Eagle Watch Start Guide

Welcome to the Eagle Watch Start Guide. This guide provides the fundamental instructions needed to navigate our Agentic AI OSINT platform, manage collaborative investigations, and understand the search intelligence categories.

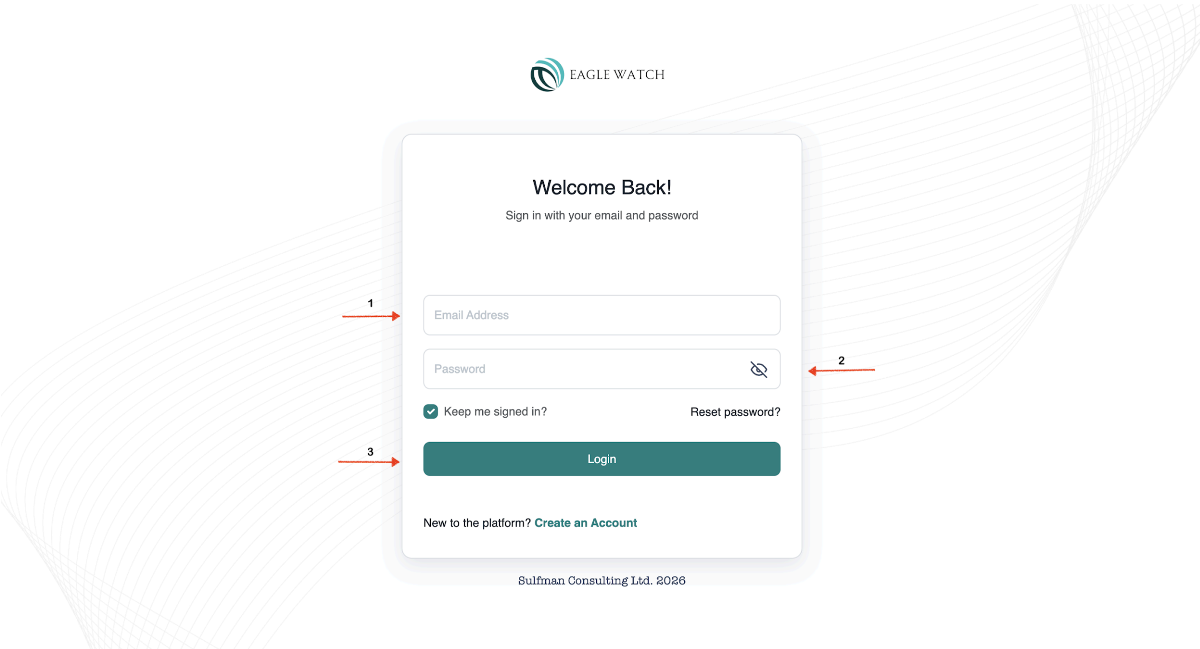
1. Case Management

All intelligence gathering on Eagle Watch begins within a **Case**. Cases serve as secure containers that keep your search results, watchlists, and vision boards organized and siloed for reference.

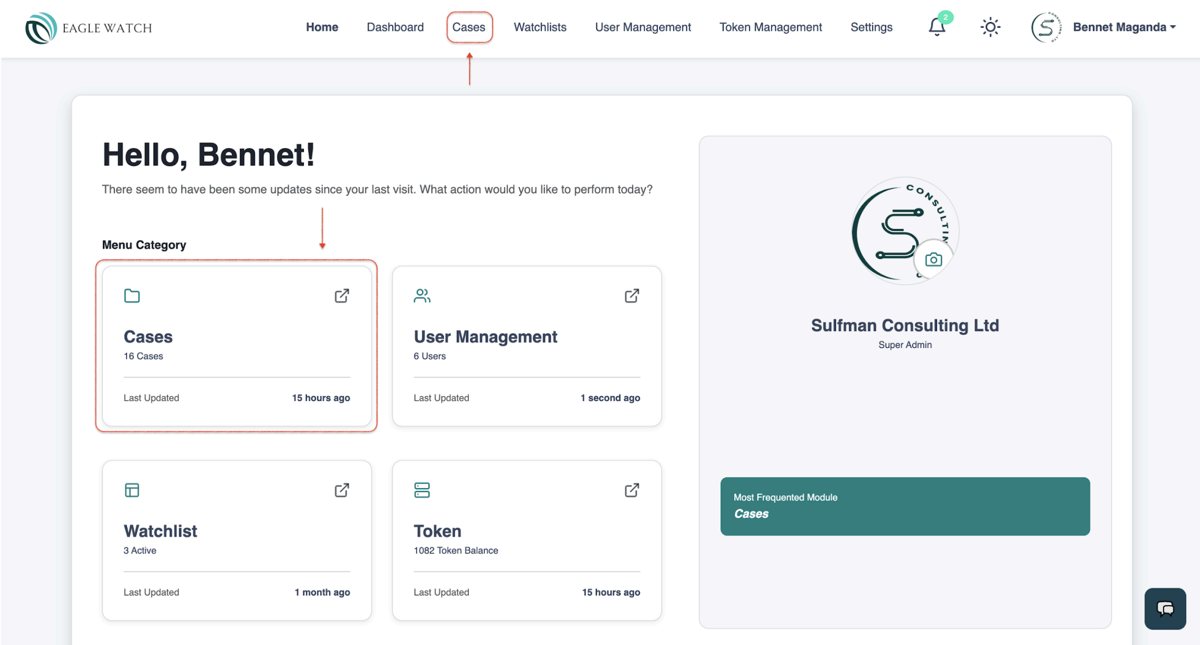
Creating a Case

To start a new investigation, you must first create a Case environment.

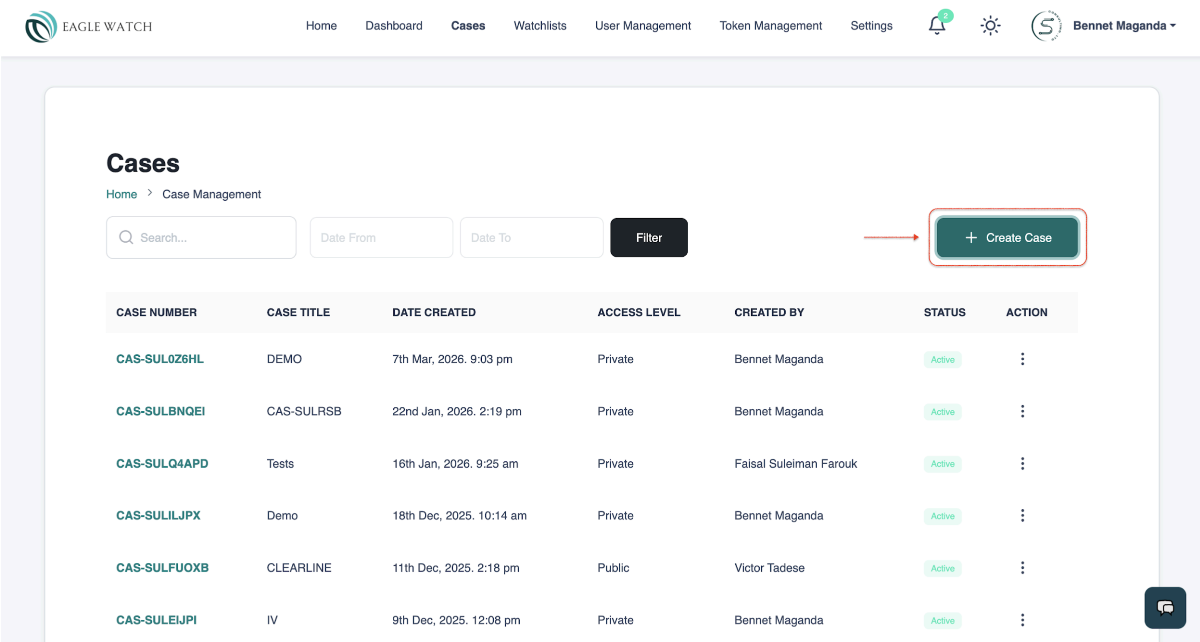
1. **Login:** Access the platform using your authorized credentials.



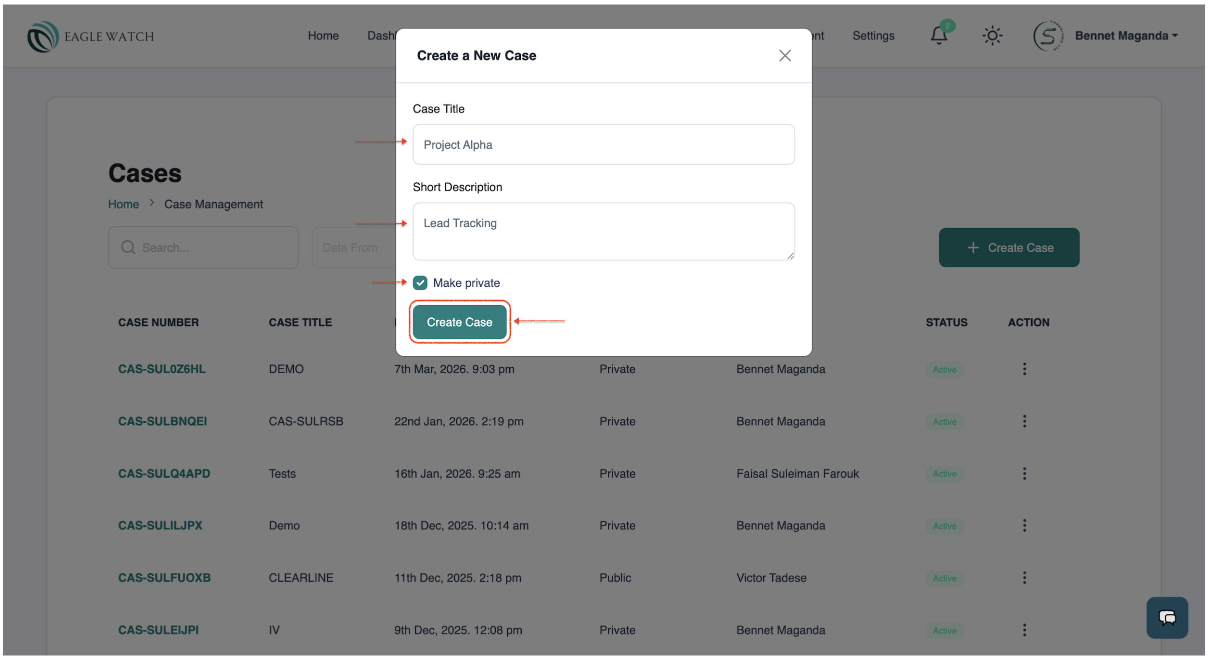
2. **Navigate:** Click on the **Cases** tab in the top navigation bar or the **Cases** card on the main dashboard.



3. **Initialize:** Click the **Create Case** button.



4. **Define:** In the pop-up modal, enter a **Case Title** (e.g., *Project Alpha - Lead Tracking*) and a **Short Description** of the case, and set access level (Private or Public).



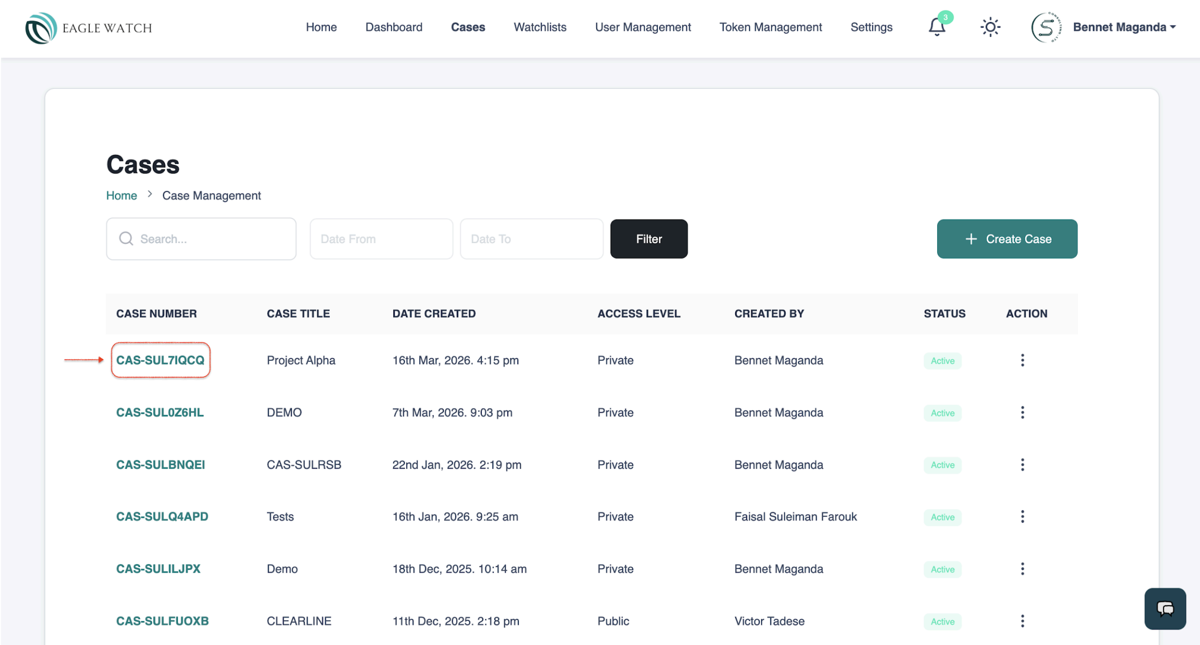
5. **Finalize:** Click **Create Case**.

- **Best Practice:** Use specific naming conventions for Case Titles to make them easily searchable as your investigative library grows.
- **Best Practice:** Use **Public Access** for team-led investigations to share intelligence, or **Private Access** for sensitive missions to keep searches hidden from other teammates.

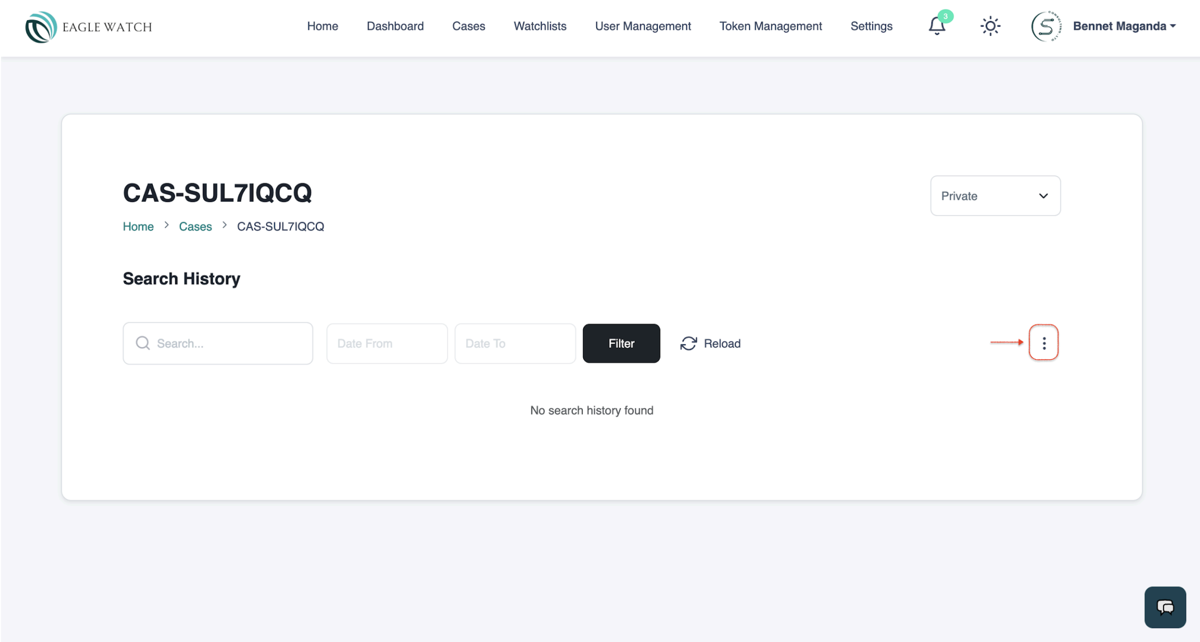
Collaborative Investigations (Sharing & Permissions)

Eagle Watch is built for teamwork, allowing you to securely share intelligence across your organization.

