项目文档

# Functional Requirement

1. Functional Requirements   
  
1.1 Email Creation Function   
Function ID: FR-01   
Description: An administrator can create a new email with subject, content, recipients (individual contacts or distribution groups), and choose an associated email account for sending.   
Input: Subject, body content, recipient list (contact IDs or distribution group IDs), selected email account ID, send/schedule option.   
Output: A new email record stored in the system (sent or saved as a draft).   
  
1.2 Email Sending Function   
Function ID: FR-02   
Description: An administrator can send an email to the selected recipients through the configured email server.   
Input: Email ID, selected email account ID, recipient list (contact IDs or distribution group IDs).   
Output: Sent email marked as "Sent" in the system and a recovery record created if retention policies are enabled.   
  
1.3 Email Receiving Function   
Function ID: FR-03   
Description: The system can receive incoming emails from the configured email server and store them in the appropriate inbox.   
Input: Email server configuration, incoming email content and metadata.   
Output: A new email record stored in the inbox of the associated email account.   
  
1.4 Email Viewing Function   
Function ID: FR-04   
Description: An administrator can view the content of a selected email, including subject, sender, recipient, body, and attachments.   
Input: Email ID.   
Output: Full email content and metadata displayed to the administrator.   
  
1.5 Email Archiving Function   
Function ID: FR-05   
Description: An administrator can move an email to the archive folder and apply a retention policy if configured.   
Input: Email ID, archive folder configuration, retention policy ID (optional).   
Output: Email marked as "Archived" and moved to the archive folder, with a recovery record created if applicable.   
  
1.6 Email Archive Search Function   
Function ID: FR-06   
Description: An administrator can search for archived emails using keywords, date range, sender, recipient, or associated email account.   
Input: Search criteria (keywords, date range, sender, recipient, account).   
Output: List of matching archived emails displayed to the administrator.   
  
1.7 Email Archive Management Function   
Function ID: FR-07   
Description: An administrator can perform actions such as restoring or deleting an archived email.   
Input: Email archive ID, action type (restore or delete).   
Output: Updated email status (e.g., restored to inbox or deleted), and a recovery record created if applicable.   
  
1.8 Calendar Creation Function   
Function ID: FR-08   
Description: An administrator can create a new calendar event with title, date, time, location, and optional email notifications to attendees.   
Input: Title, start and end times, location, attendee list (contact IDs or distribution group IDs), notification settings.   
Output: A new calendar event record stored in the system.   
  
1.9 Calendar View Function   
Function ID: FR-09   
Description: An administrator can view the details of a calendar event, including title, date, time, attendees, and description.   
Input: Calendar event ID.   
Output: Display of full event details to the administrator.   
  
1.10 Calendar Update Function   
Function ID: FR-10   
Description: An administrator can modify the details of an existing calendar event and optionally send updated notifications to attendees.   
Input: Calendar event ID, updated event details (title, date, time, location, attendees).   
Output: Updated calendar event record, with notifications sent if enabled, and a recovery record created if applicable.   
  
1.11 Calendar Event Deletion Function   
Function ID: FR-11   
Description: An administrator can delete a calendar event, with the option to send cancellation notifications to attendees.   
Input: Calendar event ID, confirmation for deletion, notification settings.   
Output: Deleted calendar event, with cancellation notifications sent if enabled, and a recovery record created if applicable.   
  
1.12 Contact Creation Function   
Function ID: FR-12   
Description: An administrator can create a new contact with name, email, phone number, and other relevant details.   
Input: Name, email address, phone number, address, and optional notes.   
Output: A new contact record stored in the system.   
  
1.13 Contact Viewing Function   
Function ID: FR-13   
Description: An administrator can view the details of a selected contact, including name, email, phone number, and any additional notes.   
Input: Contact ID.   
Output: Display of full contact details to the administrator.   
  
1.14 Contact Update Function   
Function ID: FR-14   
Description: An administrator can update the details of an existing contact, such as name, email, phone number, or address.   
Input: Contact ID, updated contact details.   
Output: Updated contact record stored in the system, with a recovery record created if applicable.   
  
1.15 Contact Deletion Function   
Function ID: FR-15   
Description: An administrator can delete a contact, updating any related records (e.g., distribution groups or calendar events) if needed.   
Input: Contact ID, confirmation for deletion.   
Output: Deleted contact record, with related references updated and a recovery record created if applicable.   
  
1.16 Distribution Group Creation Function   
Function ID: FR-16   
Description: An administrator can create a new distribution group with a name, description, and a list of contacts to include.   
Input: Group name, description, and selected contact IDs.   
Output: A new distribution group record stored in the system.   
  
1.17 Distribution Group Modification Function   
Function ID: FR-17   
Description: An administrator can add or remove contacts from a distribution group.   
Input: Distribution group ID, list of contacts to add or remove.   
Output: Updated distribution group record, with a recovery record created if applicable.   
  
1.18 Distribution Group Deletion Function   
Function ID: FR-18   
Description: An administrator can delete a distribution group, ensuring all associated email references are updated or removed.   
Input: Distribution group ID, confirmation for deletion.   
Output: Deleted distribution group record, with a recovery record created if applicable.   
  
1.19 Email Account Creation Function   
Function ID: FR-19   
Description: An administrator can create a new email account with username, password, and server configuration.   
Input: Username, password, server settings (e.g., IMAP/SMTP), account type.   
Output: A new email account record stored in the system.   
  
1.20 Email Account Deletion Function   
Function ID: FR-20   
Description: An administrator can delete an email account and process any associated emails or recovery records.   
Input: Email account ID, confirmation for deletion.   
Output: Deleted email account record, with associated data processed and a recovery record created if applicable.   
  
1.21 Email Account Management Function   
Function ID: FR-21   
Description: An administrator can update the configuration of an existing email account, including password, server settings, or account type.   
Input: Email account ID, updated configuration details.   
Output: Updated email account record and a recovery record created if applicable.   
  
1.22 User Account Creation Function   
Function ID: FR-22   
Description: An administrator can create a new user account with name, email, password, and role.   
Input: Name, email, password, role.   
Output: A new user account record stored in the system.   
  
1.23 User Account Management Function   
Function ID: FR-23   
Description: An administrator can update or delete a user account, updating related data (e.g., email accounts, calendars, contacts) as needed.   
Input: User ID, action type (update or delete), updated details (if updating).   
Output: Updated or deleted user account record, with a recovery record created if applicable.   
  
1.24 User Account Viewing Function   
Function ID: FR-24   
Description: An administrator can view the details of a user account, including name, role, associated email accounts, and access logs.   
Input: User ID.   
Output: Display of full user account details to the administrator.   
  
1.25 Retention Policy Creation Function   
Function ID: FR-25   
Description: An administrator can define a new retention policy with a name, description, duration, and trigger condition.   
Input: Policy name, description, duration, trigger condition.   
Output: A new retention policy record stored in the system.   
  
1.26 Retention Policy Application Function   
Function ID: FR-26   
Description: An administrator can apply a retention policy to an email or folder, ensuring the policy is enforced on the selected data.   
Input: Email or folder ID, retention policy ID.   
Output: Updated retention policy status for the selected data, and a recovery record created if applicable.   
  
1.27 Retention Policy Management Function   
Function ID: FR-27   
Description: An administrator can update or delete a retention policy, and the system will apply changes to affected data.   
Input: Retention policy ID, action type (update or delete), updated policy details (if updating).   
Output: Updated or deleted retention policy record, with a recovery record created if applicable.   
  
1.28 Expired Email Management Function   
Function ID: FR-28   
Description: An administrator can manage expired emails, including restoring or permanently deleting them.   
Input: Expired email ID, action type (restore or delete).   
Output: Updated email status (restored or deleted), and a recovery record created if applicable.   
  
1.29 Recovery Record Creation Function   
Function ID: FR-29   
Description: When an email, contact, event, or policy is modified or deleted, a recovery record is automatically created for audit and restoration purposes.   
Input: Modified or deleted data ID, action type, initiator ID.   
Output: A new recovery record stored in the system.   
  
1.30 Recovery Record Viewing Function   
Function ID: FR-30   
Description: An administrator can view recovery records to audit past actions and determine the feasibility of restoration.   
Input: Recovery record ID.   
Output: Display of full recovery record details to the administrator.

# 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 users, external systems, hardware, and communication channels to fulfill its functional requirements.  
  
2.1 User Interface Output   
The system provides a graphical user interface (GUI) for administrators to interact with and manage email, calendar, contact, distribution group, email account, user account, and retention policy data. The interface includes screens and forms for creating, viewing, updating, and deleting these entities, as well as for performing search and management operations.   
  
- \*\*Email Management Interface\*\*:   
 - Functionality: Allows administrators to create, send, view, archive, and delete emails.   
 - Input/Output: Subject, body content, recipient list, email account selection, send/schedule option; displays email content, metadata, and status (e.g., "Sent", "Archived").   
  
- \*\*Calendar Management Interface\*\*:   
 - Functionality: Enables administrators to create, view, update, and delete calendar events.   
 - Input/Output: Title, start/end times, location, attendee list, notification settings; displays event details and updates with optional notifications.   
  
- \*\*Contact Management Interface\*\*:   
 - Functionality: Provides tools for administrators to create, view, update, and delete contacts.   
 - Input/Output: Name, email, phone number, address, notes; displays full contact details and updates.   
  
- \*\*Distribution Group Management Interface\*\*:   
 - Functionality: Allows administrators to create, modify, and delete distribution groups.   
 - Input/Output: Group name, description, contact list; displays updated group information and recovery records if applicable.   
  
- \*\*Email Account Management Interface\*\*:   
 - Functionality: Enables administrators to create, update, and delete email account records.   
 - Input/Output: Username, password, server settings, account type; displays account details and updates.   
  
- \*\*User Account Management Interface\*\*:   
 - Functionality: Provides tools for administrators to create, view, update, and delete user accounts.   
 - Input/Output: Name, email, password, role, access logs; displays user details and updates.   
  
- \*\*Retention Policy Management Interface\*\*:   
 - Functionality: Enables administrators to create, apply, and manage retention policies.   
 - Input/Output: Policy name, description, duration, trigger condition; displays policy details and changes.   
  
- \*\*Email Archive Search Interface\*\*:   
 - Functionality: Allows administrators to search for archived emails using criteria such as keywords, date ranges, senders, recipients, and email accounts.   
 - Input/Output: Search criteria; displays a list of matching archived emails.   
  
- \*\*Recovery Record Viewing Interface\*\*:   
 - Functionality: Provides administrators with the ability to view recovery records to audit past actions and assess restoration feasibility.   
 - Input/Output: Recovery record ID; displays full details of the record (e.g., action type, initiator, affected data ID).   
  
