Use Case Name: Delete Usage Records   
Use Case ID: UC-23   
Actors: Administrator, User, Asset, Usage Record, Audit Log, Email Notification, Database Record   
  
Preconditions:   
1. The Administrator or User must be logged in with valid credentials and have the authority to delete usage records.   
2. The target usage record must exist in the system and be associated with a valid asset.   
3. The system must have access to the database to retrieve and delete usage records.   
4. The system must be able to log the deletion action in the audit log.   
5. The system must be connected to the email notification service to send confirmation or alerts.   
  
Postconditions:   
1. The selected usage record is successfully deleted from the database.   
2. An audit log entry is created to record the deletion event.   
3. The system updates the asset’s usage history to reflect the change.   
4. The Administrator or User receives a confirmation message.   
5. If configured, an email notification is sent to inform relevant stakeholders of the deletion.   
  
Main Flow:   
1. The Administrator or User logs into the system with valid credentials.   
2. The Administrator or User navigates to the usage record deletion page.   
3. The Administrator or User selects an asset and views its associated usage records.   
4. The Administrator or User selects the specific usage record to be deleted.   
5. The system displays a confirmation prompt to ensure the deletion is intentional.   
6. The Administrator or User confirms the deletion.   
7. The system deletes the selected usage record from the database.   
8. The system logs the deletion event in the audit log.   
9. The system displays a confirmation message to the Administrator or User.   
10. If configured, the system sends an email notification to relevant stakeholders.   
  
Alternative Flow:   
1. If the Administrator or User does not have sufficient permissions, the system denies access and displays an error message.   
2. If the selected usage record is not found in the database, the system displays a message indicating the record does not exist.   
3. If the system cannot delete the usage record due to database constraints, an error message is displayed, and the issue is logged for troubleshooting.   
4. If the deletion is canceled by the Administrator or User, the system returns to the usage record list without making changes.   
5. If the system fails to log the deletion in the audit log, an error message is shown, and the issue is logged for troubleshooting.   
6. If the system fails to send the email notification, an error message is displayed, and the issue is logged for troubleshooting.  
  
Use Case Name: View Audit Log   
Use Case ID: UC-24   
Actors: Administrator, User, Audit Log, Database Record, Permission   
  
Preconditions:   
1. The user or Administrator must be logged in with valid credentials and have the necessary permissions to view audit logs.   
2. The system must have access to the database to retrieve audit log records.   
3. Audit log records must exist in the system.   
  
Postconditions:   
1. The user or Administrator is presented with the requested audit log entries.   
2. The system logs the viewing action in the audit log.   
3. The audit log data is retrieved from the database without modification.   
4. The user or Administrator may optionally receive an email notification with the audit log details.   
  
Main Flow:   
1. The user or Administrator logs into the system with valid credentials.   
2. The user or Administrator navigates to the audit log viewing page.   
3. The user or Administrator selects a specific time range, user, or action to filter the audit logs.   
4. The system retrieves the relevant audit log entries from the database.   
5. The system displays the audit log details (e.g., timestamp, action performed, user involved, affected entity).   
6. The system logs the viewing action in the audit log.   
7. The user or Administrator reviews the audit log information.   
8. The user or Administrator may request an email notification with the audit log details.   
9. The system sends the email notification if requested.   
  
Alternative Flow:   
1. If the user or Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If no audit log entries match the search criteria, the system displays a message indicating no results.   
3. If the system fails to retrieve audit log records from the database, an error message is displayed and the issue is logged for troubleshooting.   
4. If the system fails to log the viewing action in the audit log, an error message is shown, and the issue is logged for troubleshooting.   
5. If the user or Administrator requests an email notification and the system cannot send it, an error message is displayed, and the issue is logged for troubleshooting.  
  
Use Case Name: Generate Audit Report   
Use Case ID: UC-25   
Actors: Administrator, Audit Log, Email Notification, Database Record, Permission   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to generate audit reports.   
2. The system must have access to the audit log and database records to retrieve relevant information.   
3. The system must be connected to the email notification service if sending the report via email.   
  
Postconditions:   
1. The audit report is successfully generated and saved in the system.   
2. An audit log entry is created to record the report generation event.   
3. The Administrator receives the audit report either on the system interface or via email.   
4. The system updates the report history for future reference.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the audit report generation page.   
3. The Administrator selects the time range or filters for the audit log entries to include in the report.   
4. The system retrieves the relevant audit log entries from the database.   
5. The system compiles the selected entries into a structured audit report.   
6. The system logs the report generation event in the audit log.   
7. The Administrator chooses to either download the report or send it via email.   
8. If sending via email, the system sends the audit report to the Administrator's email address.   
9. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If no audit log entries match the selected criteria, the system displays a message indicating no data is available for the report.   
3. If the system fails to retrieve the audit log data, an error message is displayed, and the issue is logged for troubleshooting.   
4. If the system fails to generate the report due to data processing errors, an error message is shown, and the issue is logged.   
5. If the system fails to send the email notification, an error message is displayed, and the issue is logged for troubleshooting.  
  