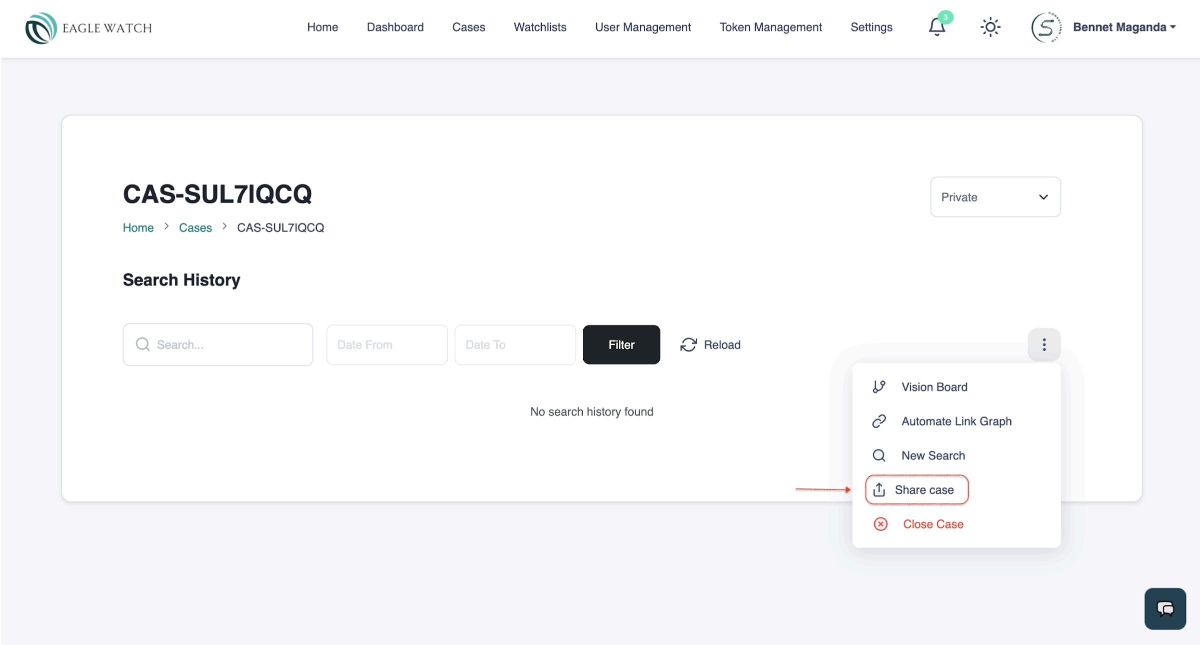
1. **Open Case:** Navigate to your Cases and click on the specific case you wish to share.



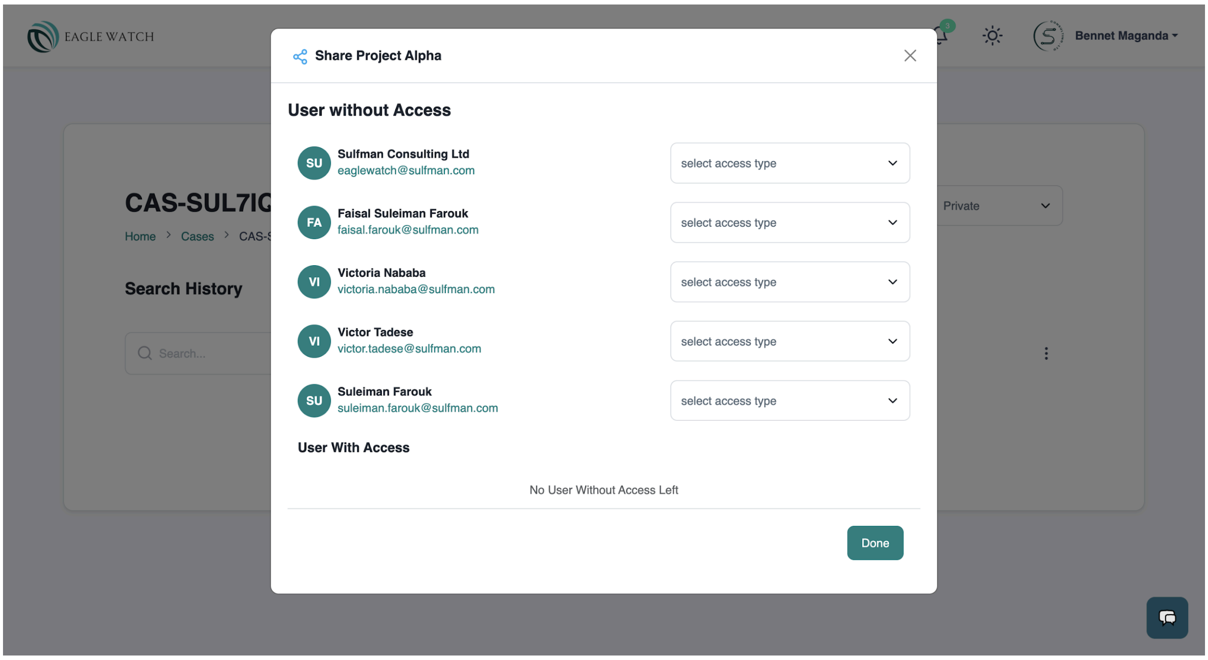
2. **Access Menu:** Click the **Three-Dot Menu (Kebab)** on the right-hand side.



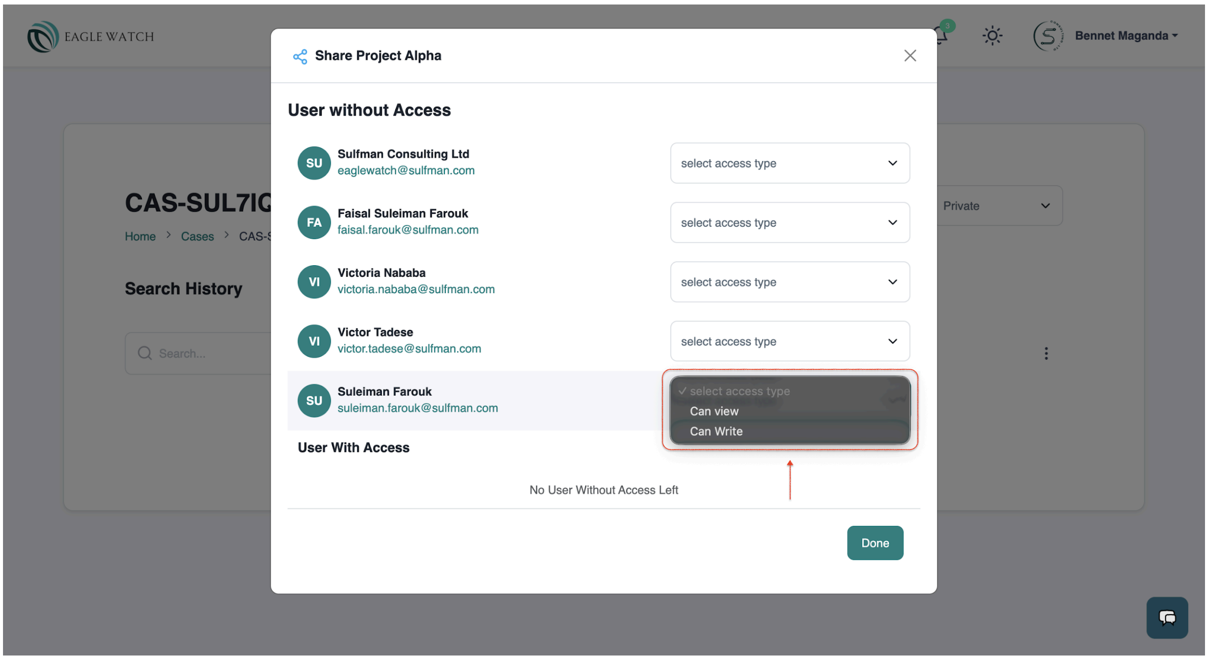
3. **Select Share:** Choose **Share Case** from the dropdown menu.



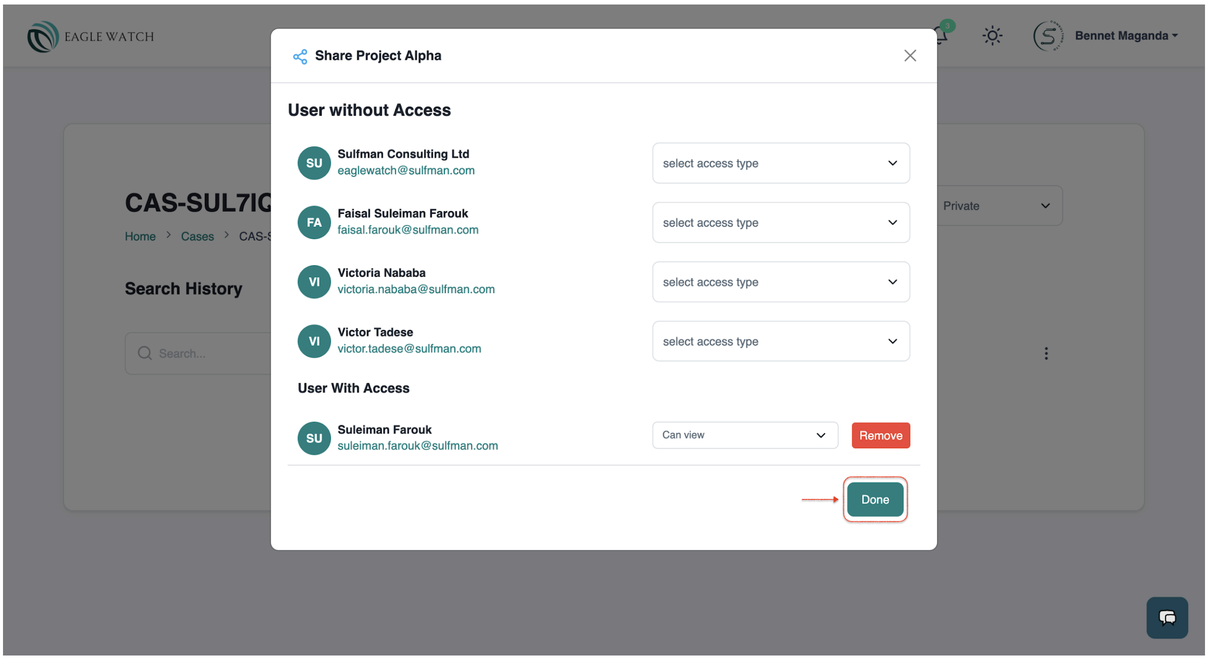
4. **Assign Users:** Select the team members you wish to invite to the investigation.



5. **Set Permissions:**
    a. **View:** Allows the user to view results and the interactive vision board.
    b. **Write:** Allows the user to initiate new searches and add entities to the watchlist.

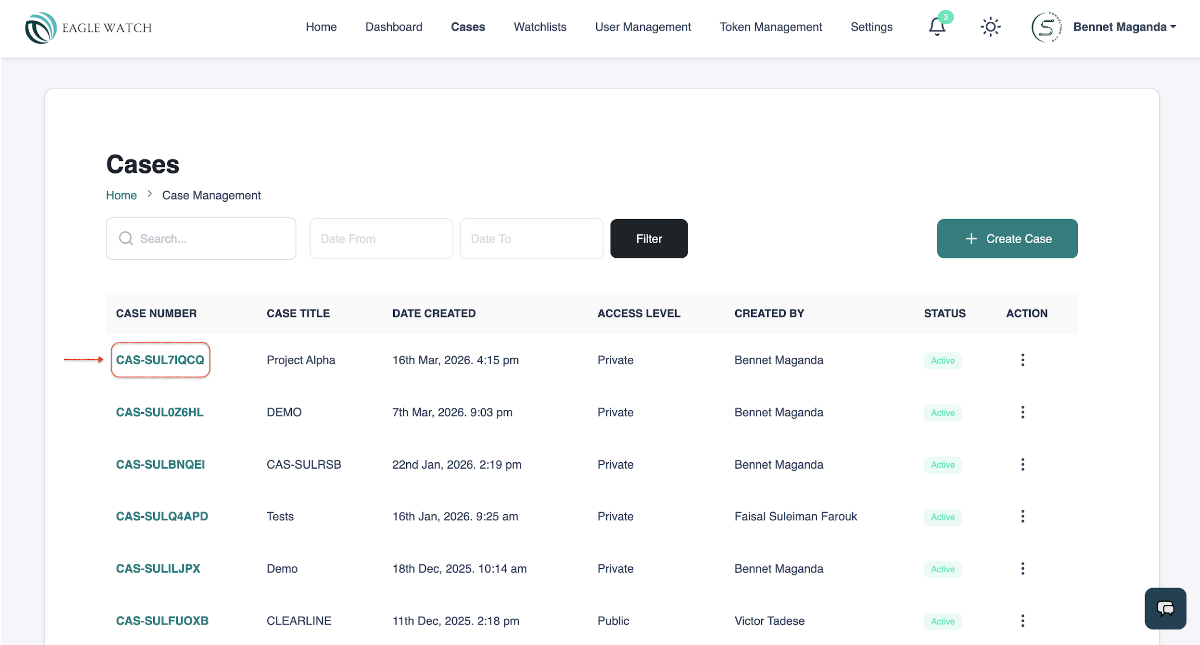


6. **Save:** Click **Done** to grant access.