2.2 Hardware Interface Output   
The system does not directly interface with specific hardware devices. All hardware interactions are mediated through software interfaces and communication protocols. However, it relies on standard hardware components such as servers, storage devices, and network infrastructure to operate efficiently and securely.   
  
- \*\*Server Infrastructure\*\*:   
 - Role: Hosts the system and provides computational resources for processing requests and managing data.   
 - Interaction Method: Standard server-client architecture with system software running on physical or virtual servers.   
  
- \*\*Storage Devices\*\*:   
 - Role: Stores the system’s data, including emails, calendar events, contacts, distribution groups, email accounts, user accounts, and recovery records.   
 - Interaction Method: File system or block storage access for data persistence.   
  
2.3 Software Interface Output   
The system interacts with external software components and databases to manage data and provide functionality. These include email servers, databases, and third-party tools for notification and authentication.   
  
- \*\*Email Server (IMAP/SMTP)\*\*:   
 - Role: Provides the backend for sending and receiving emails.   
 - Interaction Method: IMAP and SMTP protocols for retrieving and sending emails.   
 - Input/Output: Server configuration details (e.g., host, port, authentication credentials); incoming email content and metadata; outgoing email content and status.   
  
- \*\*Database System\*\*:   
 - Role: Stores and manages all system data, including email records, calendar events, contacts, distribution groups, user accounts, retention policies, and recovery records.   
 - Interaction Method: SQL or NoSQL database queries for data storage and retrieval.   
 - Input/Output: Data records for emails, contacts, calendar events, etc., and query results for search and management operations.   
  
- \*\*Authentication and Authorization System (e.g., LDAP, OAuth)\*\*:   
 - Role: Manages user authentication and role-based access control.   
 - Interaction Method: LDAP or OAuth API calls for user login and permissions verification.   
 - Input/Output: User credentials and role assignments; authentication status and authorization tokens.   
  
- \*\*Notification Service (e.g., Email Notification Engine)\*\*:   
 - Role: Sends notifications to users for calendar events and other system-generated alerts.   
 - Interaction Method: RESTful API or message queue integration.   
 - Input/Output: Notification settings and recipient list; confirmation of notification delivery.   
  
2.4 Communication Interface Output   
The system communicates with external systems and users via network-based protocols and services, including email communication, web-based interactions, and API calls.   
  
- \*\*Email Communication Interface\*\*:   
 - Role: Enables the system to send and receive emails via configured email servers.   
 - Interaction Method: SMTP for sending emails, IMAP for receiving emails.   
 - Input/Output: Email content, recipient list, server credentials; incoming email content and metadata.   
  
- \*\*Web-Based Communication Interface\*\*:   
 - Role: Provides access to the system through a web browser or application for administrative tasks.   
 - Interaction Method: HTTP/HTTPS for secure data exchange between the system and the web client.   
 - Input/Output: User input via web forms; system responses in HTML, JSON, or XML for rendering.   
  
- \*\*API Interface for Integration\*\*:   
 - Role: Supports integration with external systems for data exchange and automation.   
 - Interaction Method: RESTful API for programmatic access to system functionalities.   
 - Input/Output: JSON/XML payloads for function inputs; structured responses for function outputs (e.g., success/failure status, record IDs).   
  
- \*\*Message Push Interface (e.g., for notifications)\*\*:   
 - Role: Sends real-time notifications to users for events and updates.   
 - Interaction Method: Webhooks or message queues for asynchronous delivery.   
 - Input/Output: Notification events (e.g., calendar updates, email deletions); delivery confirmation and user response.   
  
By clearly defining these external interfaces, the system ensures that all interactions with users, hardware, software, and communication channels are consistent, reliable, and aligned with the functional requirements outlined in this specification. Developers can use these descriptions to design and implement the system with minimal ambiguity and reduced communication overhead.

# Use Case

Use Case Name: Create Email   
Use Case ID: UC-01   
Actors: Administrator, Email Account, Email, Calendar, Contact, Distribution Group, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one valid email account configured.   
3. The system supports email creation and distribution.   
  
Postconditions:   
1. A new email is created and saved in the system.   
2. The email is associated with the correct email account.   
3. The email is sent to the intended recipients or saved as a draft.   
  
Main Flow:   
1. The administrator selects the "Create Email" option from the system interface.   
2. The system displays the email creation form with fields for subject, content, recipients, and attachments.   
3. The administrator fills in the subject and content of the email.   
4. The administrator selects the recipients, which may include individual contacts, distribution groups, or calendar participants.   
5. The administrator chooses the associated email account from which the email will be sent.   
6. The administrator decides whether to send the email immediately or save it as a draft.   
7. The system validates the input and confirms the email is ready to be sent or saved.   
8. If sending immediately, the system sends the email to the selected recipients.   
9. If saving as a draft, the system stores the email in the draft folder for later retrieval.   
  
Alternative Flow:   
1. If the administrator does not select a valid email account, the system displays an error message and prompts the administrator to choose a valid one.   
2. If the email content is empty or invalid, the system displays a warning and does not proceed with sending or saving.   
3. If the selected recipients are invalid or not available, the system alerts the administrator and allows the option to correct the selection.   
4. If the administrator cancels the operation during the email creation process, the system discards any unsaved changes and returns to the previous screen.  
  
Use Case Name: Send Email   
Use Case ID: UC-02   
Actors: Administrator, Email Account, Email, Calendar, Contact, Distribution Group, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The administrator has created an email (either as a draft or ready to send).   
3. The email is associated with a valid email account.   
4. The system has a valid internet connection and email server access.   
  
Postconditions:   
1. The email is successfully sent to the selected recipients.   
2. The email is marked as sent in the system and removed from the draft folder if applicable.   
3. A recovery record is created if the email is sent with retention policies enabled.   
  
Main Flow:   
1. The administrator selects an email from the draft folder or composes a new one.   
2. The administrator confirms that the email details (subject, content, recipients, and email account) are correct.   
3. The administrator clicks the "Send" button to initiate the sending process.   
4. The system verifies the email account and recipient details for validity.   
5. The system schedules or initiates the sending of the email through the configured email server.   
6. The system confirms the successful delivery of the email to the recipients.   
7. The system updates the email status to "Sent" and logs the action.   
  
Alternative Flow:   
1. If the email account is not active or configured properly, the system displays an error and prompts the administrator to select a valid one.   
2. If the email fails to send due to server issues, the system logs the failure and provides a recovery option.   
3. If the recipients are unreachable or invalid, the system alerts the administrator and provides the option to modify recipient details.   
4. If the administrator cancels the send operation, the system returns to the email editing screen without sending the email.  
  
Use Case Name: Receive Email   
Use Case ID: UC-03   
Actors: Administrator, Email Account, Email, Calendar, Contact, Distribution Group, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one valid email account configured.   
3. The email server is active and accessible.   
4. The system is set to monitor incoming emails.   
  
Postconditions:   
1. The incoming email is successfully retrieved and displayed in the system's inbox.   
2. The email is associated with the correct email account.   
3. A recovery record is created if the email is subject to retention policies.   
4. The administrator is notified of the new email.   
  
Main Flow:   
1. The system detects a new email arriving at the configured email account.   
2. The system retrieves the email from the server and processes it.   
3. The system validates the email's structure and content.   
4. The email is stored in the appropriate folder (e.g., inbox) of the email account.   
5. The system generates a notification for the administrator about the received email.   
6. The administrator can view, reply, forward, or archive the email.   
  
Alternative Flow:   
1. If the email fails validation (e.g., corrupted content), the system logs the error and may move the email to a quarantine or error folder.   
2. If the system cannot connect to the email server, it logs the failure and provides a recovery option.   
3. If the email account is not configured properly, the system alerts the administrator and suggests corrective actions.   
4. If the administrator chooses to archive the email, the system moves it to the archive folder and updates the retention policy status.   
5. If the administrator cancels the notification or ignores the email, the system stores it in the inbox without further action.  
  
Use Case Name: View Email   
Use Case ID: UC-04   
Actors: Administrator, Email, Email Account, Contact, Calendar, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. There is at least one email in the system's inbox or archive.   
3. The email is associated with a valid email account.   
  
Postconditions:   
1. The administrator is able to view the full content of the selected email.   
2. The email remains in its original folder (e.g., inbox, archive).   
3. If the email is subject to retention policies, the system updates the view access log accordingly.   
  
Main Flow:   
1. The administrator navigates to the inbox or archive section of the system.   
2. The system displays a list of available emails with summary details.   
3. The administrator selects a specific email to view.   
4. The system retrieves the email and displays its full content, including subject, sender, recipients, and attachments.   
5. The administrator reviews the email and may choose to reply, forward, or archive it.   
6. The system updates the view count or logs the access if retention policies are enabled.   
  
Alternative Flow:   
1. If the selected email is corrupted or cannot be retrieved, the system displays an error message and suggests recovery options.   
2. If the email account is not active or configured correctly, the system alerts the administrator and prompts for correction.   
3. If the administrator cancels the view operation, the system returns to the email list without making any changes.   
4. If the email is marked as expired, the system displays a warning and may move it to a recovery record for potential restoration.  
  
Use Case Name: Archive Email   
Use Case ID: UC-05   
Actors: Administrator, Email, Email Account, Archive, Retention Policy, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. There is at least one email in the inbox or archive folder.   
3. The system has a configured archive folder and retention policy.   
4. The email to be archived is accessible and not expired.   
  
Postconditions:   
1. The selected email is moved to the archive folder.   
2. The archive status of the email is updated in the system.   
3. If applicable, the retention policy is applied to the archived email.   
4. A recovery record is created for the archived email.   
  
Main Flow:   
1. The administrator navigates to the inbox or archive section of the system.   
2. The system displays a list of available emails.   
3. The administrator selects an email to archive.   
4. The administrator clicks the "Archive" button.   
5. The system verifies the archive folder and retention policy configuration.   
6. The system moves the selected email to the archive folder.   
7. The system updates the email status to "Archived" and logs the action.   
8. A recovery record is created for the archived email if retention policies are enabled.   
9. The system confirms the successful archiving of the email.   
  
Alternative Flow:   
1. If the archive folder is not configured, the system displays an error and prompts the administrator to set it up.   
2. If the email is already archived or expired, the system displays a message indicating the action cannot be performed.   
3. If the retention policy is not assigned, the system archives the email without applying any policy.   
4. If the administrator cancels the archiving operation, the system returns to the email list without making any changes.   
5. If the selected email is corrupted or cannot be archived, the system displays an error and suggests recovery options.  
  