Use Case Name: Send Email Notification   
Use Case ID: UC-26   
Actors: User, Administrator, Email Notification, Database Record, Audit Log   
  
Preconditions:   
1. The system must be connected to an email notification service.   
2. The user or Administrator must be logged in with valid credentials and have the authority to send email notifications.   
3. The target recipient must exist in the system with a valid email address.   
4. The system must have access to the database to retrieve relevant data for the notification.   
5. The system must be able to log the email notification action in the audit log.   
  
Postconditions:   
1. The email notification is successfully sent to the designated recipient.   
2. An audit log entry is created to record the email notification event.   
3. The email content includes the relevant information (e.g., asset status, user permissions, system updates).   
4. The system displays a confirmation message to the user or Administrator.   
5. The email notification is logged for tracking and reference.   
  
Main Flow:   
1. The user or Administrator logs into the system with valid credentials.   
2. The user or Administrator navigates to the notification or email sending interface.   
3. The user or Administrator selects the recipient or enters the email address.   
4. The system retrieves the recipient's information from the database.   
5. The user or Administrator composes the email message or selects a pre-defined template.   
6. The system validates the email content and recipient information.   
7. The system sends the email notification through the email service.   
8. The system logs the email notification event in the audit log.   
9. The system displays a confirmation message to the user or Administrator.   
  
Alternative Flow:   
1. If the user or Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the recipient is not found in the database, the system displays a message indicating that the recipient does not exist.   
3. If the email address is invalid or missing, the system displays an error message and prompts the user or Administrator to correct the input.   
4. If the system fails to send the email notification, an error message is displayed, and the issue is logged for troubleshooting.   
5. If the system fails to log the action in the audit log, an error message is shown, and the issue is logged for troubleshooting.  
  
Use Case Name: Manage Permission Assignment   
Use Case ID: UC-27   
Actors: Administrator, User, Permission, Permission Assignment, Department, Database Record, Audit Log, Email Notification   
  
Preconditions:   
1. The Administrator must be logged in with valid credentials and have the authority to manage permission assignments.   
2. The target user must exist in the system.   
3. The system must have access to the database to retrieve and update permission assignment records.   
4. The system must be able to log the permission assignment management action in the audit log.   
5. The system must be connected to the email notification service to send confirmation or alerts.   
  
Postconditions:   
1. Permission assignments for the user are successfully created, modified, or removed in the database.   
2. An audit log entry is created for each permission assignment management action.   
3. The user receives an email notification (if applicable) regarding the permission changes.   
4. The updated permission assignments take effect in the system immediately.   
5. The Administrator is informed of the success or failure of the operation.   
  
Main Flow:   
1. The Administrator logs into the system with valid credentials.   
2. The Administrator navigates to the permission assignment management page.   
3. The Administrator selects a user from the list or searches for them using identifiers such as username or department.   
4. The system retrieves the current permission assignments for the selected user from the database.   
5. The Administrator chooses an action: "Assign Permission," "Modify Permission," or "Revoke Permission."   
6. If assigning a new permission, the Administrator selects the permission to assign.   
7. If modifying a permission, the Administrator updates the permission details or selects a new permission.   
8. If revoking a permission, the Administrator selects the permission to remove and confirms the revocation.   
9. The system validates the requested permission assignment and checks for conflicts or constraints.   
10. The system updates the Permission Assignment record in the database.   
11. The system logs the permission assignment management action in the audit log.   
12. The system sends an email notification to the user (if applicable) about the permission changes.   
13. The system displays a confirmation message to the Administrator.   
  
Alternative Flow:   
1. If the Administrator does not have sufficient permissions, the system denies access and displays an error message.   
2. If the selected user does not exist in the database, the system displays a message indicating that the user does not exist.   
3. If the requested permission is invalid or incompatible with the user's role or department, the system displays an error message and prompts the Administrator to select valid permissions.   
4. If the system fails to update the permission assignment record in the database, an error message is displayed, and the issue is logged for troubleshooting.   
5. If the system fails to log the action in the audit log, an error message is shown, and the issue is logged for troubleshooting.   
6. If the system fails to send the email notification to the user, an error message is displayed, and the issue is logged for troubleshooting.