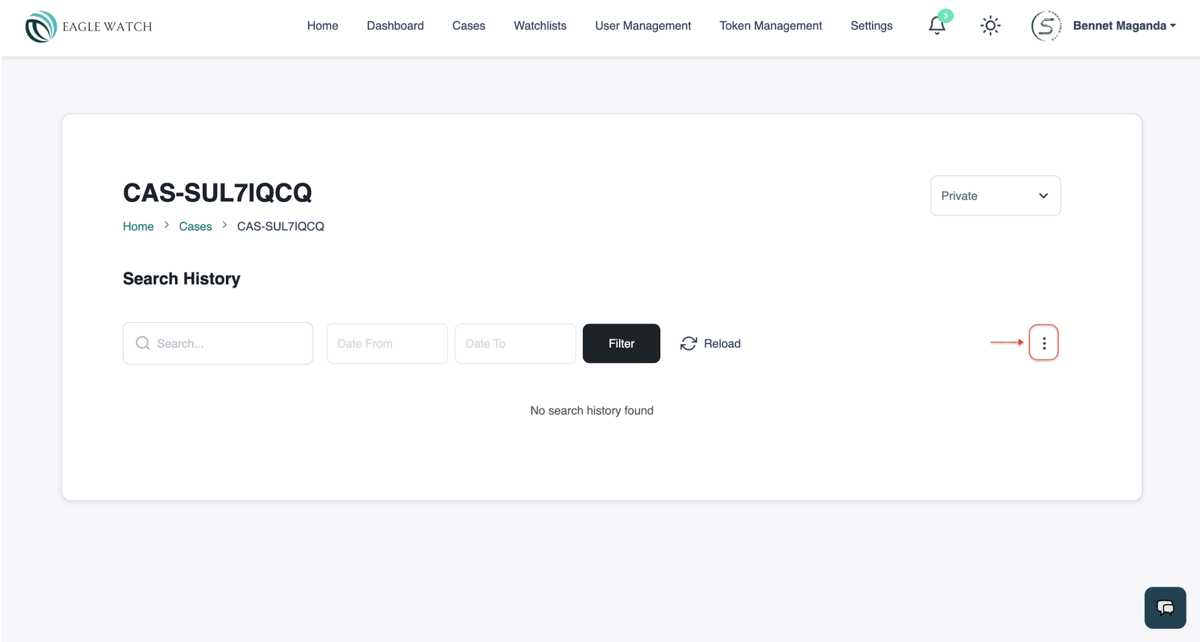


Closing a Case

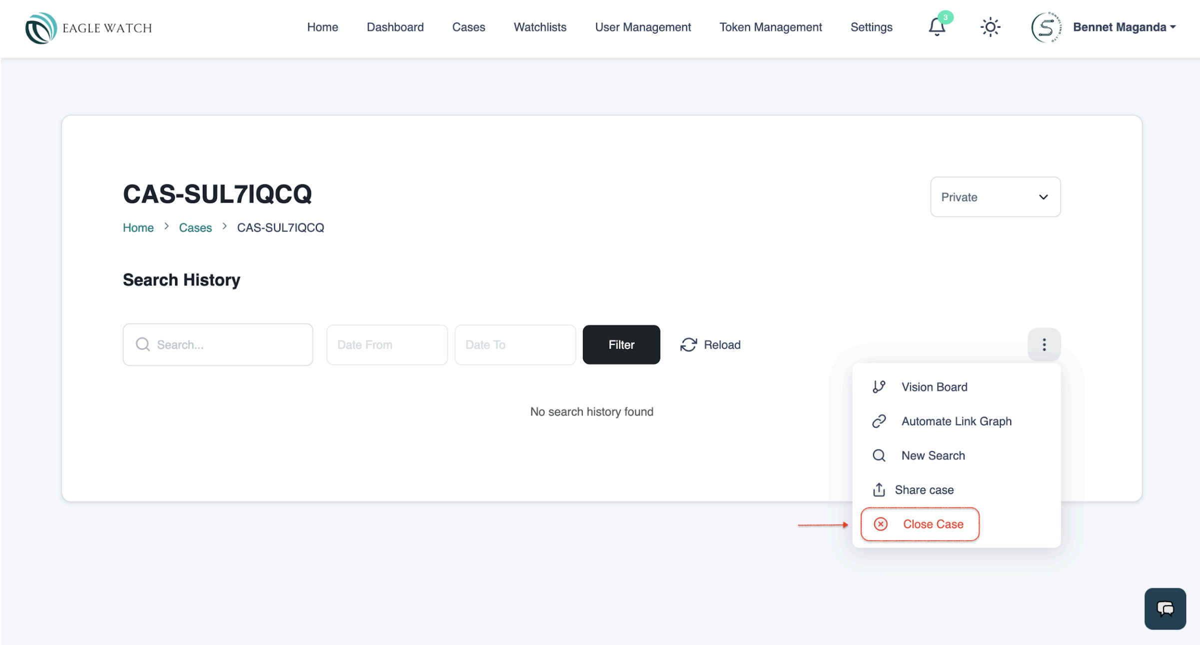
1. **Open Case:** Navigate to your Cases and click on the specific case you wish to close.



2. **Access Menu:** Click the **Three-Dot Menu (Kebab)** on the right-hand side.



3. **Closing a Case:** Once an investigation is finalized, select **Close Case** to archive the data.



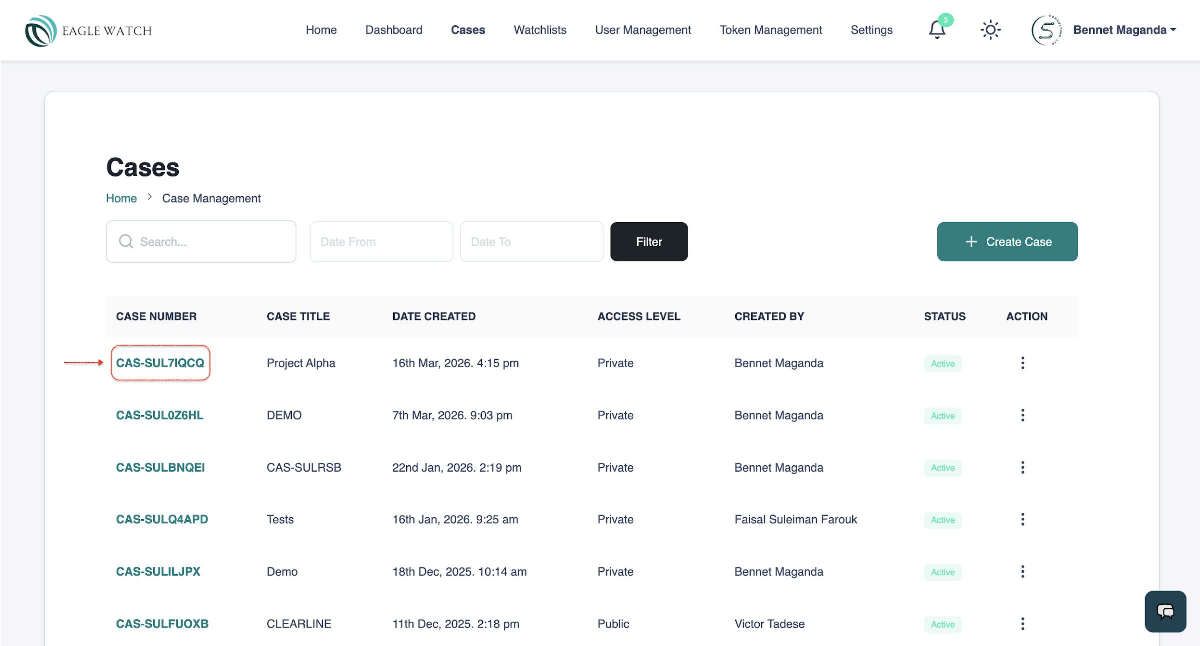
2. Intelligence Categories

Our specialized agents are designed to handle complex queries across different data domains.

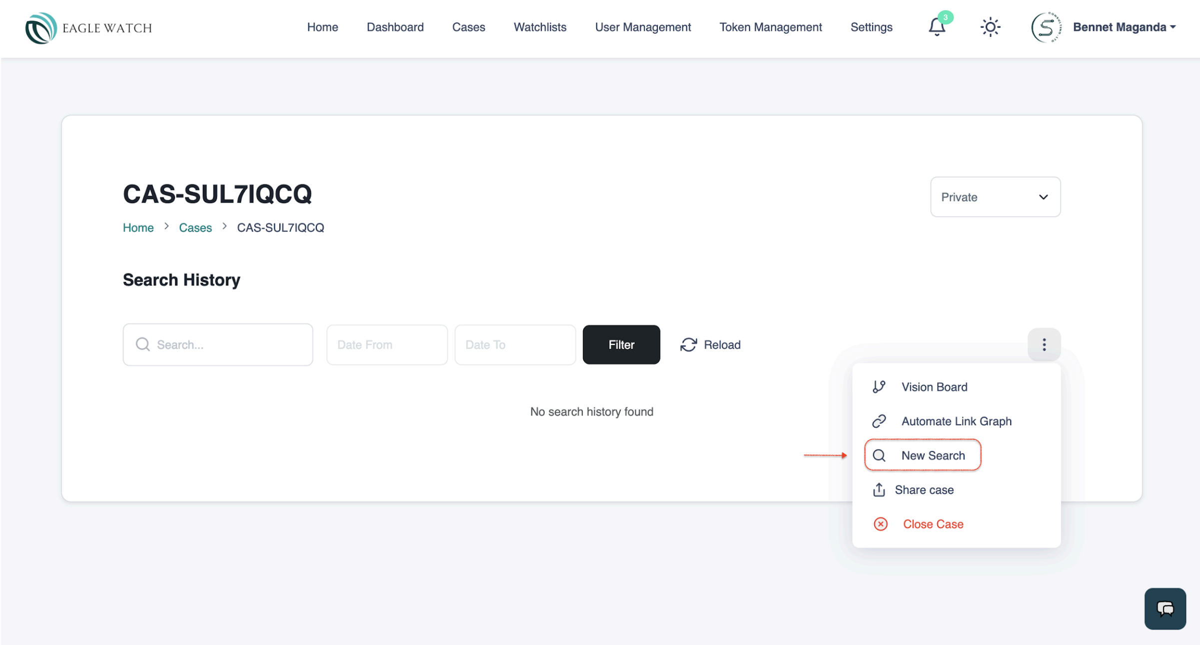
Performing a New Search

Once a case is active, you can deploy agents to gather intelligence.

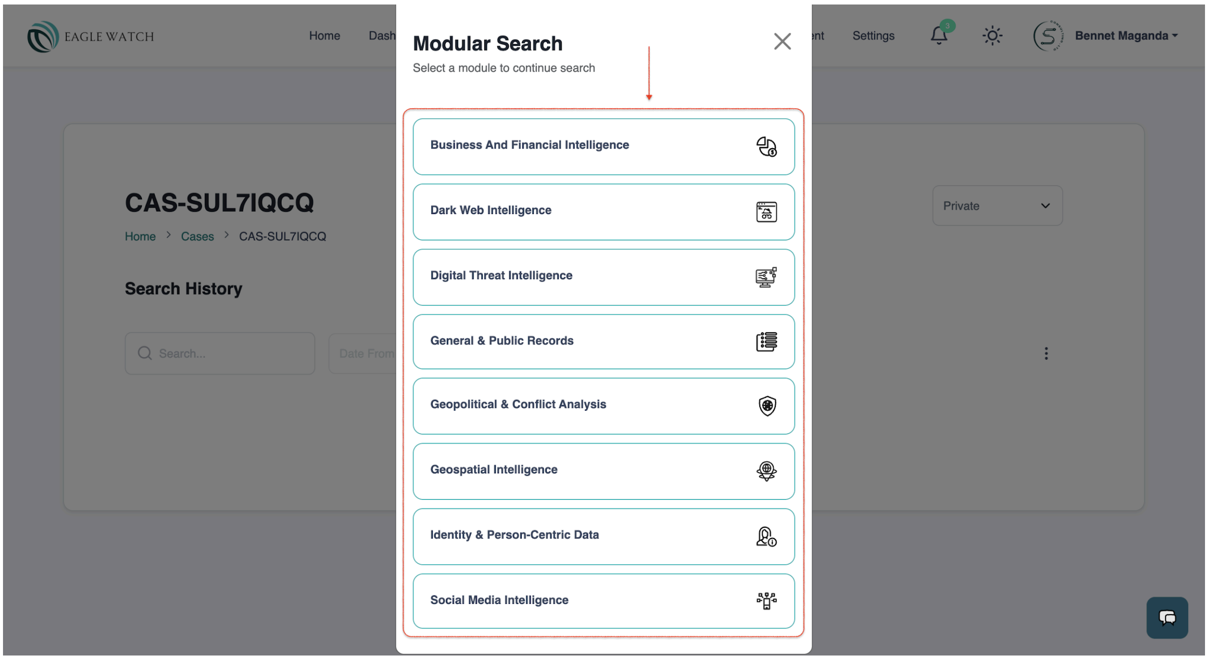
1. **Enter Case:** Open the relevant case from your dashboard.



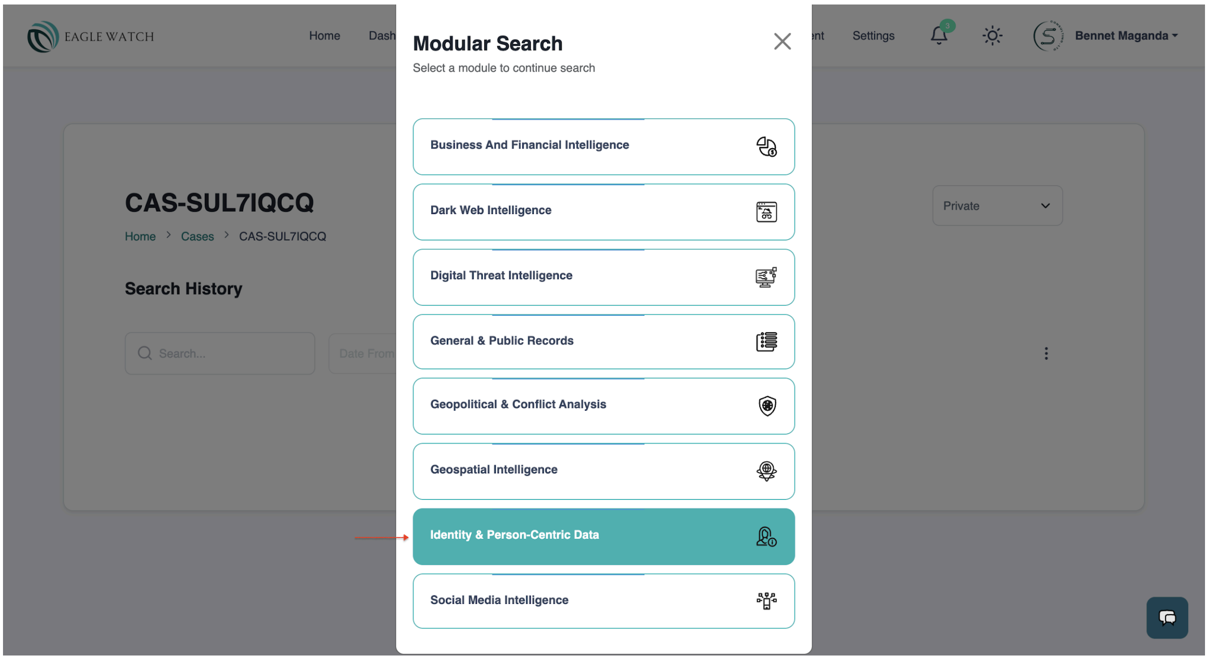
2. **Initiate Search:** Click the **Three-Dot Menu** and select **New Search**.