Use Case Name: Search Email Archive   
Use Case ID: UC-06   
Actors: Administrator, Email Archive, Email, Email Account, Retention Policy, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one email in the archive folder.   
3. The system supports searching within the email archive.   
4. The archive folder is properly configured.   
  
Postconditions:   
1. The administrator receives a list of emails matching the search criteria.   
2. The system displays the search results without modifying the archive.   
3. The administrator can select and view specific emails from the results.   
4. A recovery record is created if the viewed emails are subject to retention policies.   
  
Main Flow:   
1. The administrator navigates to the "Email Archive" section of the system.   
2. The system displays the search interface with options for keywords, date range, sender, recipient, and email account.   
3. The administrator enters search criteria and clicks the "Search" button.   
4. The system processes the query and retrieves matching emails from the archive.   
5. The system displays the search results to the administrator.   
6. The administrator selects an email from the results for viewing or further action.   
7. The system retrieves and displays the selected email's content.   
  
Alternative Flow:   
1. If no emails match the search criteria, the system displays a message indicating no results were found.   
2. If the search criteria are invalid or incomplete, the system prompts the administrator to correct them.   
3. If the archive folder is empty or not configured, the system alerts the administrator and suggests corrective actions.   
4. If the administrator cancels the search operation, the system returns to the archive interface without performing a search.   
5. If the selected email is corrupted or cannot be retrieved, the system displays an error message and suggests recovery options.  
  
Use Case Name: Manage Email Archive   
Use Case ID: UC-07   
Actors: Administrator, Email Archive, Email, Email Account, Retention Policy, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one email in the archive folder.   
3. The email archive is properly configured and accessible.   
4. The administrator has the necessary permissions to manage archived emails.   
  
Postconditions:   
1. The administrator can perform actions such as view, restore, or delete an email in the archive.   
2. The email's status is updated in the system (e.g., restored to inbox or deleted permanently).   
3. A recovery record is created if the email is restored or deleted.   
4. If retention policies are enabled, the system logs the archive management action.   
  
Main Flow:   
1. The administrator navigates to the "Email Archive" section of the system.   
2. The system displays a list of archived emails with summary details.   
3. The administrator selects an email to manage (e.g., view, restore, delete).   
4. The system retrieves the selected email and presents the available actions.   
5. The administrator chooses an action (e.g., restore to inbox or delete permanently).   
6. The system verifies the action is valid for the selected email.   
7. The system performs the requested action and updates the email status accordingly.   
8. A recovery record is created for the email if retention policies are in effect.   
9. The system confirms the action was completed and updates the archive list.   
  
Alternative Flow:   
1. If the selected email is corrupted or cannot be accessed, the system displays an error and suggests recovery options.   
2. If the administrator attempts to delete an email subject to a retention policy, the system displays a warning and may prevent deletion until the policy allows it.   
3. If the archive folder is not configured, the system displays an error and prompts the administrator to set it up.   
4. If the administrator cancels the management operation, the system returns to the archive list without making any changes.   
5. If the system cannot perform the requested action due to insufficient permissions, it alerts the administrator and suggests contacting a higher-level administrator for assistance.  
  
Use Case Name: Create Calendar   
Use Case ID: UC-08   
Actors: Administrator, Calendar, Email, Contact, Distribution Group, Email Account, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has access to the calendar functionality.   
3. The administrator has the necessary permissions to create calendar events.   
4. The system supports integration with contacts and distribution groups.   
  
Postconditions:   
1. A new calendar event is created and saved in the system.   
2. The event details are associated with the administrator and relevant contacts or distribution groups.   
3. The system updates the calendar view to reflect the new event.   
4. If applicable, the system creates a recovery record for the calendar event under retention policies.   
  
Main Flow:   
1. The administrator selects the "Create Calendar" option from the system interface.   
2. The system displays the calendar event creation form with fields for title, date and time, location, attendees, and description.   
3. The administrator fills in the event title, date, time, and location.   
4. The administrator selects attendees, which may include individual contacts or distribution groups.   
5. The administrator optionally adds a description or additional details for the event.   
6. The administrator confirms the event details and clicks "Save."   
7. The system validates the input and creates the calendar event.   
8. The system updates the calendar view and notifies the administrator of the event creation.   
  
Alternative Flow:   
1. If the administrator does not provide a valid date or time, the system displays an error message and prompts for correction.   
2. If the selected attendees are invalid or not available, the system alerts the administrator and allows modification.   
3. If the administrator cancels the operation during event creation, the system discards any unsaved changes and returns to the previous screen.   
4. If the system fails to save the event due to technical issues, it logs the error and provides a recovery option.   
5. If the event creation is subject to retention policies and the system is configured to track it, a recovery record is created automatically.  
  
Use Case Name: View Calendar   
Use Case ID: UC-09   
Actors: Administrator, Calendar, Email, Contact, Distribution Group, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one calendar event configured.   
3. The calendar functionality is active and accessible.   
4. The administrator has permission to view calendar events.   
  
Postconditions:   
1. The administrator is able to view the details of the calendar event.   
2. The system displays the event without modifying it.   
3. If retention policies are enabled, the system logs the access to the calendar event.   
4. A recovery record is created if the calendar event is subject to retention policies.   
  
Main Flow:   
1. The administrator navigates to the "Calendar" section of the system.   
2. The system displays a list of calendar events with summary details (title, date, time, attendees).   
3. The administrator selects a specific calendar event to view.   
4. The system retrieves the event details and displays the full information, including title, date and time, location, attendees, and description.   
5. The administrator reviews the event information.   
6. The system updates the view count or logs the access if retention policies are enabled.   
  
Alternative Flow:   
1. If the selected calendar event is corrupted or cannot be retrieved, the system displays an error message and suggests recovery options.   
2. If the calendar is not configured, the system alerts the administrator and prompts for correction.   
3. If the administrator cancels the view operation, the system returns to the calendar list without making any changes.   
4. If the event is marked as expired, the system displays a warning and may move it to a recovery record for potential restoration.  
  
Use Case Name: Update Calendar   
Use Case ID: UC-10   
Actors: Administrator, Calendar, Email, Contact, Distribution Group, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing calendar event.   
3. The administrator has the necessary permissions to update calendar events.   
4. The system supports calendar modifications and notifications.   
  
Postconditions:   
1. The selected calendar event is updated with new details.   
2. The calendar view is refreshed to reflect the changes.   
3. Attendees are notified of the event update if applicable.   
4. A recovery record is created if the update is subject to retention policies.   
  
Main Flow:   
1. The administrator navigates to the "Calendar" section of the system.   
2. The system displays a list of calendar events with summary details.   
3. The administrator selects a specific calendar event to update.   
4. The system retrieves the event details and opens the event editing form.   
5. The administrator modifies the event details, such as title, date, time, location, or attendees.   
6. The administrator clicks the "Update" button to save the changes.   
7. The system validates the updated input and confirms the event is ready to be saved.   
8. The system updates the calendar event and refreshes the calendar view.   
9. If the event has attendees, the system sends a notification to inform them of the changes.   
  
Alternative Flow:   
1. If the administrator does not provide a valid date or time, the system displays an error message and prompts for correction.   
2. If the selected attendees are invalid or not available, the system alerts the administrator and allows modification.   
3. If the administrator cancels the update operation, the system discards any changes and returns to the calendar view.   
4. If the system fails to update the event due to technical issues, it logs the error and provides a recovery option.   
5. If the event is marked as expired, the system displays a warning and may move it to a recovery record for potential restoration.  
  
Use Case Name: Delete Calendar   
Use Case ID: UC-11   
Actors: Administrator, Calendar, Email, Contact, Distribution Group, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing calendar event.   
3. The administrator has the necessary permissions to delete calendar events.   
4. The calendar functionality is active and accessible.   
  
Postconditions:   
1. The selected calendar event is deleted from the system.   
2. The calendar view is refreshed to reflect the deletion.   
3. Attendees are notified of the event cancellation if applicable.   
4. A recovery record is created if the deletion is subject to retention policies.   
  
Main Flow:   
1. The administrator navigates to the "Calendar" section of the system.   
2. The system displays a list of calendar events with summary details.   
3. The administrator selects a specific calendar event to delete.   
4. The system confirms the deletion with a prompt to ensure the action is intentional.   
5. The administrator confirms the deletion by clicking "Delete."   
6. The system verifies the administrator's permissions and processes the deletion.   
7. The system removes the event from the calendar and updates the calendar view.   
8. If the event has attendees, the system sends a cancellation notification.   
9. The system logs the deletion action and creates a recovery record if retention policies are enabled.   
  
Alternative Flow:   
1. If the administrator does not confirm the deletion, the system cancels the operation and returns to the calendar view.   
2. If the system fails to delete the event due to technical issues, it logs the error and provides a recovery option.   
3. If the selected calendar event is already expired, the system displays a message and may move it to a recovery record instead of deleting it permanently.   
4. If the administrator does not have permission to delete the event, the system alerts them and suggests contacting a higher-level administrator for assistance.   
5. If the calendar is not configured properly, the system displays an error and prompts the administrator to correct the configuration.  
  
Use Case Name: Schedule Event   
Use Case ID: UC-12   
Actors: Administrator, Calendar, Email, Contact, Distribution Group, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one calendar configured.   
3. The administrator has the necessary permissions to schedule events.   
4. The system supports event scheduling and sending email notifications.   
  
Postconditions:   
1. A new event is scheduled in the calendar.   
2. The event is associated with the administrator and relevant attendees.   
3. Email notifications are sent to the attendees if configured.   
4. A recovery record is created if the event is subject to retention policies.   
  
Main Flow:   
1. The administrator selects the "Schedule Event" option from the calendar interface.   
2. The system displays the event scheduling form with fields for title, date and time, location, and attendees.   
3. The administrator fills in the event title, date, time, and location.   
4. The administrator selects attendees, which may include individual contacts or distribution groups.   
5. The administrator optionally configures email notifications for the attendees.   
6. The administrator confirms the event details and clicks "Schedule."   
7. The system validates the input and confirms the event is ready to be scheduled.   
8. The system adds the event to the calendar and updates the calendar view.   
9. If email notifications are enabled, the system sends the notifications to the selected attendees.   
  
Alternative Flow:   
1. If the administrator does not provide a valid date or time, the system displays an error message and prompts for correction.   
2. If the selected attendees are invalid or not available, the system alerts the administrator and allows modification.   
3. If the system fails to send email notifications, it logs the failure and provides a recovery option.   
4. If the administrator cancels the operation during event scheduling, the system discards any unsaved changes and returns to the calendar view.   
5. If the system fails to schedule the event due to technical issues, it logs the error and provides a recovery option.  
  