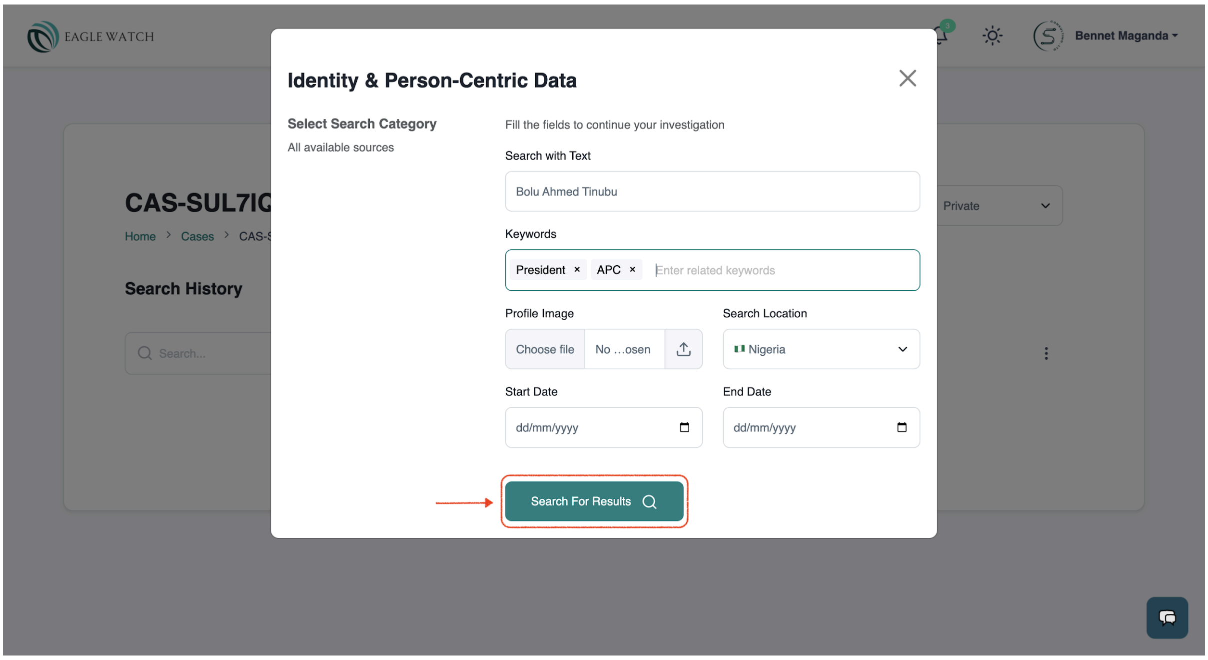
3. **Category Selection:** A modal pop-up will appear displaying the available intelligence categories.



4. **Choose a Category:** Select the primary category that fits your current objective (e.g., *Identity & Person-Centric Data*).



5. **Execute:** Fill in the search parameters and click **Search For Results**.



5. Client Onboarding

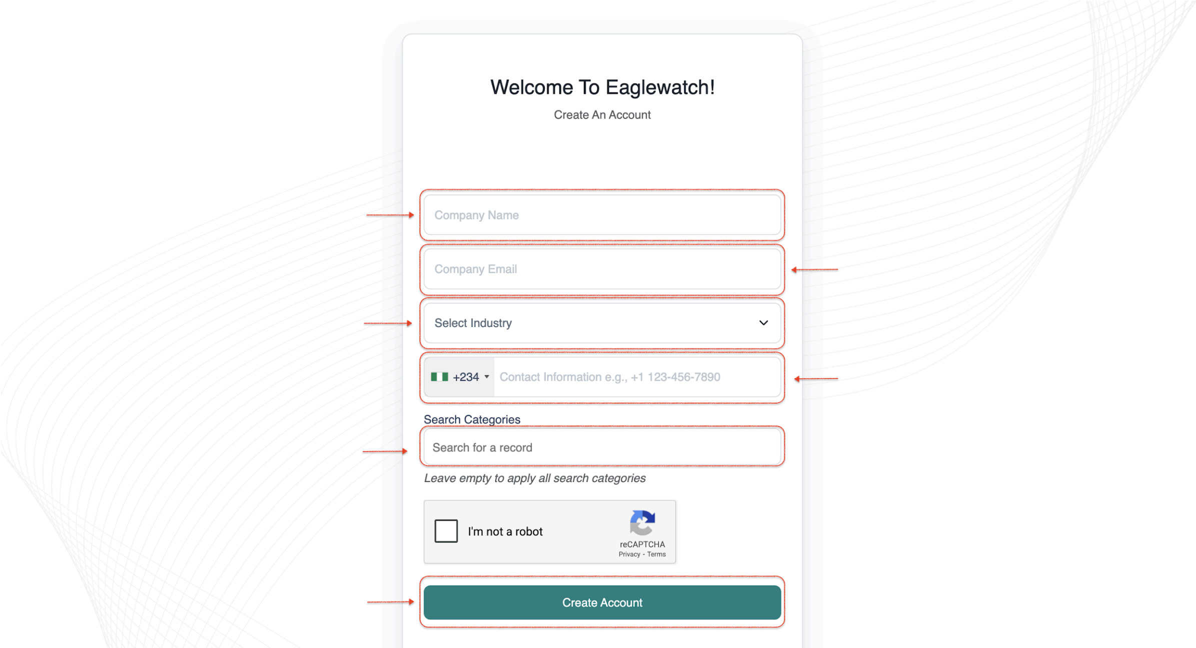
Eagle Watch supports two primary onboarding paths: **Self-Registration** and **Direct Onboarding**.

Self-Registration Flow

This path is for new organizations joining the platform.

1. **Navigate to Registration:** Visit the [Eagle Watch Registration Page].

2. **Input Details:** Provide your **Company Name**, **Company Email**, **Industry**, and **Contact Information** (including country code).



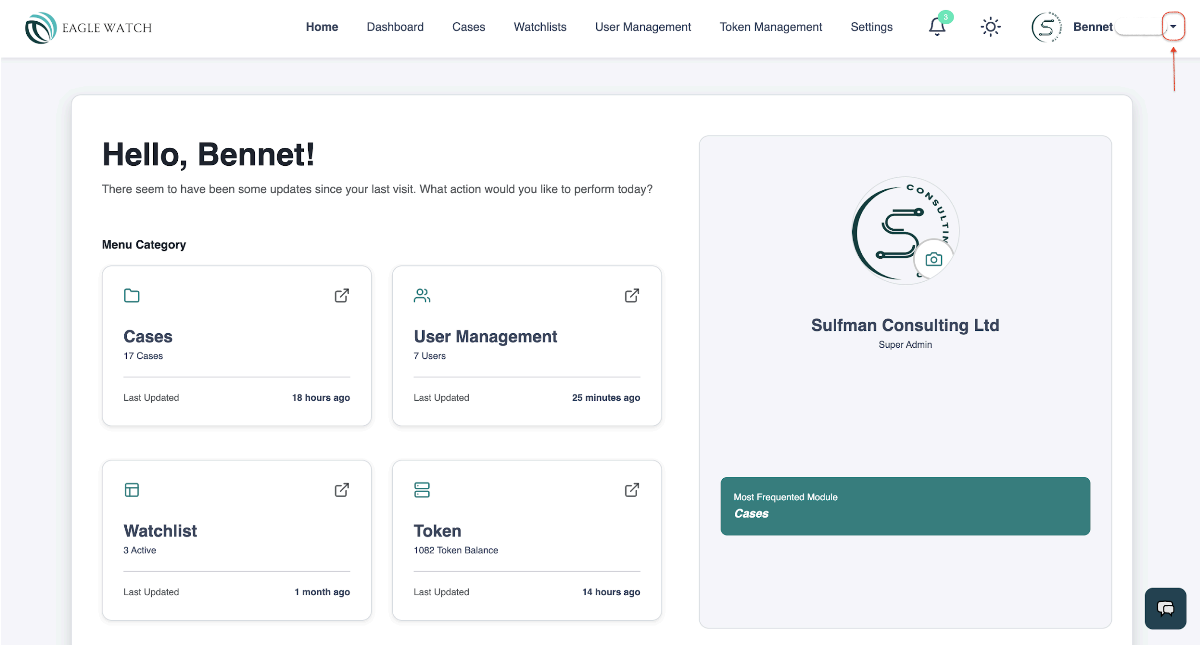
3. **Select Categories:** Choose the intelligence modules (Social, Dark Web, etc.) relevant to your organization. The client can choose either some or all categories.
4. **Submit:** Click **Create Account**.

6. Admin Account Management

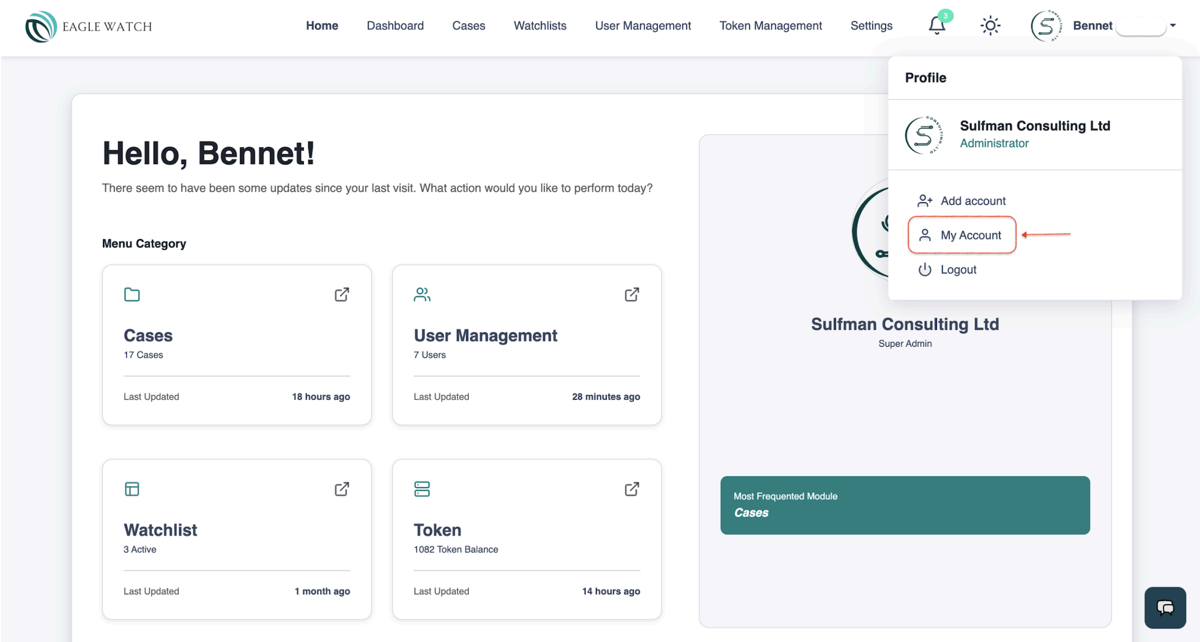
Administrators can monitor their account activity and review platform interactions through the **My Account** section.

Managing Account Activities

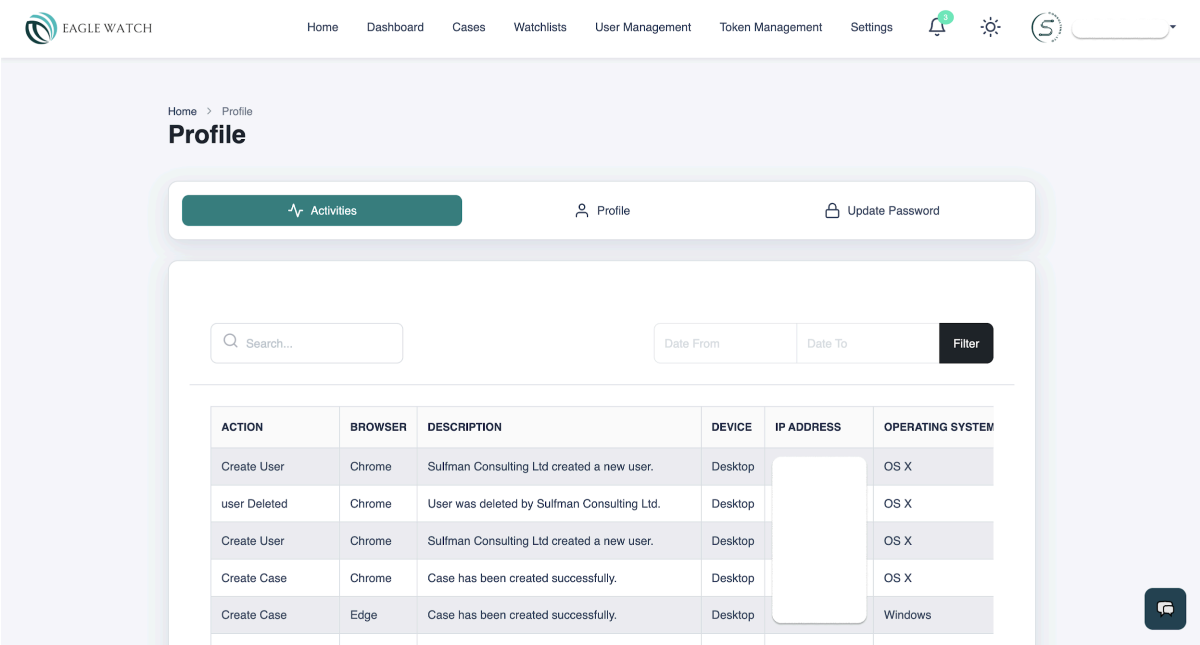
1. **Navigate:** Go to the top-right corner of any page.
2. **Initialize:** Click on your **profile icon** to open the account menu.



3. **Access Account:** Select **My Account** from the dropdown options.



4. **View Activities:** Review your recent activities, including actions performed within the platform.



5. **Finalize:** Confirm that all actions and logs reflect your recent interactions accurately.

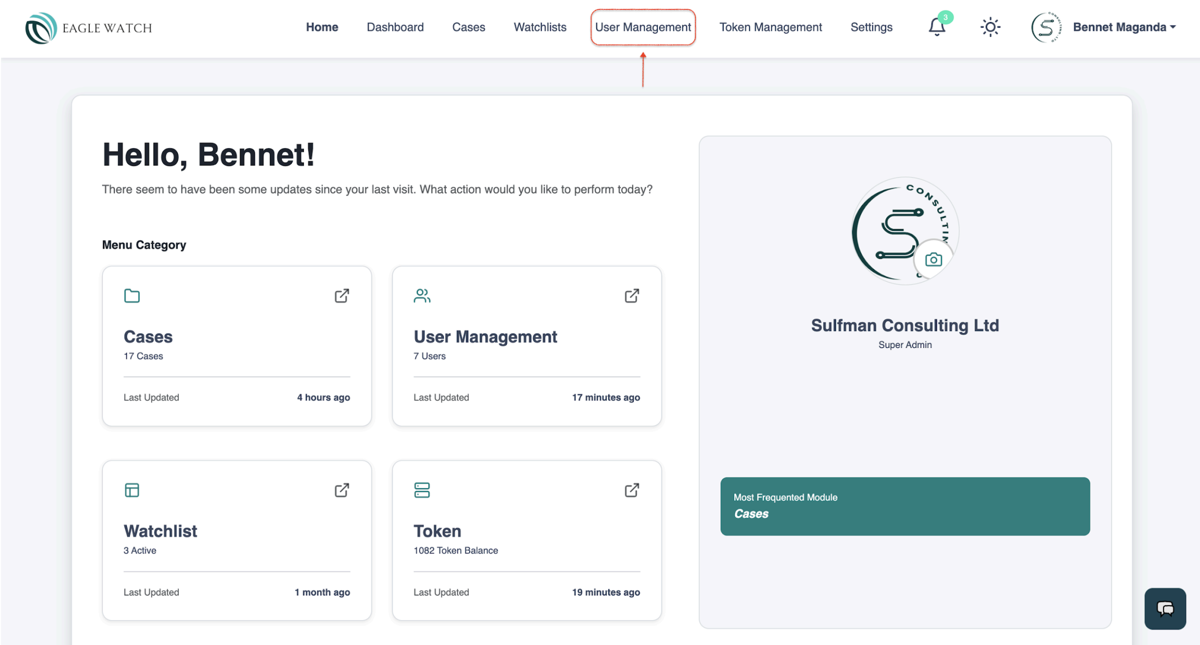
Best Practice: Regularly review your account activity to ensure all actions are authorized and to quickly identify any unusual behavior.