Use Case Name: Modify Event   
Use Case ID: UC-13   
Actors: Administrator, Calendar, Email, Contact, Distribution Group, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing calendar event.   
3. The administrator has the necessary permissions to modify calendar events.   
4. The system supports event modification and notification updates.   
  
Postconditions:   
1. The selected calendar event is updated with the new details.   
2. The calendar view reflects the changes.   
3. Attendees are notified of the event modification if applicable.   
4. A recovery record is created if the event is subject to retention policies.   
  
Main Flow:   
1. The administrator navigates to the "Calendar" section of the system.   
2. The system displays a list of calendar events with summary details.   
3. The administrator selects a specific calendar event to modify.   
4. The system retrieves the event details and opens the event editing form.   
5. The administrator updates event details, such as title, date, time, location, or attendees.   
6. The administrator clicks the "Save Changes" button.   
7. The system validates the updated information and confirms the event is ready to be modified.   
8. The system updates the calendar event and refreshes the calendar view.   
9. If the event has attendees, the system sends a notification to inform them of the changes.   
  
Alternative Flow:   
1. If the administrator does not provide a valid date or time, the system displays an error message and prompts for correction.   
2. If the selected attendees are invalid or not available, the system alerts the administrator and allows modification.   
3. If the administrator cancels the modification operation, the system discards any changes and returns to the calendar view.   
4. If the system fails to update the event due to technical issues, it logs the error and provides a recovery option.   
5. If the event is marked as expired, the system displays a warning and may move it to a recovery record for potential restoration.  
  
Use Case Name: Cancel Event   
Use Case ID: UC-14   
Actors: Administrator, Calendar, Email, Contact, Distribution Group, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. There is at least one scheduled calendar event in the system.   
3. The administrator has the necessary permissions to cancel calendar events.   
4. The calendar functionality is active and accessible.   
  
Postconditions:   
1. The selected calendar event is canceled and removed from the calendar.   
2. Attendees are notified of the cancellation if applicable.   
3. A recovery record is created if the cancellation is subject to retention policies.   
4. The calendar view is updated to reflect the cancellation.   
  
Main Flow:   
1. The administrator navigates to the "Calendar" section of the system.   
2. The system displays a list of scheduled calendar events with summary details.   
3. The administrator selects a specific calendar event to cancel.   
4. The system confirms the cancellation with a prompt to ensure the action is intentional.   
5. The administrator confirms the cancellation by clicking "Cancel Event."   
6. The system verifies the administrator's permissions and processes the cancellation.   
7. The system removes the event from the calendar and updates the calendar view.   
8. If the event has attendees, the system sends a cancellation notification.   
9. The system logs the cancellation action and creates a recovery record if retention policies are enabled.   
  
Alternative Flow:   
1. If the administrator does not confirm the cancellation, the system cancels the operation and returns to the calendar view.   
2. If the system fails to send cancellation notifications, it logs the failure and provides a recovery option.   
3. If the selected calendar event is already expired, the system displays a message and may move it to a recovery record instead of canceling it.   
4. If the administrator does not have permission to cancel the event, the system alerts them and suggests contacting a higher-level administrator for assistance.   
5. If the calendar is not configured properly, the system displays an error and prompts the administrator to correct the configuration.  
  
Use Case Name: Create Contact   
Use Case ID: UC-15   
Actors: Administrator, Contact, Email, Email Account, Distribution Group, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system supports contact creation and management.   
3. The administrator has the necessary permissions to create contacts.   
4. At least one valid email account is configured in the system.   
  
Postconditions:   
1. A new contact is created and saved in the system.   
2. The contact is associated with the correct email account if applicable.   
3. The contact can be used in future email and calendar operations.   
4. A recovery record is created if the contact is subject to retention policies.   
  
Main Flow:   
1. The administrator selects the "Create Contact" option from the system interface.   
2. The system displays the contact creation form with fields for name, email address, phone number, and additional details.   
3. The administrator enters the contact's name and primary email address.   
4. The administrator optionally adds a phone number or other relevant information.   
5. The administrator selects the associated email account for the contact if needed.   
6. The administrator confirms the contact details and clicks "Save."   
7. The system validates the input and creates the contact.   
8. The system updates the contact list and notifies the administrator of the successful creation.   
  
Alternative Flow:   
1. If the administrator does not provide a valid email address, the system displays an error message and prompts for correction.   
2. If the selected email account is invalid or not available, the system alerts the administrator and allows modification.   
3. If the administrator cancels the operation during contact creation, the system discards any unsaved changes and returns to the previous screen.   
4. If the system fails to save the contact due to technical issues, it logs the error and provides a recovery option.   
5. If the contact is subject to retention policies, a recovery record is created automatically.  
  
Use Case Name: View Contact   
Use Case ID: UC-16   
Actors: Administrator, Contact, Email, Email Account, Distribution Group, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one contact configured.   
3. The contact functionality is active and accessible.   
4. The administrator has permission to view contacts.   
  
Postconditions:   
1. The administrator is able to view the full details of the selected contact.   
2. The contact details remain unchanged in the system.   
3. If retention policies are enabled, the system logs the access to the contact record.   
4. A recovery record is created if the contact is subject to retention policies.   
  
Main Flow:   
1. The administrator navigates to the "Contacts" section of the system.   
2. The system displays a list of contacts with summary details (name, email address, phone number).   
3. The administrator selects a specific contact to view.   
4. The system retrieves the contact details and displays the full information, including name, email, phone number, and any additional notes.   
5. The administrator reviews the contact information.   
6. The system logs the view action if retention policies are enabled.   
  
Alternative Flow:   
1. If the selected contact is corrupted or cannot be retrieved, the system displays an error message and suggests recovery options.   
2. If the contact list is empty or not configured, the system alerts the administrator and suggests creating a new contact.   
3. If the administrator cancels the view operation, the system returns to the contact list without making any changes.   
4. If the contact is marked as expired, the system displays a warning and may move it to a recovery record for potential restoration.  
  
Use Case Name: Update Contact   
Use Case ID: UC-17   
Actors: Administrator, Contact, Email, Email Account, Distribution Group, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing contact.   
3. The administrator has the necessary permissions to update contacts.   
4. The contact functionality is active and accessible.   
  
Postconditions:   
1. The selected contact is updated with the new information.   
2. The contact list is refreshed to reflect the changes.   
3. If applicable, the system updates the associated email account or distribution group.   
4. A recovery record is created if the update is subject to retention policies.   
  
Main Flow:   
1. The administrator navigates to the "Contacts" section of the system.   
2. The system displays a list of contacts with summary details.   
3. The administrator selects a specific contact to update.   
4. The system retrieves the contact details and opens the contact editing form.   
5. The administrator modifies the contact's information, such as name, email address, phone number, or additional notes.   
6. The administrator clicks the "Update" button to save the changes.   
7. The system validates the updated information and confirms the contact is ready to be saved.   
8. The system updates the contact record and refreshes the contact list.   
9. The system logs the update action and creates a recovery record if retention policies are enabled.   
  
Alternative Flow:   
1. If the administrator does not provide a valid email address, the system displays an error message and prompts for correction.   
2. If the system fails to update the contact due to technical issues, it logs the error and provides a recovery option.   
3. If the selected contact is already expired, the system displays a message and may move it to a recovery record for potential restoration.   
4. If the administrator cancels the update operation, the system discards any changes and returns to the contact list.   
5. If the contact is associated with a distribution group or calendar event, the system updates the relevant references and sends notifications if configured.  
  
Use Case Name: Delete Contact   
Use Case ID: UC-18   
Actors: Administrator, Contact, Email, Email Account, Distribution Group, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing contact.   
3. The administrator has the necessary permissions to delete contacts.   
4. The contact functionality is active and accessible.   
  
Postconditions:   
1. The selected contact is deleted from the system.   
2. The contact list is updated to reflect the deletion.   
3. If the contact is part of a distribution group or linked to an email, the system updates the references accordingly.   
4. A recovery record is created if the deletion is subject to retention policies.   
  
Main Flow:   
1. The administrator navigates to the "Contacts" section of the system.   
2. The system displays a list of contacts with summary details.   
3. The administrator selects a specific contact to delete.   
4. The system confirms the deletion with a prompt to ensure the action is intentional.   
5. The administrator confirms the deletion by clicking "Delete."   
6. The system verifies the administrator's permissions and processes the deletion.   
7. The system removes the contact from the contact list and updates related references.   
8. The system logs the deletion action and creates a recovery record if retention policies are enabled.   
9. The system confirms the successful deletion of the contact.   
  
Alternative Flow:   
1. If the administrator does not confirm the deletion, the system cancels the operation and returns to the contact list.   
2. If the system fails to delete the contact due to technical issues, it logs the error and provides a recovery option.   
3. If the selected contact is already expired, the system displays a message and may move it to a recovery record instead of deleting it permanently.   
4. If the administrator does not have permission to delete the contact, the system alerts them and suggests contacting a higher-level administrator for assistance.   
5. If the contact is referenced in a distribution group or email, the system displays a warning and allows the administrator to confirm or cancel the deletion to avoid unintended data loss.  
  
Use Case Name: Create Distribution Group   
Use Case ID: UC-19   
Actors: Administrator, Contact, Email, Email Account, Distribution Group, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system supports the creation of distribution groups.   
3. There are at least one or more contacts available in the system.   
4. The administrator has the necessary permissions to create distribution groups.   
  
Postconditions:   
1. A new distribution group is created and saved in the system.   
2. The group is associated with the selected contacts.   
3. The distribution group can be used in future email and calendar operations.   
4. A recovery record is created if the distribution group is subject to retention policies.   
  
Main Flow:   
1. The administrator selects the "Create Distribution Group" option from the system interface.   
2. The system displays the distribution group creation form with fields for group name, description, and contact selection.   
3. The administrator enters a name for the distribution group and an optional description.   
4. The administrator selects one or more contacts to include in the group.   
5. The administrator confirms the group details and clicks "Save."   
6. The system validates the input and creates the distribution group.   
7. The system updates the distribution group list and notifies the administrator of the successful creation.   
  
Alternative Flow:   
1. If the administrator does not provide a valid group name, the system displays an error message and prompts for correction.   
2. If the selected contacts are invalid or not available, the system alerts the administrator and allows modification.   
3. If the administrator cancels the operation during group creation, the system discards any unsaved changes and returns to the previous screen.   
4. If the system fails to save the distribution group due to technical issues, it logs the error and provides a recovery option.   
5. If the distribution group is subject to retention policies, a recovery record is created automatically.  
  
Use Case Name: Add Contact to Distribution Group   
Use Case ID: UC-20   
Actors: Administrator, Contact, Distribution Group, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing contact and one existing distribution group.   
3. The administrator has the necessary permissions to modify distribution groups.   
4. The contact and distribution group functionality is active and accessible.   
  
Postconditions:   
1. The selected contact is added to the distribution group.   
2. The distribution group is updated to include the new contact.   
3. A recovery record is created if the addition is subject to retention policies.   
4. The system confirms the successful addition of the contact to the group.   
  
Main Flow:   
1. The administrator navigates to the "Distribution Groups" section of the system.   
2. The system displays a list of existing distribution groups with summary details.   
3. The administrator selects a specific distribution group to modify.   
4. The system retrieves the group details and opens the group editing interface.   
5. The administrator searches for and selects a contact to add to the group.   
6. The system validates the contact and confirms the addition.   
7. The system updates the distribution group to include the selected contact.   
8. The system logs the action and creates a recovery record if retention policies are enabled.   
9. The system confirms the contact has been successfully added to the group.   
  
Alternative Flow:   
1. If the selected contact is invalid or not available, the system alerts the administrator and allows modification.   
2. If the administrator cancels the operation during the addition process, the system discards any changes and returns to the distribution group list.   
3. If the system fails to add the contact due to technical issues, it logs the error and provides a recovery option.   
4. If the selected contact is already part of the distribution group, the system displays a message indicating the action cannot be performed.   
5. If the distribution group is marked as expired, the system displays a warning and may move it to a recovery record for potential restoration.  
  
Use Case Name: Remove Contact from Distribution Group   
Use Case ID: UC-21   
Actors: Administrator, Contact, Distribution Group, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing distribution group and one contact.   
3. The administrator has the necessary permissions to modify distribution groups.   
4. The contact is currently a member of the selected distribution group.   
  
Postconditions:   
1. The selected contact is removed from the distribution group.   
2. The distribution group is updated to reflect the removal.   
3. A recovery record is created if the removal is subject to retention policies.   
4. The system confirms the successful removal of the contact from the group.   
  
Main Flow:   
1. The administrator navigates to the "Distribution Groups" section of the system.   
2. The system displays a list of existing distribution groups with summary details.   
3. The administrator selects a specific distribution group to modify.   
4. The system retrieves the group details and opens the group editing interface.   
5. The administrator searches for and selects a contact to remove from the group.   
6. The system confirms the removal with a prompt to ensure the action is intentional.   
7. The administrator confirms the removal by clicking "Remove."   
8. The system verifies the administrator's permissions and processes the removal.   
9. The system updates the distribution group and logs the action.   
10. If retention policies are enabled, the system creates a recovery record for the removal.   
11. The system confirms the successful removal of the contact from the distribution group.   
  
Alternative Flow:   
1. If the selected contact is not a member of the distribution group, the system displays a message indicating the action cannot be performed.   
2. If the administrator does not confirm the removal, the system cancels the operation and returns to the distribution group details.   
3. If the system fails to remove the contact due to technical issues, it logs the error and provides a recovery option.   
4. If the administrator cancels the operation during the removal process, the system discards any changes and returns to the distribution group list.   
5. If the distribution group is marked as expired, the system displays a warning and may move it to a recovery record for potential restoration.  
  
Use Case Name: Delete Distribution Group   
Use Case ID: UC-22   
Actors: Administrator, Distribution Group, Contact, Email, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing distribution group.   
3. The administrator has the necessary permissions to delete distribution groups.   
4. The distribution group functionality is active and accessible.   
  
Postconditions:   
1. The selected distribution group is deleted from the system.   
2. The distribution group list is updated to reflect the deletion.   
3. A recovery record is created if the deletion is subject to retention policies.   
4. If the group is referenced in an email or calendar event, the system updates the references accordingly.   
  
Main Flow:   
1. The administrator navigates to the "Distribution Groups" section of the system.   
2. The system displays a list of existing distribution groups with summary details.   
3. The administrator selects a specific distribution group to delete.   
4. The system confirms the deletion with a prompt to ensure the action is intentional.   
5. The administrator confirms the deletion by clicking "Delete."   
6. The system verifies the administrator's permissions and processes the deletion.   
7. The system removes the distribution group from the system and updates the group list.   
8. The system logs the deletion action and creates a recovery record if retention policies are enabled.   
9. The system confirms the successful deletion of the distribution group.   
  
Alternative Flow:   
1. If the administrator does not confirm the deletion, the system cancels the operation and returns to the distribution group list.   
2. If the system fails to delete the distribution group due to technical issues, it logs the error and provides a recovery option.   
3. If the selected distribution group is already expired, the system displays a message and may move it to a recovery record instead of deleting it permanently.   
4. If the administrator does not have permission to delete the group, the system alerts them and suggests contacting a higher-level administrator for assistance.   
5. If the distribution group is referenced in an email or calendar event, the system displays a warning and allows the administrator to confirm or cancel the deletion to avoid unintended data loss.  
  
Use Case Name: Create Email Account   
Use Case ID: UC-23   
Actors: Administrator, Email Account, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system supports email account creation and configuration.   
3. The administrator has the necessary permissions to create email accounts.   
4. The system has access to email server settings or external email service.   
  
Postconditions:   
1. A new email account is successfully created and configured in the system.   
2. The email account is accessible to the administrator for sending and receiving emails.   
3. A recovery record is created if the email account is subject to retention policies.   
4. The system updates the email account list to include the new account.   
  
Main Flow:   
1. The administrator selects the "Create Email Account" option from the system interface.   
2. The system displays the email account creation form with fields for username, password, email server settings, and account type.   
3. The administrator enters the required details, including the username, password, and server configuration (e.g., IMAP, SMTP).   
4. The administrator selects the account type (e.g., personal, group, recovery).   
5. The administrator confirms the details and clicks "Save."   
6. The system validates the input and connects to the email server to verify the account configuration.   
7. The system creates the email account and adds it to the account list.   
8. The system logs the account creation and creates a recovery record if retention policies are enabled.   
9. The system confirms the successful creation of the email account.   
  
Alternative Flow:   
1. If the administrator does not provide a valid username or password, the system displays an error message and prompts for correction.   
2. If the email server settings are incorrect or the system cannot connect to the server, the system alerts the administrator and allows modification.   
3. If the administrator cancels the operation during account creation, the system discards any unsaved changes and returns to the previous screen.   
4. If the system fails to create the email account due to technical issues, it logs the error and provides a recovery option.   
5. If the email account is subject to retention policies, a recovery record is created automatically, even if the operation is canceled or failed.  
  
Use Case Name: Delete Email Account   
Use Case ID: UC-24   
Actors: Administrator, Email Account, Email, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing email account.   
3. The administrator has the necessary permissions to delete email accounts.   
4. The email account to be deleted is not currently being used for active emails.   
  
Postconditions:   
1. The selected email account is deleted from the system.   
2. All associated data (e.g., emails) is either moved to a recovery record or deleted, depending on retention policies.   
3. The email account list is updated to reflect the deletion.   
4. A recovery record is created if the deletion is subject to retention policies.   
  
Main Flow:   
1. The administrator navigates to the "Email Accounts" section of the system.   
2. The system displays a list of existing email accounts with summary details (username, account type, status).   
3. The administrator selects a specific email account to delete.   
4. The system confirms the deletion with a prompt to ensure the action is intentional.   
5. The administrator confirms the deletion by clicking "Delete."   
6. The system verifies the administrator's permissions and processes the deletion.   
7. The system removes the selected email account and updates the account list.   
8. If retention policies are enabled, the system creates a recovery record for the deleted account.   
9. The system confirms the successful deletion of the email account.   
  
Alternative Flow:   
1. If the administrator does not confirm the deletion, the system cancels the operation and returns to the email account list.   
2. If the system fails to delete the email account due to technical issues, it logs the error and provides a recovery option.   
3. If the selected email account is already expired, the system displays a message and may move it to a recovery record instead of deleting it permanently.   
4. If the administrator does not have permission to delete the account, the system alerts them and suggests contacting a higher-level administrator for assistance.   
5. If the email account is referenced in an email or calendar event, the system displays a warning and allows the administrator to confirm or cancel the deletion to avoid unintended data loss.  
  
Use Case Name: Manage Email Account   
Use Case ID: UC-25   
Actors: Administrator, Email Account, Email, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing email account.   
3. The administrator has the necessary permissions to manage email accounts.   
4. The email account functionality is active and accessible.   
  
Postconditions:   
1. The selected email account is either updated or deleted.   
2. The system reflects the changes in the email account list.   
3. A recovery record is created if the account is deleted and subject to retention policies.   
4. The administrator is notified of the successful management of the email account.   
  
Main Flow:   
1. The administrator navigates to the "Email Accounts" section of the system.   
2. The system displays a list of existing email accounts with summary details (username, account type, status).   
3. The administrator selects a specific email account to manage.   
4. The system opens the account management interface, offering options to update or delete the account.   
5. If updating, the administrator modifies the account details (e.g., password, server settings, or account type).   
6. If deleting, the system confirms the deletion with a prompt to ensure the action is intentional.   
7. The administrator confirms the action.   
8. The system validates the changes or verifies the deletion permissions and processes the action.   
9. The system updates the email account list and logs the management action.   
10. The system confirms the successful update or deletion of the email account.   
  
Alternative Flow:   
1. If the administrator does not provide valid server settings during an update, the system displays an error and prompts for correction.   
2. If the system fails to update the email account due to technical issues, it logs the error and provides a recovery option.   
3. If the selected email account is already expired, the system displays a message and may move it to a recovery record for potential restoration.   
4. If the administrator does not have permission to manage the account, the system alerts them and suggests contacting a higher-level administrator for assistance.   
5. If the administrator cancels the operation during management, the system discards any changes and returns to the email account list.   
6. If the email account is referenced in an email or calendar event, the system displays a warning and allows the administrator to confirm or cancel the deletion to avoid unintended data loss.  
  
Use Case Name: Assign Administrator   
Use Case ID: UC-26   
Actors: Administrator, Email Account, Recovery Record   
Preconditions:   
1. The system has at least one email account configured.   
2. The administrator is logged into the system and has the necessary permissions to assign administrative privileges.   
3. The system supports assigning administrator roles to email accounts.   
  
Postconditions:   
1. The selected email account has a new administrator assigned.   
2. The administrator list for the email account is updated in the system.   
3. A recovery record is created if the assignment is subject to retention policies.   
4. The system confirms the successful assignment of the administrator.   
  