7. User Management

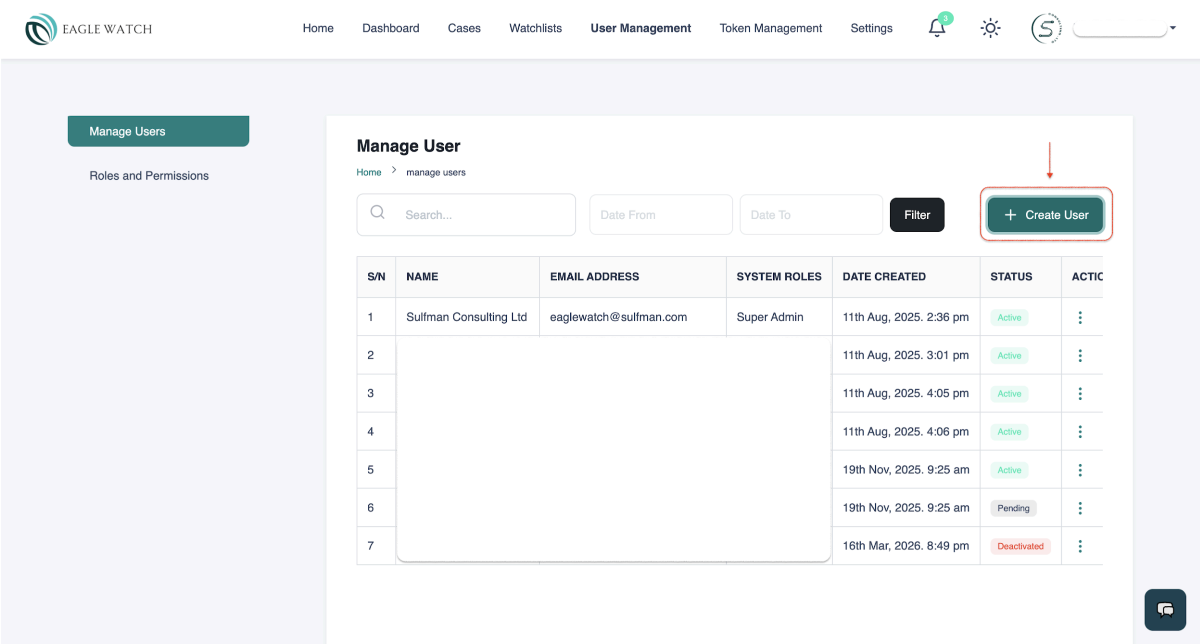
Administrators manage access levels and platform behaviour through three distinct control layers.

Managing Users – Creating a User

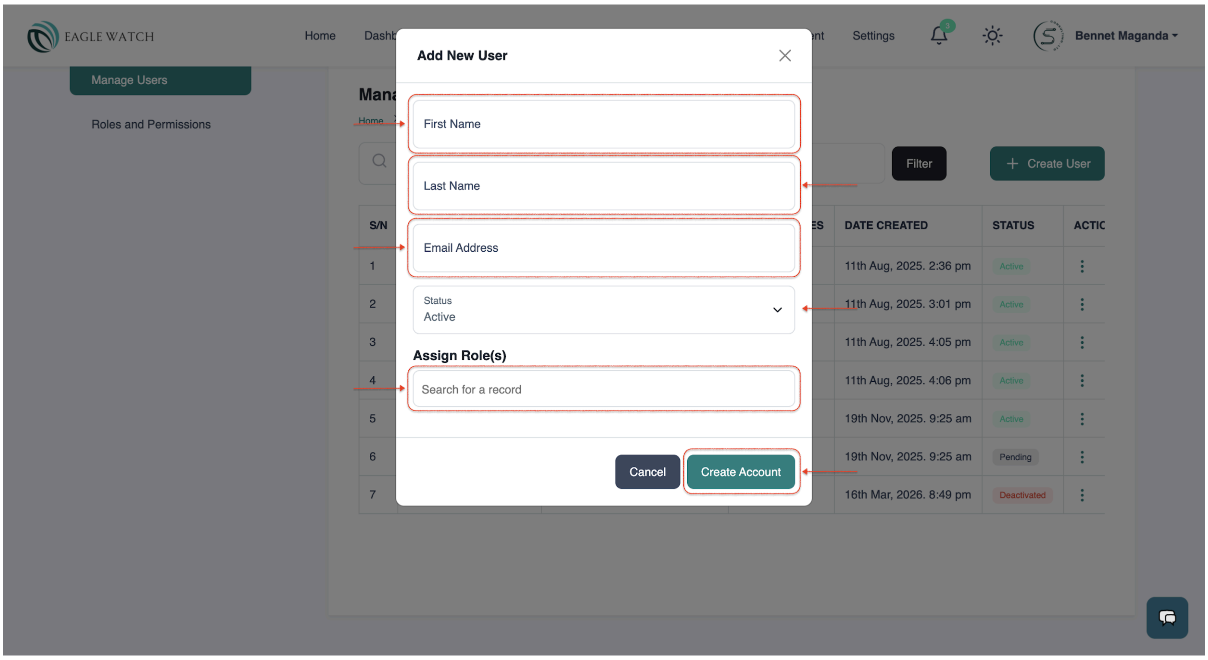
1. **Login:** Enter your credentials at the Eagle Watch Login Portal.
2. **Navigate:** Select **User Management** from the administration panel.



3. **Initialize:** Locate the **Create User** button.



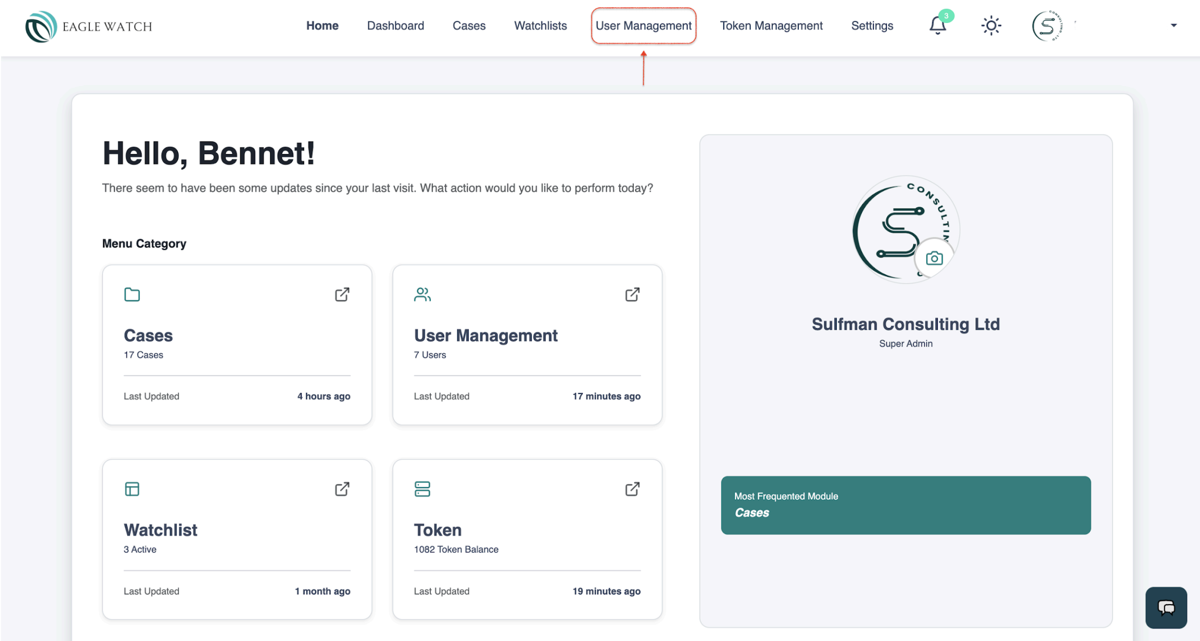
4. **Input Details:** Fill in the necessary user information.



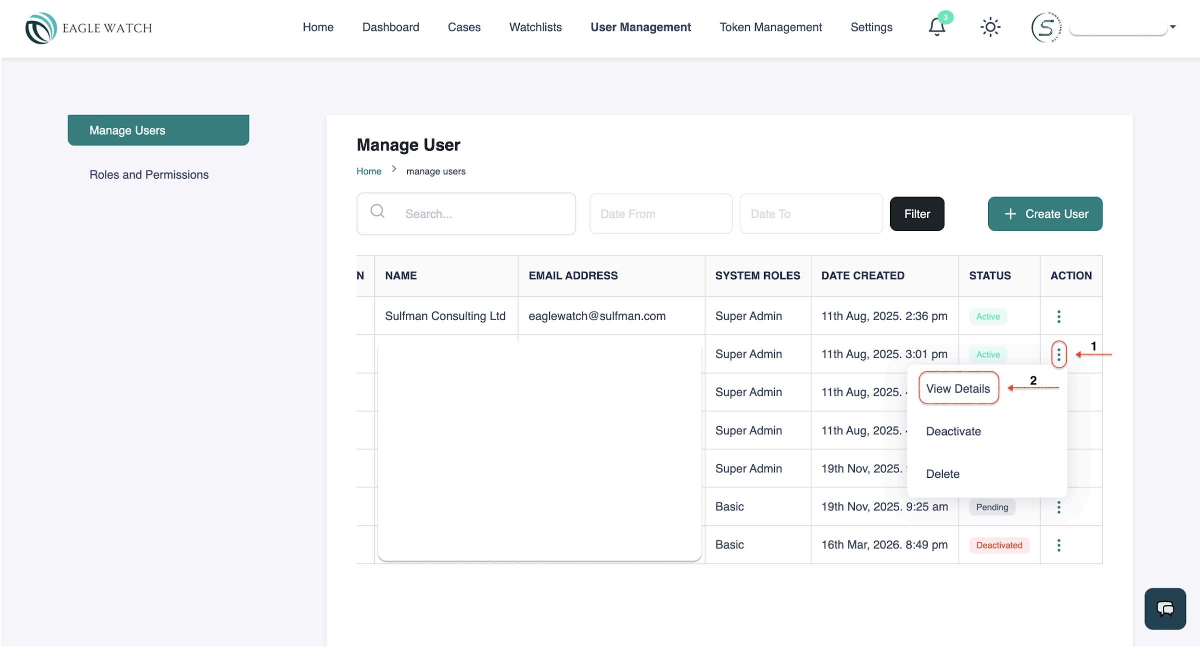
5. **Submit:** Click **Create Account**.

Managing Users - Viewing User Details

1. **Navigate:** Select **User Management** from the administration panel.

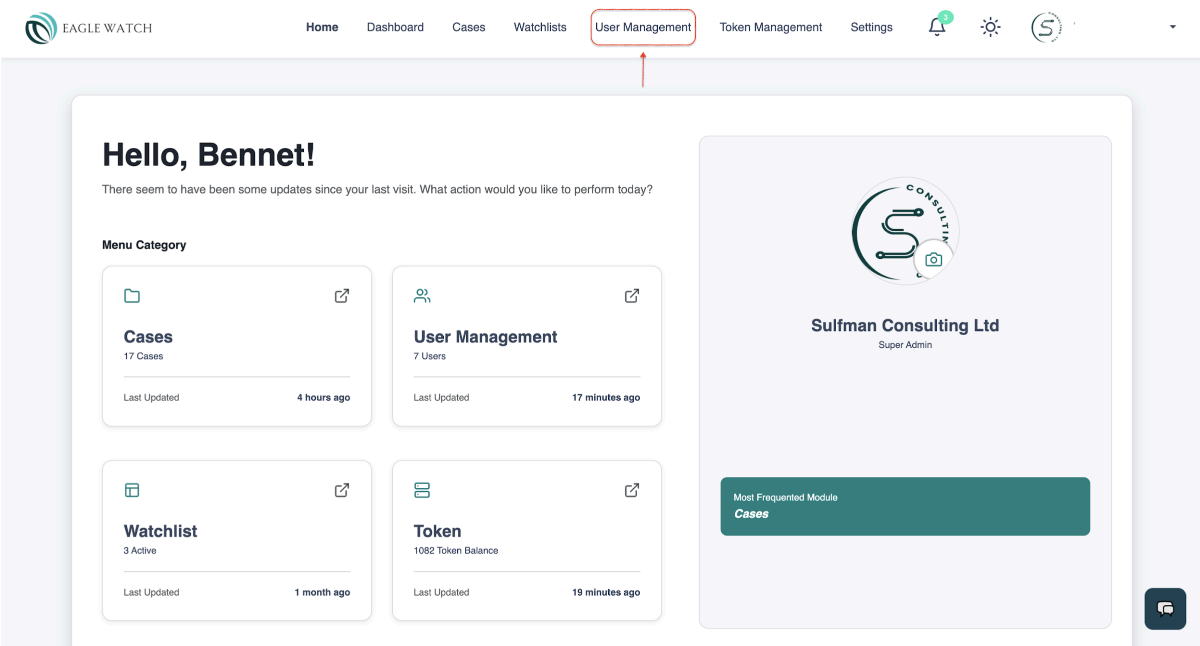


2. **Initialize:** Click the **Three-Dot Menu (Kebab)** on the right-hand side of the profile to view role assignments and account status.

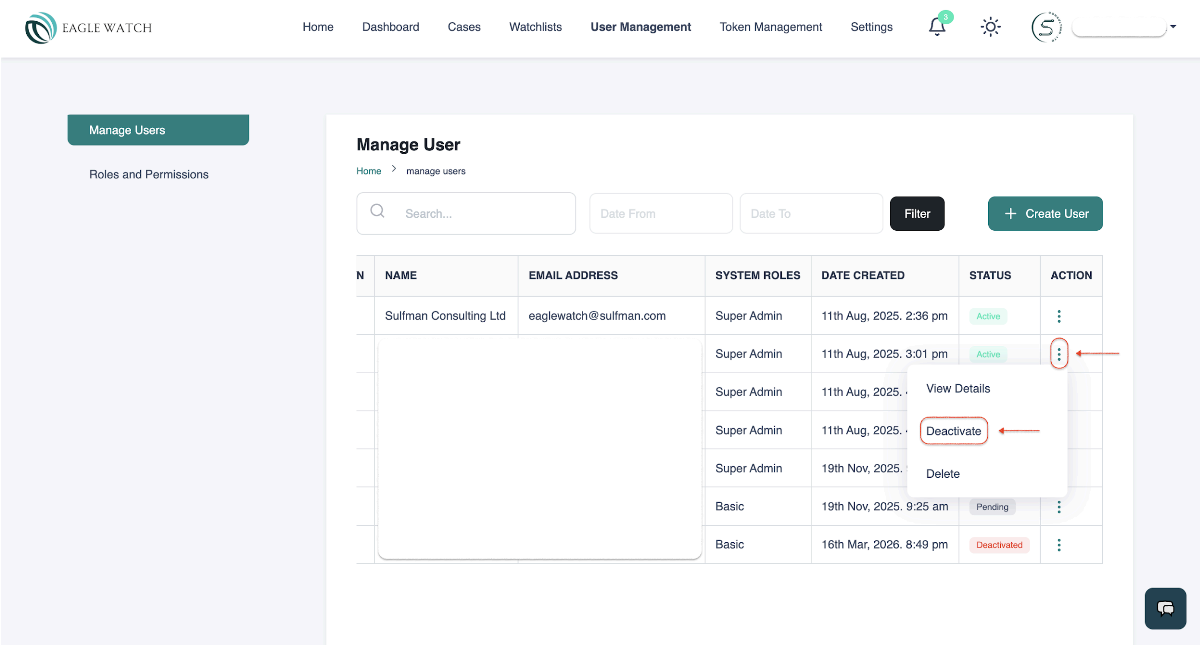


Managing Users – Deactivating a User

1. **Navigate:** Select **User Management** from the administration panel.