Main Flow:   
1. The administrator navigates to the "Email Accounts" section of the system.   
2. The system displays a list of existing email accounts with summary details.   
3. The administrator selects an email account to assign a new administrator.   
4. The system displays a list of available users or roles that can be assigned as administrators.   
5. The administrator selects a user or role to assign as the new administrator.   
6. The system confirms the assignment with a prompt to ensure the action is intentional.   
7. The administrator confirms the assignment by clicking "Assign."   
8. The system validates the selection and updates the administrator list for the email account.   
9. The system logs the assignment action and creates a recovery record if retention policies are enabled.   
10. The system confirms the successful assignment of the new administrator to the email account.   
  
Alternative Flow:   
1. If the selected user or role is invalid or not available, the system alerts the administrator and allows modification.   
2. If the administrator does not confirm the assignment, the system cancels the operation and returns to the email account list.   
3. If the system fails to assign the administrator due to technical issues, it logs the error and provides a recovery option.   
4. If the email account is already expired, the system displays a message and may move it to a recovery record for potential restoration.   
5. If the administrator does not have permission to assign roles, the system alerts them and suggests contacting a higher-level administrator for assistance.   
6. If the administrator cancels the operation during the assignment process, the system discards any changes and returns to the email account list.  
  
Use Case Name: Revoke Administrator   
Use Case ID: UC-27   
Actors: Administrator, Email Account, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one email account with an assigned administrator.   
3. The administrator has the necessary permissions to revoke administrative privileges.   
4. The system supports revoking administrator roles from email accounts.   
  
Postconditions:   
1. The selected email account has the administrator role revoked from the specified user or role.   
2. The administrator list for the email account is updated in the system.   
3. A recovery record is created if the revocation is subject to retention policies.   
4. The system confirms the successful revocation of the administrator.   
  
Main Flow:   
1. The administrator navigates to the "Email Accounts" section of the system.   
2. The system displays a list of existing email accounts with summary details.   
3. The administrator selects an email account from which to revoke an administrator.   
4. The system displays the list of currently assigned administrators for the selected email account.   
5. The administrator selects the user or role to revoke.   
6. The system confirms the revocation with a prompt to ensure the action is intentional.   
7. The administrator confirms the revocation by clicking "Revoke."   
8. The system validates the selection and revokes the administrator privileges from the email account.   
9. The system logs the revocation action and creates a recovery record if retention policies are enabled.   
10. The system confirms the successful revocation of the administrator from the email account.   
  
Alternative Flow:   
1. If the selected user or role is not an administrator of the email account, the system displays a message indicating the action cannot be performed.   
2. If the administrator does not confirm the revocation, the system cancels the operation and returns to the email account details.   
3. If the system fails to revoke the administrator due to technical issues, it logs the error and provides a recovery option.   
4. If the email account is already expired, the system displays a message and may move it to a recovery record for potential restoration.   
5. If the administrator does not have permission to revoke roles, the system alerts them and suggests contacting a higher-level administrator for assistance.   
6. If the administrator cancels the operation during the revocation process, the system discards any changes and returns to the email account list.  
  
Use Case Name: View Recovery Record   
Use Case ID: UC-28   
Actors: Administrator, Recovery Record, Email, Email Account, Retention Policy   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system contains at least one recovery record.   
3. The recovery record functionality is active and accessible.   
4. The administrator has the necessary permissions to view recovery records.   
  
Postconditions:   
1. The administrator is able to view the details of the selected recovery record.   
2. The recovery record remains in the system.   
3. If retention policies are enabled, the system logs the access to the recovery record.   
4. The administrator can identify the original email or account associated with the recovery record.   
  
Main Flow:   
1. The administrator navigates to the "Recovery Records" section of the system.   
2. The system displays a list of recovery records with summary details (record ID, associated email, date of action).   
3. The administrator selects a specific recovery record to view.   
4. The system retrieves the recovery record details and displays the full information, including the action taken, date of action, associated email or account, and any additional metadata.   
5. The administrator reviews the recovery record to understand the history of the action.   
6. The system logs the view action if retention policies are enabled.   
  
Alternative Flow:   
1. If the selected recovery record is corrupted or cannot be retrieved, the system displays an error message and suggests recovery options.   
2. If the recovery record list is empty or not configured, the system alerts the administrator and suggests checking the retention policy settings.   
3. If the administrator cancels the view operation, the system returns to the recovery record list without making any changes.   
4. If the recovery record is marked as expired, the system displays a warning and may move it to an archive for potential future reference.   
5. If the administrator does not have permission to view the recovery record, the system alerts them and suggests contacting a higher-level administrator for assistance.  
  
Use Case Name: Restore Email   
Use Case ID: UC-06   
Actors: Administrator, Email, Email Account, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system contains at least one recovery record for an expired or deleted email.   
3. The administrator has the necessary permissions to restore emails.   
4. The recovery record functionality is active and accessible.   
  
Postconditions:   
1. The selected email is restored to its original folder or a specified folder.   
2. The email status is updated to "Restored."   
3. A recovery record is updated to reflect the restoration action.   
4. The system logs the restoration and updates the retention policy accordingly.   
  
Main Flow:   
1. The administrator navigates to the "Recovery Records" section of the system.   
2. The system displays a list of recovery records with summary details (record ID, associated email, date of action).   
3. The administrator selects a recovery record for an expired or deleted email to restore.   
4. The system retrieves the recovery record details and confirms the email can be restored.   
5. The administrator selects a target folder for the restored email (e.g., inbox, archive).   
6. The system restores the email to the selected folder and updates the email status.   
7. The system updates the recovery record with the restoration action and logs the event.   
8. The system confirms the successful restoration of the email.   
  
Alternative Flow:   
1. If the selected recovery record is corrupted or invalid, the system displays an error and suggests recovery options.   
2. If the target folder is not available or configured, the system alerts the administrator and prompts for correction.   
3. If the email has already been restored, the system displays a message indicating the action cannot be performed.   
4. If the administrator cancels the restoration operation, the system returns to the recovery record list without making any changes.   
5. If the system fails to restore the email due to technical issues, it logs the error and provides a recovery option.  
  
Use Case Name: Manage Retention Policy   
Use Case ID: UC-29   
Actors: Administrator, Email, Email Account, Archive, Retention Policy, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one email or email account that can be associated with a retention policy.   
3. The administrator has the necessary permissions to manage retention policies.   
4. The retention policy functionality is active and accessible in the system.   
  
Postconditions:   
1. The retention policy is created, updated, or deleted as specified.   
2. The system applies the retention policy to the associated emails or accounts.   
3. A recovery record is created if the retention policy change affects emails subject to retention.   
4. The system confirms the successful management of the retention policy.   
  
Main Flow:   
1. The administrator navigates to the "Retention Policies" section of the system.   
2. The system displays a list of existing retention policies with summary details (policy name, duration, scope, status).   
3. The administrator selects an option to create a new retention policy or modify an existing one.   
4. If creating, the administrator fills in the policy name, duration, and selects the scope (e.g., all emails, specific account).   
5. If modifying, the system retrieves the selected policy and opens the editing interface.   
6. The administrator updates the policy details as needed (e.g., change duration, scope, or status).   
7. The administrator clicks "Save" or "Delete" to confirm the action.   
8. The system validates the input and processes the policy change.   
9. The system updates the retention policy list and logs the action.   
10. If applicable, the system updates affected emails or accounts and creates recovery records.   
11. The system confirms the successful management of the retention policy.   
  
Alternative Flow:   
1. If the administrator does not provide valid policy details (e.g., invalid duration), the system displays an error message and prompts for correction.   
2. If the system fails to save or delete the retention policy due to technical issues, it logs the error and provides a recovery option.   
3. If the administrator cancels the operation during policy creation or modification, the system discards any changes and returns to the retention policy list.   
4. If the retention policy is already expired or deleted, the system displays a message indicating the action cannot be performed.   
5. If the administrator does not have permission to manage the retention policy, the system alerts them and suggests contacting a higher-level administrator for assistance.  
  
Use Case Name: Apply Retention Policy   
Use Case ID: UC-30   
Actors: Administrator, Email, Email Account, Archive, Retention Policy, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one email or folder that can be associated with a retention policy.   
3. The administrator has the necessary permissions to apply retention policies.   
4. A retention policy is already defined and available in the system.   
5. The email or folder is not already subject to an active retention policy.   
  
Postconditions:   
1. The retention policy is successfully applied to the selected email or folder.   
2. The system logs the policy application and updates the retention policy status for the affected data.   
3. Emails or folders under the policy are subject to the defined retention rules.   
4. A recovery record is created if the applied policy affects data that can be recovered.   
  
Main Flow:   
1. The administrator navigates to the "Retention Policies" section or the email/folder management interface.   
2. The system displays available retention policies and the list of emails or folders.   
3. The administrator selects an email or folder to apply the retention policy.   
4. The administrator chooses an appropriate retention policy from the available options.   
5. The system confirms the selected email or folder is not already under another active retention policy.   
6. The administrator confirms the policy application.   
7. The system applies the retention policy to the selected email or folder.   
8. The system updates the retention policy status and logs the action.   
9. If the policy involves automatic archiving or deletion, the system schedules or triggers the action.   
10. The system confirms the successful application of the retention policy.   
  
Alternative Flow:   
1. If the selected email or folder is already under an active retention policy, the system displays a message and allows the administrator to override or cancel.   
2. If the administrator selects an invalid retention policy, the system alerts them and prompts to choose a valid one.   
3. If the system fails to apply the retention policy due to technical issues, it logs the error and provides a recovery option.   
4. If the administrator cancels the operation during the policy application, the system returns to the management interface without making any changes.   
5. If the retention policy is expired or deleted, the system displays a message and suggests selecting an active policy for application.  
  
Use Case Name: Manage Expired Email   
Use Case ID: UC-31  
Actors: Administrator, Email, Email Account, Archive, Retention Policy, Recovery Record   
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one expired email in the system.   
3. The administrator has the necessary permissions to manage expired emails.   
4. The system supports identifying and handling expired emails.   
  
Postconditions:   
1. The expired email is either restored, deleted, or moved to a recovery record.   
2. The email status is updated in the system (e.g., restored, deleted).   
3. A recovery record is created if the email is restored or deleted.   
4. The system logs the management action and updates the retention policy accordingly.   
  
Main Flow:   
1. The administrator navigates to the "Manage Expired Email" section of the system.   
2. The system displays a list of expired emails with summary details (subject, date, associated account).   
3. The administrator selects an expired email to manage.   
4. The system retrieves the email details and presents available actions (e.g., restore, delete, move to recovery record).   
5. The administrator chooses an action to perform on the selected email.   
6. The system validates the action and confirms the email can be processed.   
7. The system performs the requested action and updates the email status.   
8. If applicable, the system creates a recovery record for the email.   
9. The system logs the management action and confirms the operation was completed.   
  