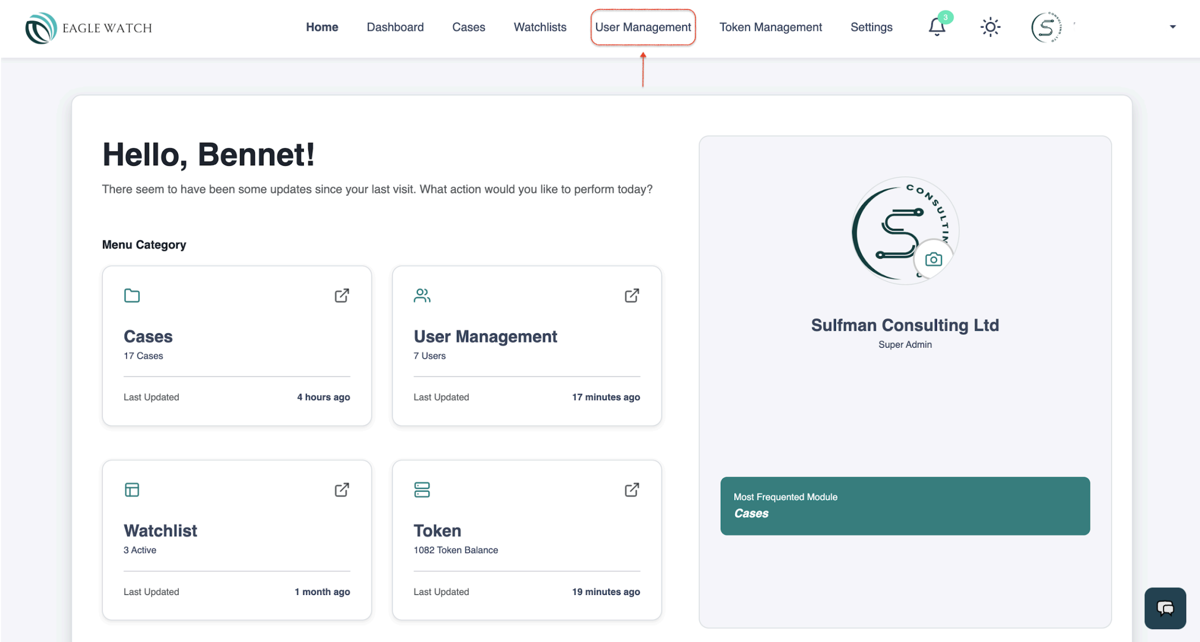


2. **Initialize:** Click the **Three-Dot Menu (Kebab)** on the right-hand side of the profile to deactivate the user account.

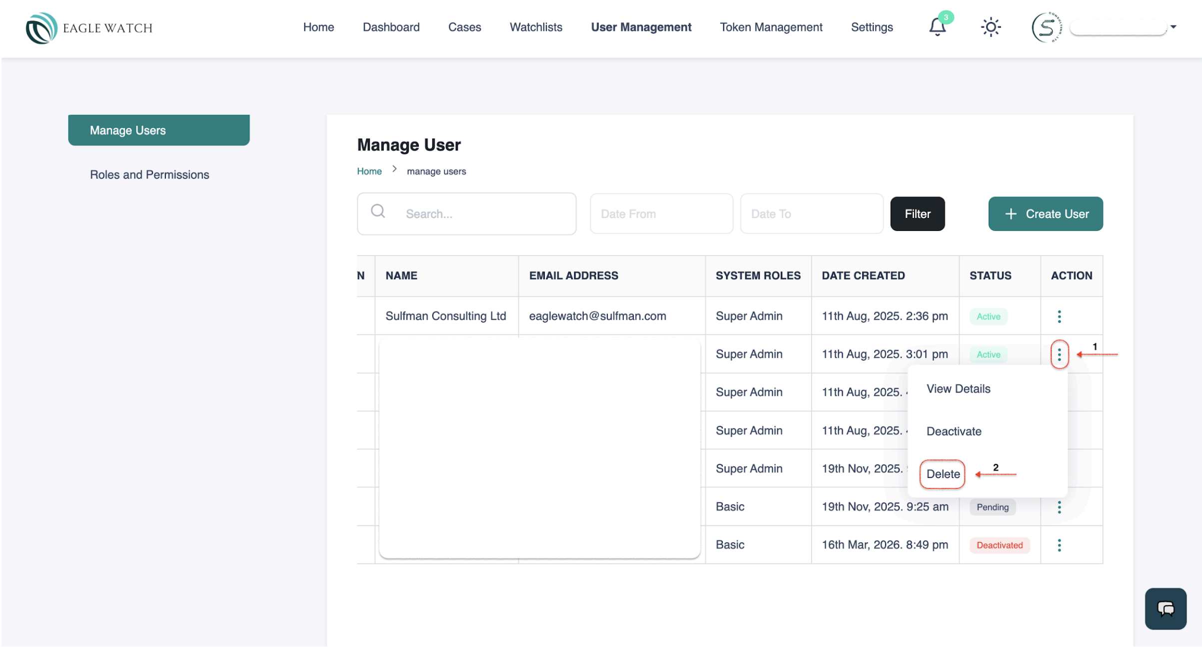


Managing Users – Deleting a User

1. **Navigate:** Select **User Management** from the administration panel.



2. **Initialize:** Click the **Three-Dot Menu (Kebab)** on the right-hand side of the profile to delete the user account.



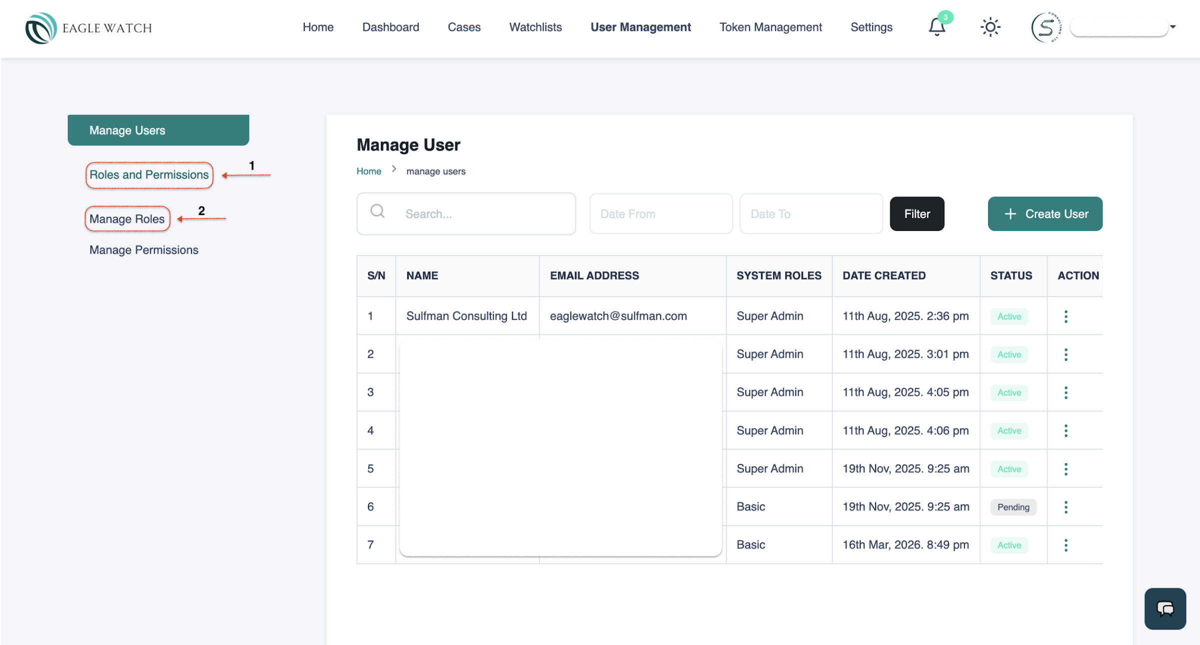
Best Practice:

- Periodically review user roles to ensure access aligns with current responsibilities.
- Deactivate users during internal reviews, role transitions, or temporary leave periods.
- Only delete user accounts that are no longer required for operational or audit purposes.
- Deleting a user deletes all their cases and search histories.

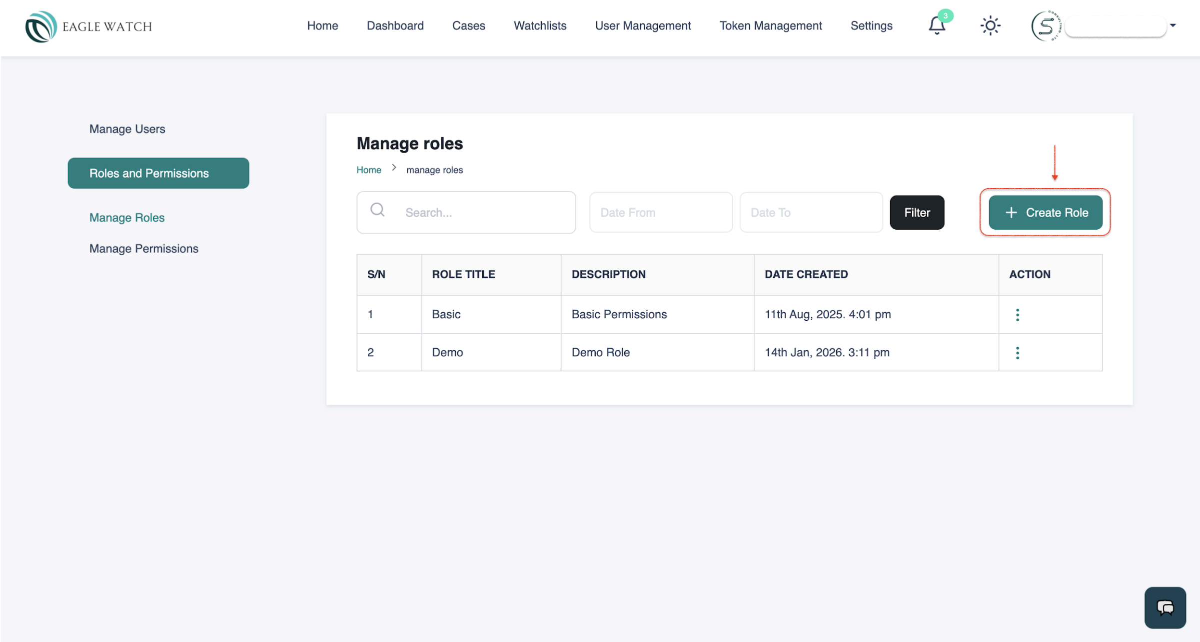
Roles Management - Creating a Role

Roles act as templates for access control.

1. **Navigate:** Select **Roles and Permission** from the User Management Tab.

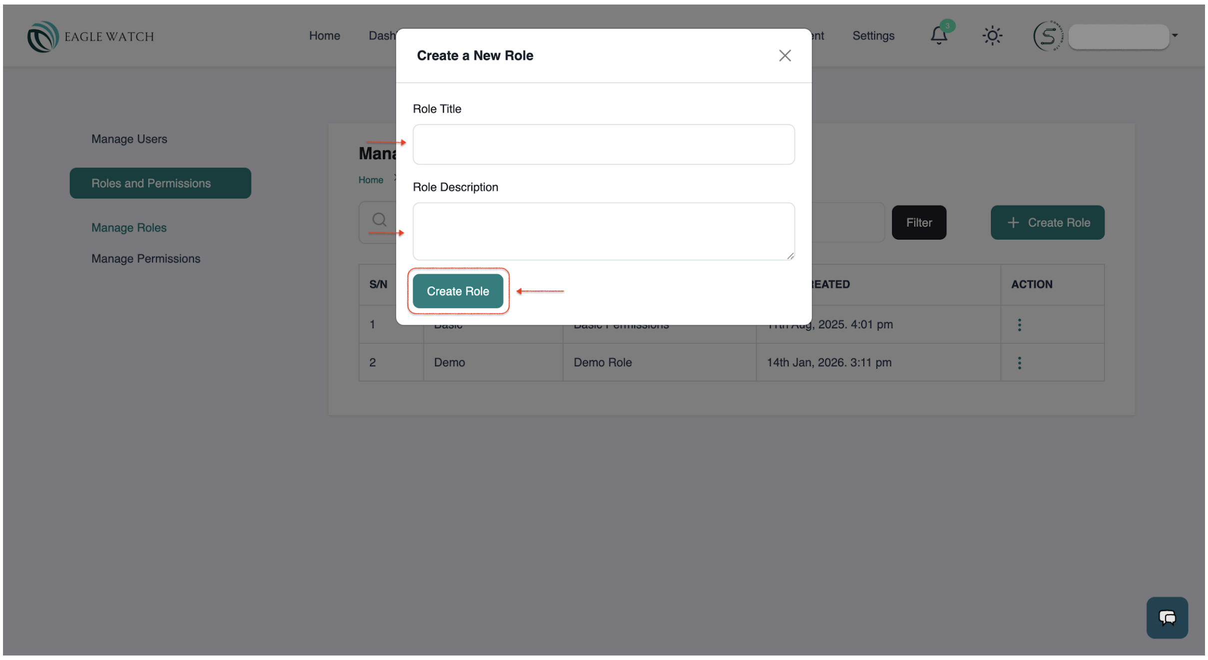


2. **Initialize:** Click the **Create Role** button.



   a. **Define Role:**
      i. Enter a **Role Title** (e.g., *Senior Lead* or *Junior Analyst*).
      ii. Add a **Role Description** outlining the responsibilities and intended access scope.