Alternative Flow:   
1. If the selected expired email is corrupted or cannot be accessed, the system displays an error message and suggests recovery options.   
2. If the administrator attempts to delete an email subject to a retention policy, the system displays a warning and prevents deletion until the policy allows it.   
3. If the system fails to perform the requested action due to technical issues, it logs the error and provides a recovery option.   
4. If the administrator cancels the management operation, the system returns to the expired email list without making any changes.   
5. If the email is already in a recovery record, the system displays a message indicating the action cannot be performed.  
  
Use Case Name: Delete Expired Email   
Use Case ID: UC-32   
Actors: Administrator, Email, Email Account, Archive, Retention Policy, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one expired email in the system.   
3. The administrator has the necessary permissions to delete expired emails.   
4. The system supports identifying and handling expired emails.   
  
Postconditions:   
1. The expired email is permanently deleted from the system.   
2. The email status is updated to "Deleted."   
3. A recovery record is created if the deletion is subject to retention policies.   
4. The system logs the deletion action and updates the retention policy accordingly.   
  
Main Flow:   
1. The administrator navigates to the "Manage Expired Email" section of the system.   
2. The system displays a list of expired emails with summary details (subject, date, associated account).   
3. The administrator selects an expired email to delete.   
4. The system confirms the deletion with a prompt to ensure the action is intentional.   
5. The administrator confirms the deletion by clicking "Delete."   
6. The system verifies the administrator's permissions and processes the deletion.   
7. The system permanently deletes the expired email and updates the email list.   
8. If retention policies are enabled, the system creates a recovery record for the deleted email.   
9. The system logs the deletion action and confirms the operation was completed.   
  
Alternative Flow:   
1. If the selected expired email is corrupted or cannot be accessed, the system displays an error message and suggests recovery options.   
2. If the administrator does not confirm the deletion, the system cancels the operation and returns to the expired email list.   
3. If the system fails to delete the expired email due to technical issues, it logs the error and provides a recovery option.   
4. If the administrator cancels the operation during the deletion process, the system returns to the expired email list without making any changes.   
5. If the email is already in a recovery record, the system displays a message indicating the action cannot be performed.  
  
Use Case Name: Manage User   
Use Case ID: UC-33   
Actors: Administrator, User, Email Account, Contact, Calendar, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one user account configured.   
3. The administrator has the necessary permissions to manage user accounts.   
4. The user management functionality is active and accessible.   
  
Postconditions:   
1. The selected user account is either updated or deleted.   
2. The system reflects the changes in the user account list.   
3. If the user is deleted, any associated data (e.g., email accounts, calendar events, contacts) is either moved to a recovery record or deleted, depending on retention policies.   
4. A recovery record is created if the user account is deleted and subject to retention policies.   
5. The system confirms the successful management of the user account.   
  
Main Flow:   
1. The administrator navigates to the "User Management" section of the system.   
2. The system displays a list of existing user accounts with summary details (username, role, status).   
3. The administrator selects a specific user account to manage.   
4. The system opens the user management interface, offering options to update or delete the user.   
5. If updating, the administrator modifies the user's details (e.g., role, permissions, status).   
6. If deleting, the system confirms the deletion with a prompt to ensure the action is intentional.   
7. The administrator confirms the action (update or delete).   
8. The system validates the changes or verifies the deletion permissions and processes the action.   
9. The system updates the user account list and logs the management action.   
10. If the user is deleted, the system identifies and processes any associated data (e.g., email accounts, calendar events, contacts) based on the configured retention policies.   
11. The system confirms the successful update or deletion of the user account.   
  
Alternative Flow:   
1. If the administrator does not provide valid user details during an update, the system displays an error and prompts for correction.   
2. If the system fails to update the user account due to technical issues, it logs the error and provides a recovery option.   
3. If the selected user is already expired or marked for deletion, the system displays a message and may move it to a recovery record instead of proceeding with the action.   
4. If the administrator does not have permission to manage the user, the system alerts them and suggests contacting a higher-level administrator for assistance.   
5. If the administrator cancels the operation during user management, the system discards any changes and returns to the user account list.   
6. If the user account is referenced in an email, calendar event, or contact, the system displays a warning and allows the administrator to confirm or cancel the deletion to avoid unintended data loss.  
  
Use Case Name: View User   
Use Case ID: UC-34   
Actors: Administrator, User, Email Account, Contact, Calendar, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one user account configured.   
3. The user functionality is active and accessible.   
4. The administrator has permission to view user account details.   
  
Postconditions:   
1. The administrator is able to view the full details of the selected user.   
2. The user account remains unchanged in the system.   
3. If retention policies are enabled, the system logs the access to the user record.   
4. A recovery record is created if the user is subject to retention policies and the action is tracked.   
  
Main Flow:   
1. The administrator navigates to the "User Management" section of the system.   
2. The system displays a list of existing user accounts with summary details (username, role, status).   
3. The administrator selects a specific user account to view.   
4. The system retrieves the user details and displays the full information, including username, role, permissions, associated email accounts, and any related calendar or contact data.   
5. The administrator reviews the user information for administrative or audit purposes.   
6. The system logs the view action if retention policies are enabled.   
  
Alternative Flow:   
1. If the selected user is corrupted or cannot be retrieved, the system displays an error message and suggests recovery options.   
2. If the user list is empty or not configured, the system alerts the administrator and suggests creating a new user.   
3. If the administrator cancels the view operation, the system returns to the user list without making any changes.   
4. If the user is marked as expired, the system displays a warning and may move it to a recovery record for potential restoration.   
5. If the administrator does not have permission to view the user details, the system alerts them and suggests contacting a higher-level administrator for assistance.  
  
Use Case Name: Update User   
Use Case ID: UC-35   
Actors: Administrator, User, Email Account, Contact, Calendar, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing user account.   
3. The administrator has the necessary permissions to update user accounts.   
4. The user management functionality is active and accessible.   
  
Postconditions:   
1. The selected user account is updated with the new information.   
2. The system reflects the changes in the user account list.   
3. If the user is associated with email accounts, calendar events, or contacts, those associations are updated accordingly.   
4. A recovery record is created if the update is subject to retention policies.   
5. The system confirms the successful update of the user account.   
  
Main Flow:   
1. The administrator navigates to the "User Management" section of the system.   
2. The system displays a list of existing user accounts with summary details (username, role, status).   
3. The administrator selects a specific user account to update.   
4. The system retrieves the user details and opens the user editing interface.   
5. The administrator modifies the user's information, such as username, role, permissions, or status.   
6. The administrator clicks the "Update" button to save the changes.   
7. The system validates the updated information and confirms the user is ready to be saved.   
8. The system updates the user account and refreshes the user list.   
9. The system logs the update action and creates a recovery record if retention policies are enabled.   
10. The system confirms the successful update of the user account.   
  
Alternative Flow:   
1. If the administrator does not provide valid user details during an update, the system displays an error and prompts for correction.   
2. If the system fails to update the user account due to technical issues, it logs the error and provides a recovery option.   
3. If the selected user is already expired or marked for deletion, the system displays a message and may move it to a recovery record instead of proceeding with the update.   
4. If the administrator does not have permission to update the user, the system alerts them and suggests contacting a higher-level administrator for assistance.   
5. If the user account is referenced in an email, calendar event, or contact, the system displays a warning and allows the administrator to confirm or cancel the update to avoid unintended data loss.  
  
Use Case Name: Create Event   
Use Case ID: UC-12   
Actors: Administrator, Calendar, Event, Contact, Distribution Group, Email Account, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one calendar configured and accessible.   
3. The administrator has the necessary permissions to create events.   
4. The system supports adding events with attendees and optional email notifications.   
5. The contact and distribution group functionality is active and accessible.   
  
Postconditions:   
1. A new event is created and added to the calendar.   
2. The event is associated with the administrator and any selected attendees.   
3. If configured, email notifications are sent to the attendees.   
4. A recovery record is created if the event is subject to retention policies.   
5. The system confirms the event creation and updates the calendar view.   
  
Main Flow:   
1. The administrator selects the "Create Event" option from the calendar interface.   
2. The system displays the event creation form with fields for title, date and time, location, attendees, and optional email notification settings.   
3. The administrator fills in the event title, date, time, and location.   
4. The administrator selects attendees, which may include individual contacts or distribution groups.   
5. The administrator optionally configures email notifications to be sent to attendees.   
6. The administrator clicks the "Save" button to create the event.   
7. The system validates the input and confirms the event is ready to be saved.   
8. The system creates the event in the calendar and updates the calendar view.   
9. If email notifications are enabled, the system sends the notification to the selected attendees.   
10. The system logs the event creation and creates a recovery record if retention policies are enabled.   
11. The system confirms the successful creation of the event.   
  
Alternative Flow:   
1. If the administrator does not provide a valid date or time, the system displays an error message and prompts for correction.   
2. If the selected attendees are invalid or not available, the system alerts the administrator and allows modification.   
3. If the system fails to send email notifications, it logs the failure and provides a recovery option.   
4. If the administrator cancels the operation during event creation, the system discards any unsaved changes and returns to the calendar view.   
5. If the system fails to create the event due to technical issues, it logs the error and provides a recovery option.   
6. If the event is subject to retention policies, a recovery record is created automatically, even if the operation is canceled or failed.  
  
Use Case Name: View Event   
Use Case ID: UC-14   
Actors: Administrator, Event, Calendar, Contact, Distribution Group, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one calendar event configured.   
3. The calendar functionality is active and accessible.   
4. The administrator has permission to view calendar events.   
  
Postconditions:   
1. The administrator is able to view the full details of the selected event.   
2. The event remains in its original state in the system.   
3. If retention policies are enabled, the system logs the access to the event record.   
4. A recovery record is created if the event is subject to retention policies and the view action is tracked.   
  
Main Flow:   
1. The administrator navigates to the "Calendar" section of the system.   
2. The system displays a list of calendar events with summary details (title, date, time, location, attendees).   
3. The administrator selects a specific calendar event to view.   
4. The system retrieves the event details and displays the full information, including title, date and time, location, attendees, and description.   
5. The administrator reviews the event information for reference or planning.   
6. The system updates the view count or logs the access if retention policies are enabled.   
  