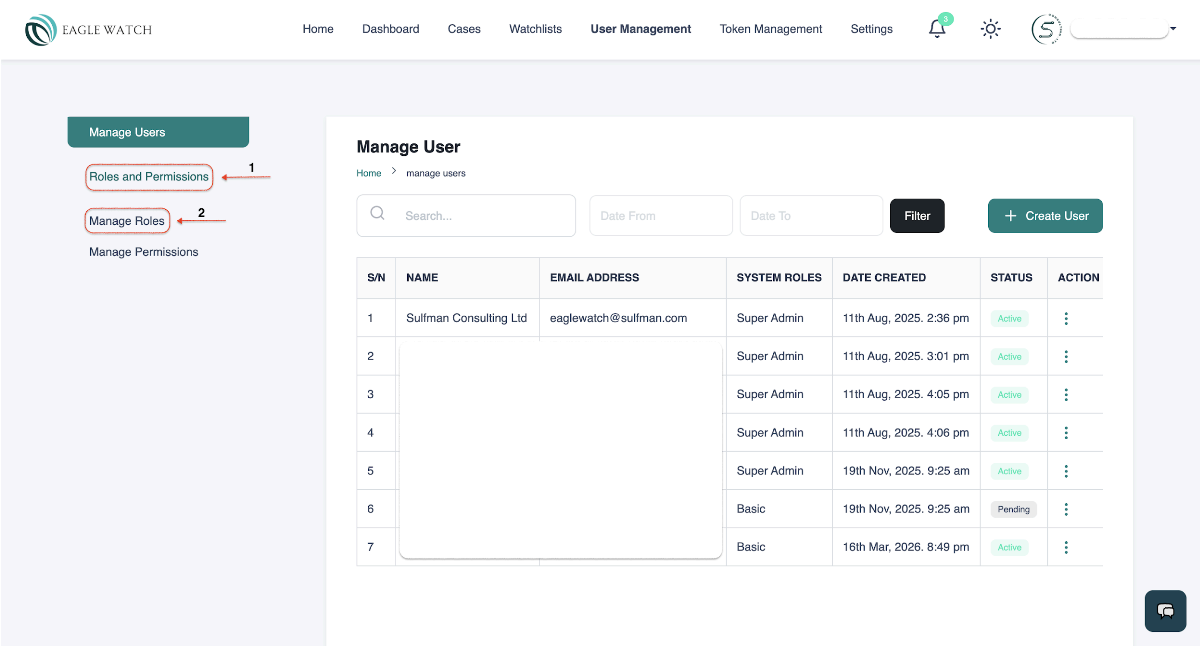
3. **Finalize:** Click **Create Role** to add it to the role library.



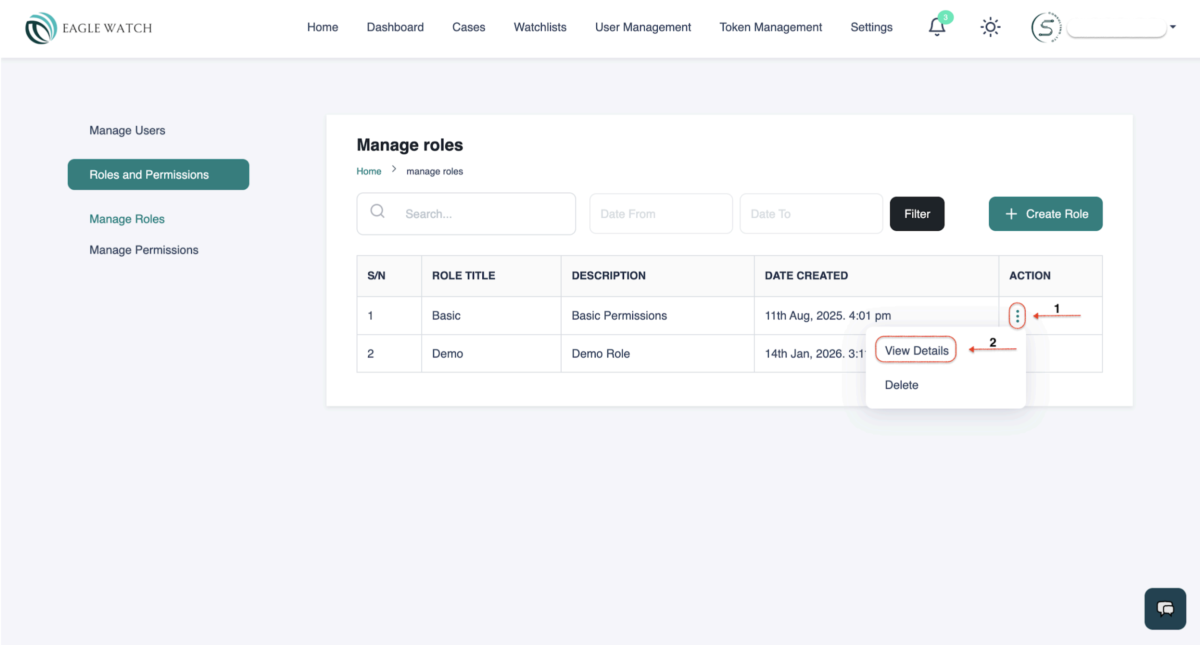
Best Practice: Use descriptive names that clearly indicate the level of access granted.

Roles Management - Viewing Role Details

1. **Navigate:** Select **Roles and Permission** from the User Management Tab.



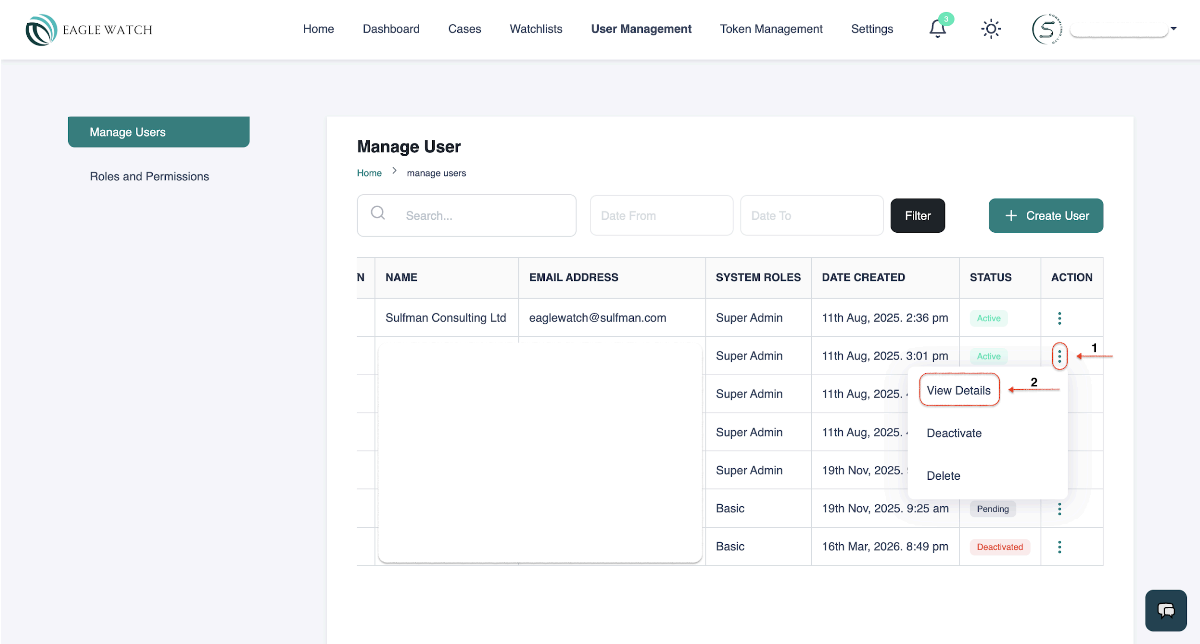
2. **Initialize:** Click the **Three-Dot Menu (Kebab)** on the right-hand side of the role to view role details and assigned users.



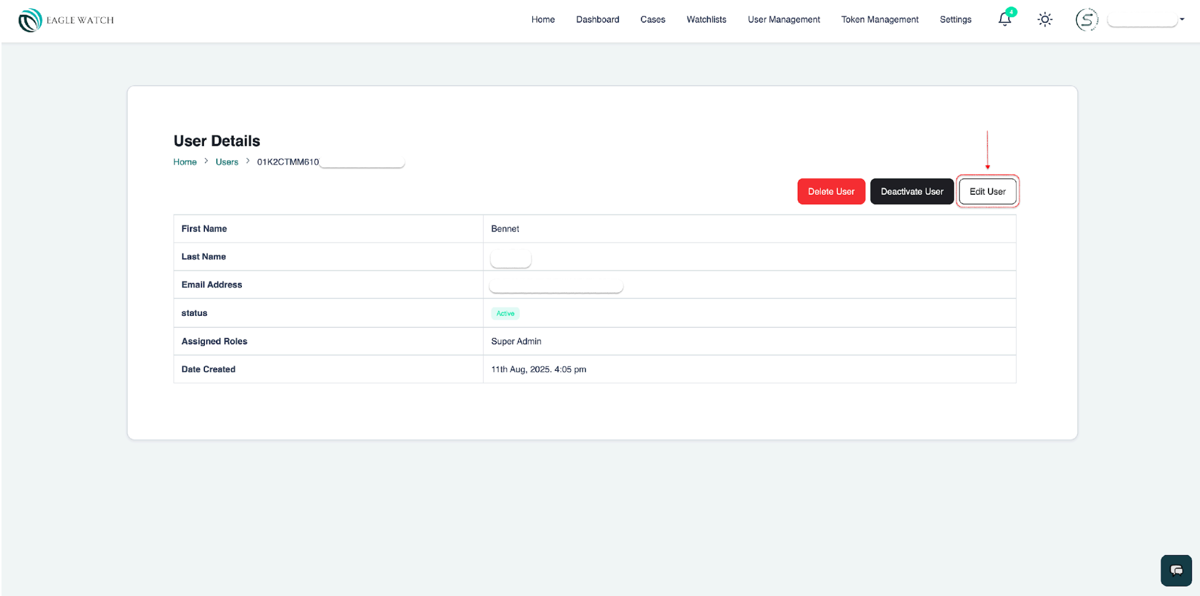
Roles Management – Reassigning a Role

Reassigning a role allows administrators to quickly update a user's access level as their responsibilities change within the organization.

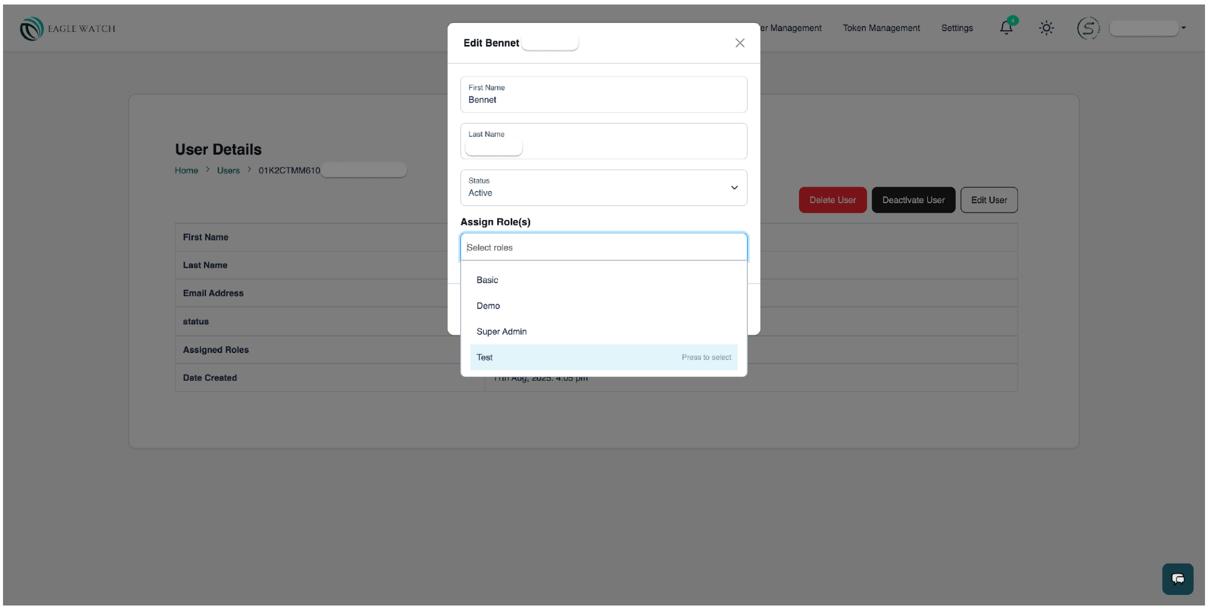
1. **Navigate:** Select **Manage Users** from the User Management Tab.
2. **Initialize:** Click the **Three-Dot Menu (Kebab)** on the right-hand side of the profile to view details.



3. **Select New Role:** Click the **Edit User** button.



4. **Finalize:** Click on **Assign Roles** to reassign the new role and apply the updated permissions immediately.

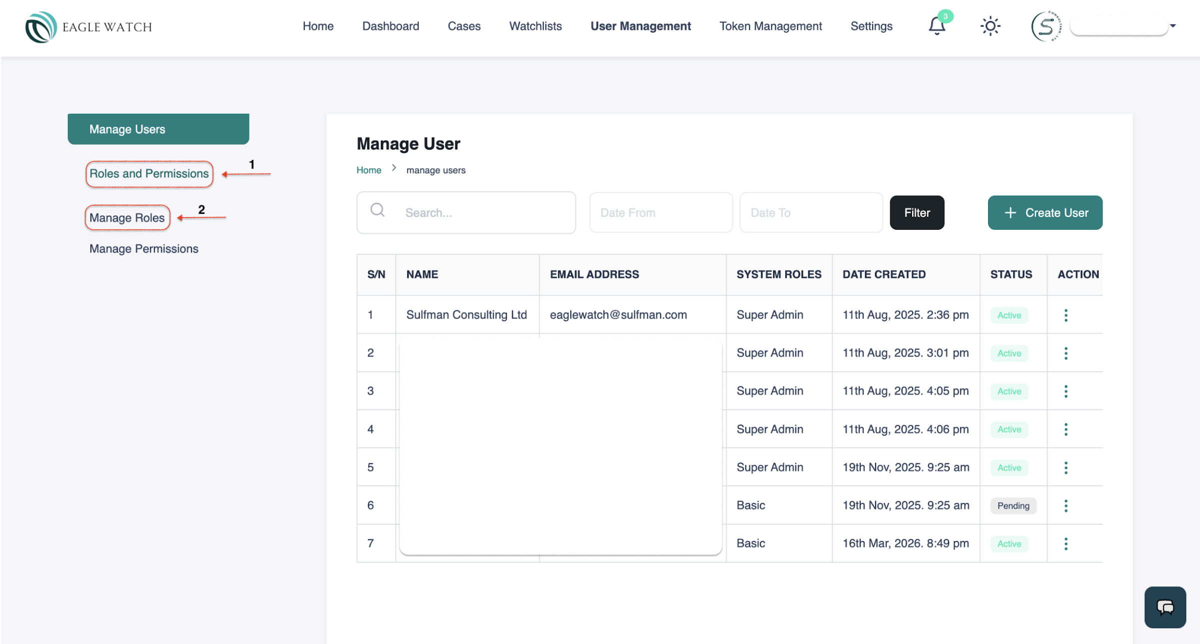


Best Practice: After reassigning a role, advise the user to refresh their browser or re-log to ensure the new **Permissions Management** settings are fully synced with their active session.

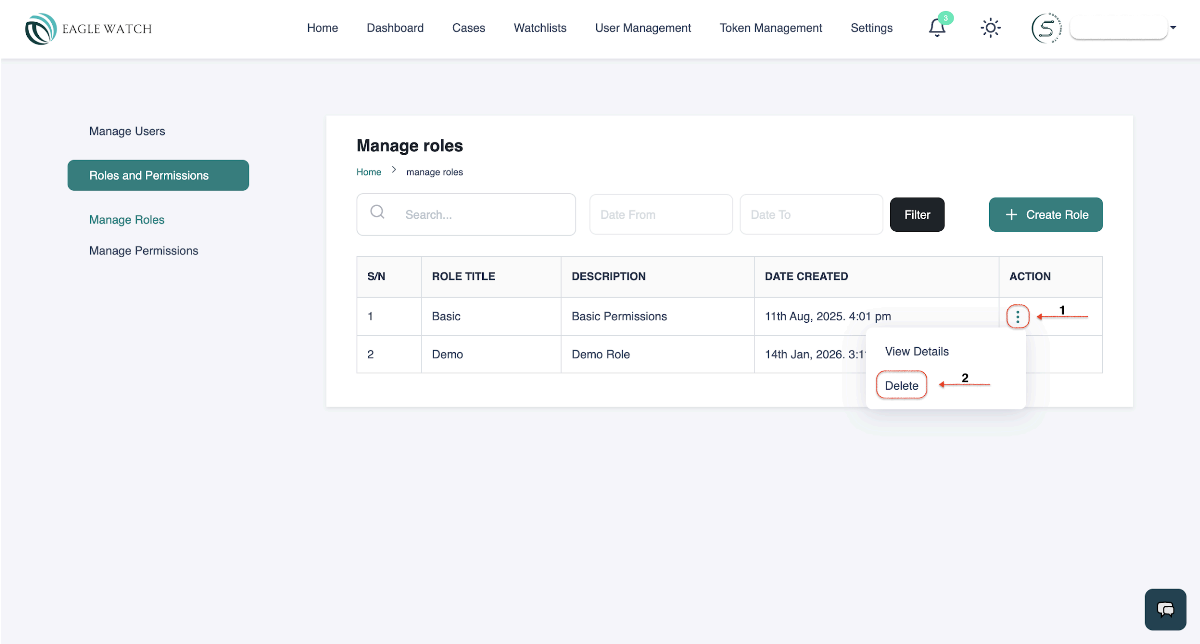
Roles Management – Deleting a Role

Before deleting a role, all users assigned to that role must be reassigned.

1. **Navigate:** Select **Roles and Permission** from the User Management Tab.



2. **Initialize:** Click the **Three-Dot Menu (Kebab)** on the right-hand side of the role to delete the role and its assigned users.



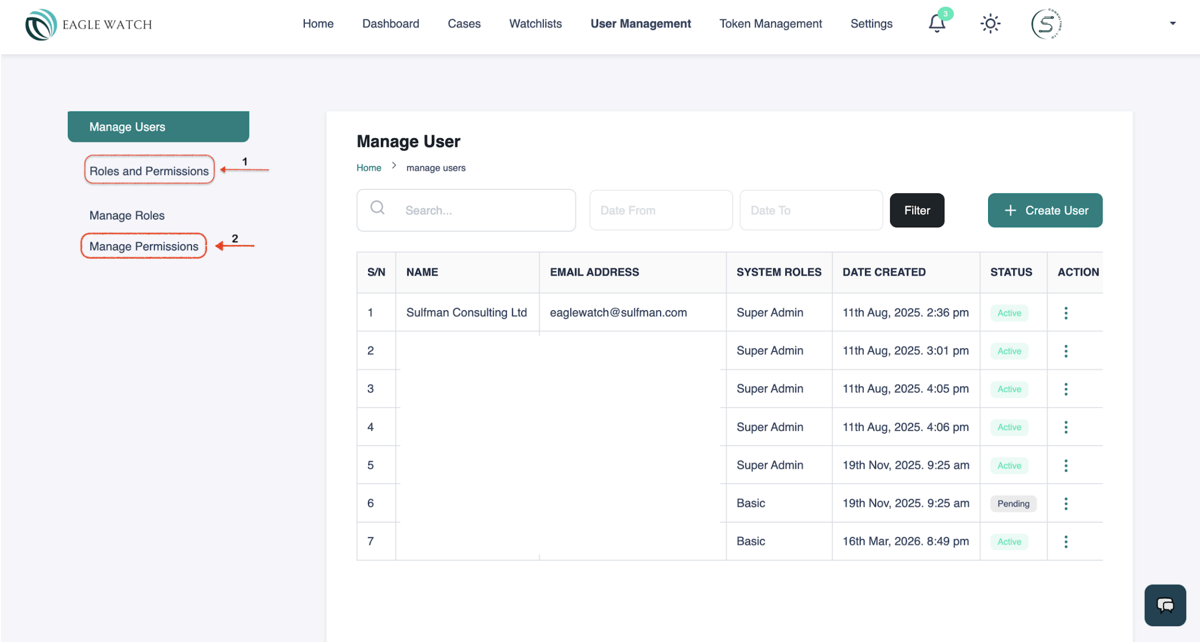
Best Practices:

- Confirm the role configuration aligns with access governance policies.
- Regularly review role templates and remove outdated or unused roles.

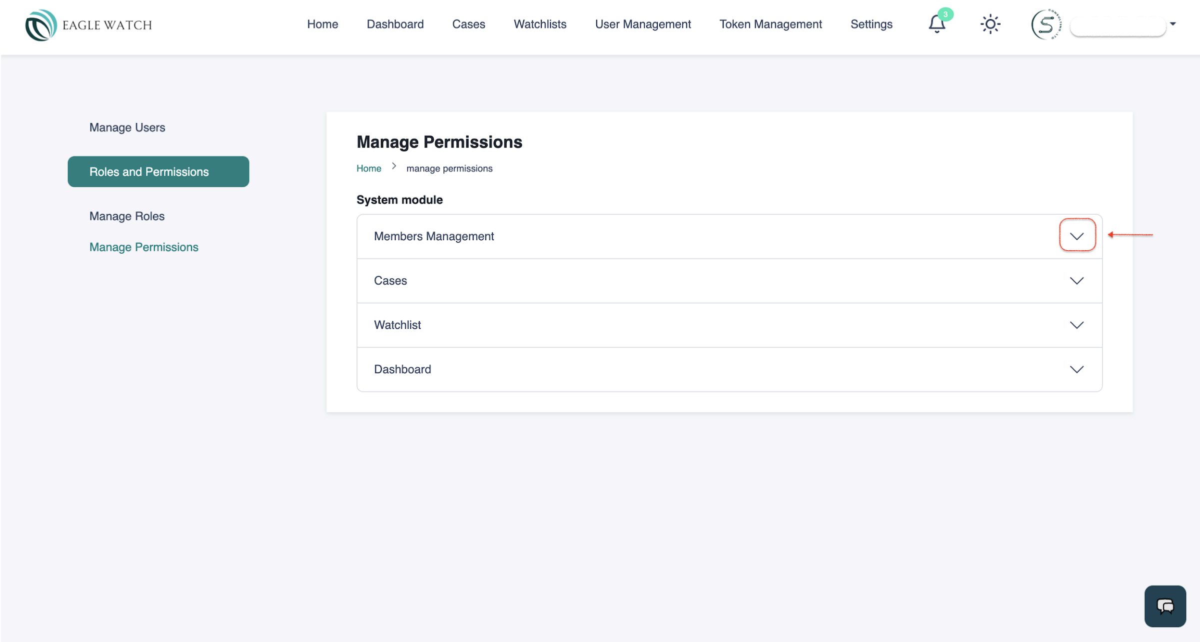
Permissions Management

Permissions define the specific actions a user can take within the platform:

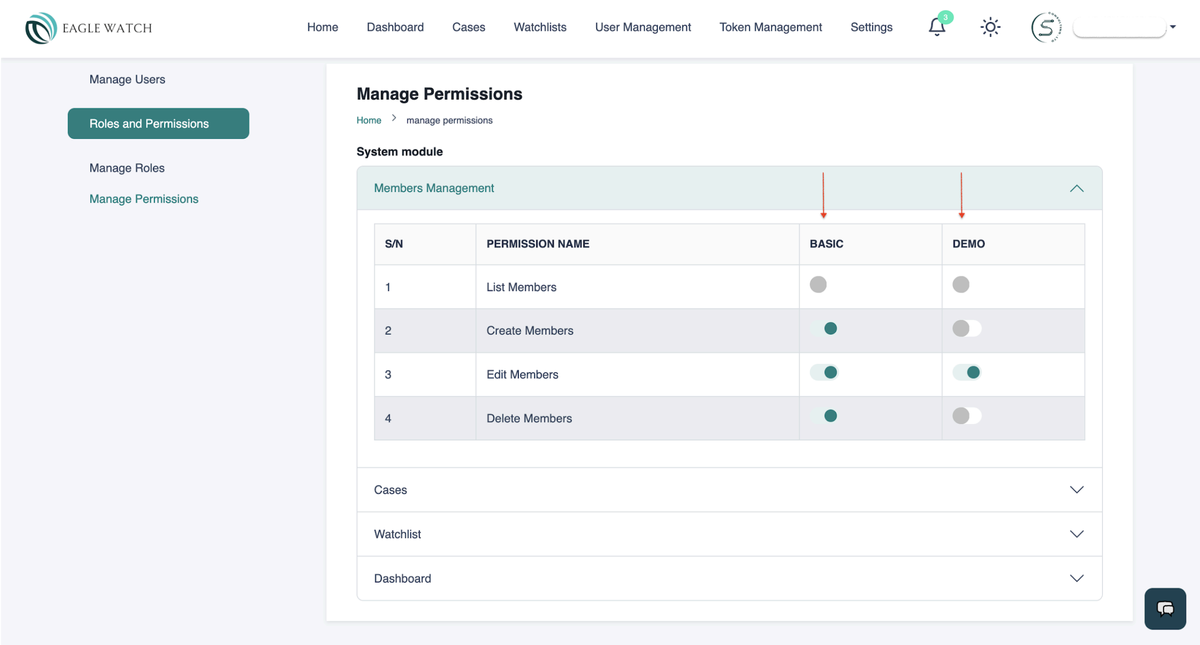
1. **Navigate:** Select **Manage Permissions** from the User Management Tab.



2. **Initialize:** Select the system module to define permissions for the chosen role.



3. **Define Permissions:** Enable or disable access across the available permission categories:

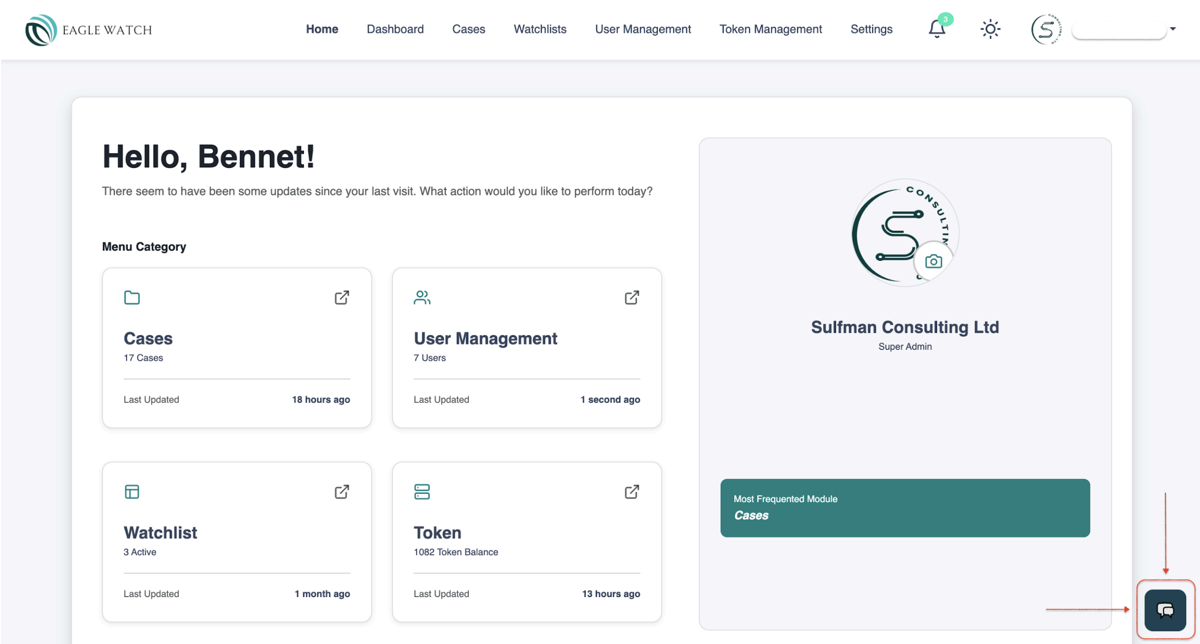


Best Practice: Apply the **principle of least privilege,** grant users only the permissions required to perform their duties.

Submitting Feedback

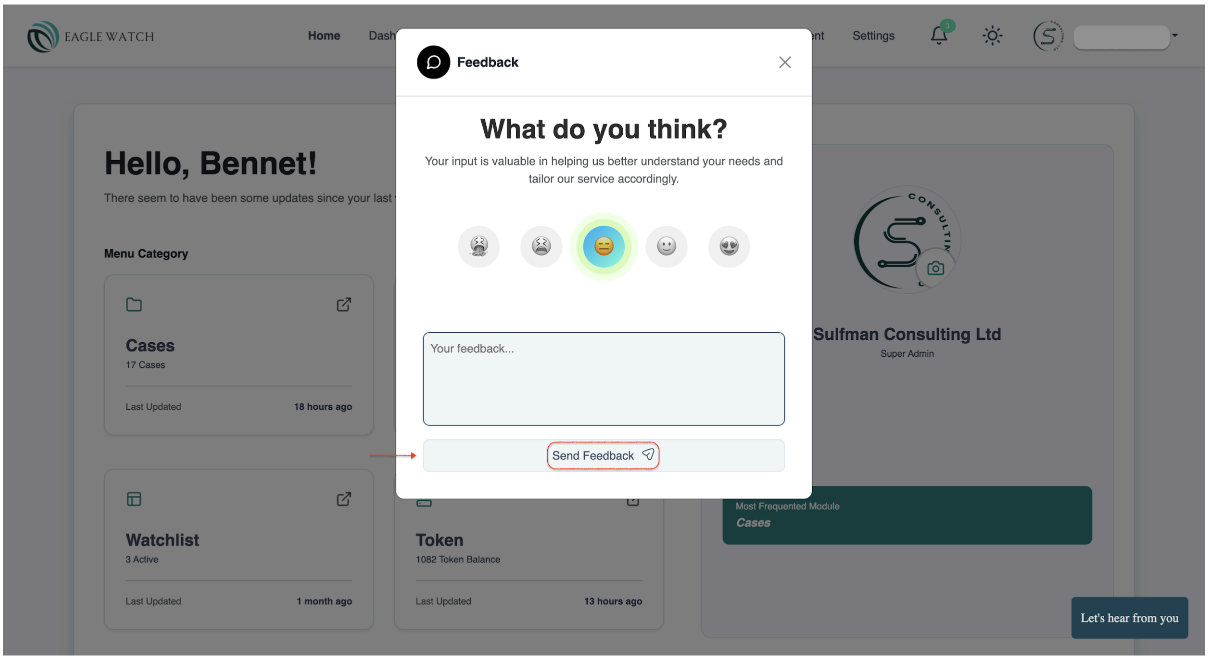
Use the platform's **Feedback** tool to quickly share your experience or report technical issues from any page, noting that submissions are limited to once every seven days to ensure quality review, or contact us directly at **eaglewatch@sulfman.com**.

1. **Navigate:** Access any page within the platform.
2. **Locate:** Find the **Feedback** button fixed at the bottom-right corner of the screen.



3. **Initialize:** Click the **Feedback** button to open the feedback panel.

4. **Select Emotion:** Scroll through the emoji carousel and choose the option that best reflects your experience.
5. **Describe Feedback:** Enter your comments, observations, or issues in the provided text box.
6. **Submit:** Click the **Send Feedback** button to submit your feedback.



Best Practice: Provide clear and specific feedback, including context (e.g., page, action taken), to help improve response time and resolution quality.