Alternative Flow:   
1. If the selected calendar event is corrupted or cannot be retrieved, the system displays an error message and suggests recovery options.   
2. If the calendar is not configured properly, the system displays an error and prompts the administrator to correct the configuration.   
3. If the administrator cancels the view operation, the system returns to the calendar list without making any changes.   
4. If the event is marked as expired, the system displays a warning and may move it to a recovery record for potential restoration.   
5. If the administrator does not have permission to view the event, the system alerts them and suggests contacting a higher-level administrator for assistance.  
  
Use Case Name: Update Event   
Use Case ID: UC-13   
Actors: Administrator, Calendar, Event, Contact, Distribution Group, Email Account, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing calendar event.   
3. The administrator has the necessary permissions to update calendar events.   
4. The calendar and email notification functionalities are active and properly configured.   
5. The system supports updating event details and sending notifications to attendees.   
  
Postconditions:   
1. The selected calendar event is updated with the new details provided by the administrator.   
2. The calendar view is refreshed to reflect the updated event.   
3. Attendees are notified of the changes if email notifications are enabled.   
4. A recovery record is created if the update is subject to retention policies.   
5. The system confirms the successful update of the event.   
  
Main Flow:   
1. The administrator navigates to the "Calendar" section of the system.   
2. The system displays a list of calendar events with summary details (title, date, time, attendees).   
3. The administrator selects a specific calendar event to update.   
4. The system retrieves the event details and opens the event editing form.   
5. The administrator modifies the event details, such as title, date, time, location, or attendees.   
6. The administrator optionally updates the email notification settings for the event.   
7. The administrator clicks the "Update" button to save the changes.   
8. The system validates the updated input and confirms the event is ready to be modified.   
9. The system updates the calendar event and refreshes the calendar view.   
10. If email notifications are enabled, the system sends the updated information to the event attendees.   
11. The system logs the update action and creates a recovery record if retention policies are enabled.   
12. The system confirms the successful update of the event.   
  
Alternative Flow:   
1. If the administrator does not provide a valid date or time, the system displays an error message and prompts for correction.   
2. If the selected attendees are invalid or not available, the system alerts the administrator and allows modification.   
3. If the system fails to send email notifications to attendees, it logs the failure and provides a recovery option.   
4. If the administrator cancels the update operation, the system discards any changes and returns to the calendar view.   
5. If the system fails to update the event due to technical issues, it logs the error and provides a recovery option.   
6. If the event is marked as expired, the system displays a warning and may move it to a recovery record for potential restoration.   
7. If the administrator does not have permission to update the event, the system alerts them and suggests contacting a higher-level administrator for assistance.  
  
Use Case Name: Delete Event   
Use Case ID: UC-15   
Actors: Administrator, Calendar, Event, Contact, Distribution Group, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one existing calendar event.   
3. The administrator has the necessary permissions to delete calendar events.   
4. The calendar functionality is active and properly configured.   
5. The system supports the deletion of events and handling of associated data.   
  
Postconditions:   
1. The selected calendar event is deleted from the system.   
2. The calendar view is updated to reflect the deletion.   
3. Attendees are notified of the event cancellation if email notifications are enabled.   
4. A recovery record is created if the deletion is subject to retention policies.   
5. The system logs the deletion action and confirms the operation was completed.   
  
Main Flow:   
1. The administrator navigates to the "Calendar" section of the system.   
2. The system displays a list of calendar events with summary details (title, date, time, attendees).   
3. The administrator selects a specific calendar event to delete.   
4. The system confirms the deletion with a prompt to ensure the action is intentional.   
5. The administrator confirms the deletion by clicking "Delete."   
6. The system verifies the administrator's permissions and processes the deletion.   
7. The system removes the event from the calendar and updates the calendar view.   
8. If the event has attendees, the system sends a cancellation notification.   
9. The system logs the deletion action and creates a recovery record if retention policies are enabled.   
10. The system confirms the successful deletion of the calendar event.   
  
Alternative Flow:   
1. If the administrator does not confirm the deletion, the system cancels the operation and returns to the calendar view.   
2. If the system fails to delete the event due to technical issues, it logs the error and provides a recovery option.   
3. If the selected calendar event is already expired, the system displays a message and may move it to a recovery record instead of deleting it permanently.   
4. If the administrator does not have permission to delete the event, the system alerts them and suggests contacting a higher-level administrator for assistance.   
5. If the event is referenced in a distribution group or email, the system displays a warning and allows the administrator to confirm or cancel the deletion to avoid unintended data loss.  
  
Use Case Name: Manage UserContactAssociation   
Use Case ID: UC-36   
Actors: Administrator, User, Contact, UserContactAssociation, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one user account and one contact configured.   
3. The administrator has the necessary permissions to manage user-contact associations.   
4. The user-contact association functionality is active and accessible.   
5. The system supports linking users to contacts for email and calendar operations.   
  
Postconditions:   
1. The user-contact association is either created, updated, or deleted.   
2. The association status is updated in the system.   
3. A recovery record is created if the association is deleted and subject to retention policies.   
4. The system confirms the successful management of the user-contact association.   
5. The user and contact remain in the system, but their association is modified.   
  
Main Flow:   
1. The administrator navigates to the "User Contact Associations" section of the system.   
2. The system displays a list of existing user-contact associations with summary details (user name, contact name, status).   
3. The administrator selects an option to create a new association, modify an existing one, or delete an association.   
4. If creating, the administrator selects a user and a contact to associate.   
5. If modifying, the administrator selects an existing association and updates the user or contact details as needed.   
6. If deleting, the system confirms the deletion with a prompt to ensure the action is intentional.   
7. The administrator confirms the action.   
8. The system validates the selected users and contacts and processes the association change.   
9. The system updates the user-contact association list and logs the action.   
10. If the association is deleted and subject to retention policies, the system creates a recovery record.   
11. The system confirms the successful management of the user-contact association.   
  
Alternative Flow:   
1. If the administrator selects an invalid user or contact, the system displays an error and prompts for a valid selection.   
2. If the system fails to create or update the association due to technical issues, it logs the error and provides a recovery option.   
3. If the administrator does not confirm the deletion, the system cancels the operation and returns to the association list.   
4. If the selected association is already expired or marked for deletion, the system displays a message and may move it to a recovery record instead of proceeding with the action.   
5. If the administrator does not have permission to manage user-contact associations, the system alerts them and suggests contacting a higher-level administrator for assistance.   
6. If the administrator cancels the operation during the management process, the system discards any changes and returns to the association list.  
  
Use Case Name: Manage UserCalendarAssociation   
Use Case ID: UC-37   
Actors: Administrator, User, Calendar, UserCalendarAssociation, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one user account and one calendar configured.   
3. The administrator has the necessary permissions to manage user-calendar associations.   
4. The user-calendar association functionality is active and accessible.   
5. The system supports linking users to calendars for event access and management.   
  
Postconditions:   
1. The user-calendar association is either created, updated, or deleted.   
2. The association status is updated in the system.   
3. A recovery record is created if the association is deleted and subject to retention policies.   
4. The system confirms the successful management of the user-calendar association.   
5. The user and calendar remain in the system, but their association is modified.   
  
Main Flow:   
1. The administrator navigates to the "User Calendar Associations" section of the system.   
2. The system displays a list of existing user-calendar associations with summary details (user name, calendar name, access level, status).   
3. The administrator selects an option to create a new association, modify an existing one, or delete an association.   
4. If creating, the administrator selects a user and a calendar to associate, and specifies the access level (e.g., view-only, edit).   
5. If modifying, the administrator selects an existing association and updates the access level or calendar details as needed.   
6. If deleting, the system confirms the deletion with a prompt to ensure the action is intentional.   
7. The administrator confirms the action.   
8. The system validates the selected users and calendars and processes the association change.   
9. The system updates the user-calendar association list and logs the action.   
10. If the association is deleted and subject to retention policies, the system creates a recovery record.   
11. The system confirms the successful management of the user-calendar association.   
  
Alternative Flow:   
1. If the administrator selects an invalid user or calendar, the system displays an error and prompts for a valid selection.   
2. If the system fails to create or update the association due to technical issues, it logs the error and provides a recovery option.   
3. If the administrator does not confirm the deletion, the system cancels the operation and returns to the association list.   
4. If the selected association is already expired or marked for deletion, the system displays a message and may move it to a recovery record instead of proceeding with the action.   
5. If the administrator does not have permission to manage user-calendar associations, the system alerts them and suggests contacting a higher-level administrator for assistance.   
6. If the administrator cancels the operation during the management process, the system discards any changes and returns to the association list.  
  
Use Case Name: Manage UserEmailAccountAssociation   
Use Case ID: UC-38   
Actors: Administrator, User, Email Account, UserEmailAccountAssociation, Recovery Record   
  
Preconditions:   
1. The administrator is logged into the system.   
2. The system has at least one user account and one email account configured.   
3. The administrator has the necessary permissions to manage user-email account associations.   
4. The user-email account association functionality is active and accessible.   
5. The system supports linking users to email accounts for access and management of emails.   
  
Postconditions:   
1. The user-email account association is either created, updated, or deleted.   
2. The association status is updated in the system.   
3. A recovery record is created if the association is deleted and subject to retention policies.   
4. The system confirms the successful management of the user-email account association.   
5. The user and email account remain in the system, but their association is modified.   
  
Main Flow:   
1. The administrator navigates to the "User Email Account Associations" section of the system.   
2. The system displays a list of existing user-email account associations with summary details (user name, email account, access level, status).   
3. The administrator selects an option to create a new association, modify an existing one, or delete an association.   
4. If creating, the administrator selects a user and an email account to associate, and specifies the access level (e.g., send/receive, view-only).   
5. If modifying, the administrator selects an existing association and updates the access level or email account details as needed.   
6. If deleting, the system confirms the deletion with a prompt to ensure the action is intentional.   
7. The administrator confirms the action.   
8. The system validates the selected users and email accounts and processes the association change.   
9. The system updates the user-email account association list and logs the action.   
10. If the association is deleted and subject to retention policies, the system creates a recovery record.   
11. The system confirms the successful management of the user-email account association.   
  
Alternative Flow:   
1. If the administrator selects an invalid user or email account, the system displays an error and prompts for a valid selection.   
2. If the system fails to create or update the association due to technical issues, it logs the error and provides a recovery option.   
3. If the administrator does not confirm the deletion, the system cancels the operation and returns to the association list.   
4. If the selected association is already expired or marked for deletion, the system displays a message and may move it to a recovery record instead of proceeding with the action.   
5. If the administrator does not have permission to manage user-email account associations, the system alerts them and suggests contacting a higher-level administrator for assistance.   
6. If the administrator cancels the operation during the management process, the system discards any changes and returns to the association list.