***Prevent User Deletion if Assigned to an Incident***

**Name:** Tangudu Nagamani

**Roll No:** 22A51A12C6

**Branch:** Information Technology

**Introduction**

In IT service management and security systems, maintaining data integrity and accountability is critical. One important control is the prevention of user deletion when that user is actively assigned to an incident. Incidents often require clear ownership, tracking, and historical records for auditing and compliance. If a user assigned to an open or unresolved incident is deleted, it can lead to gaps in accountability, broken workflows, and loss of critical information about incident resolution.

To avoid these risks, organizations implement rules that restrict user deletion until their incident responsibilities are reassigned or closed. This ensures that incident ownership remains consistent, historical data is preserved, and reporting or auditing processes remain accurate. Ultimately, this safeguard improves operational reliability, security, and compliance within the system.

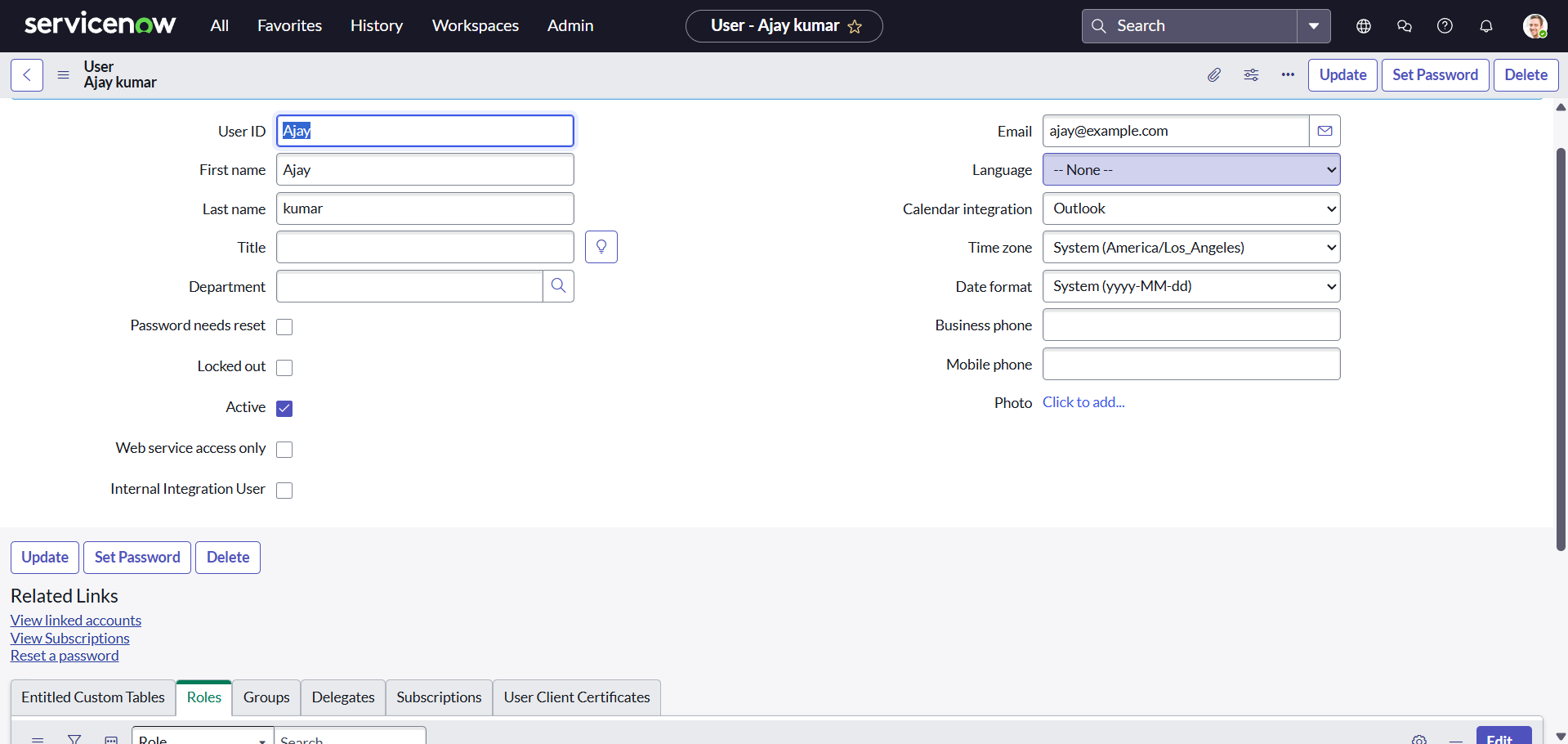
**Problem Statement**

In an IT Service Management environment, users are frequently assigned to incidents for issue resolution and tracking. However, the current system lacks a validation mechanism to prevent the deletion of a user who is still actively assigned to incidents. This can lead to broken data references, loss of accountability, and disruption in workflow continuity.  
There is a need to implement a safeguard that prevents such deletions unless all assigned incidents are closed or reassigned.

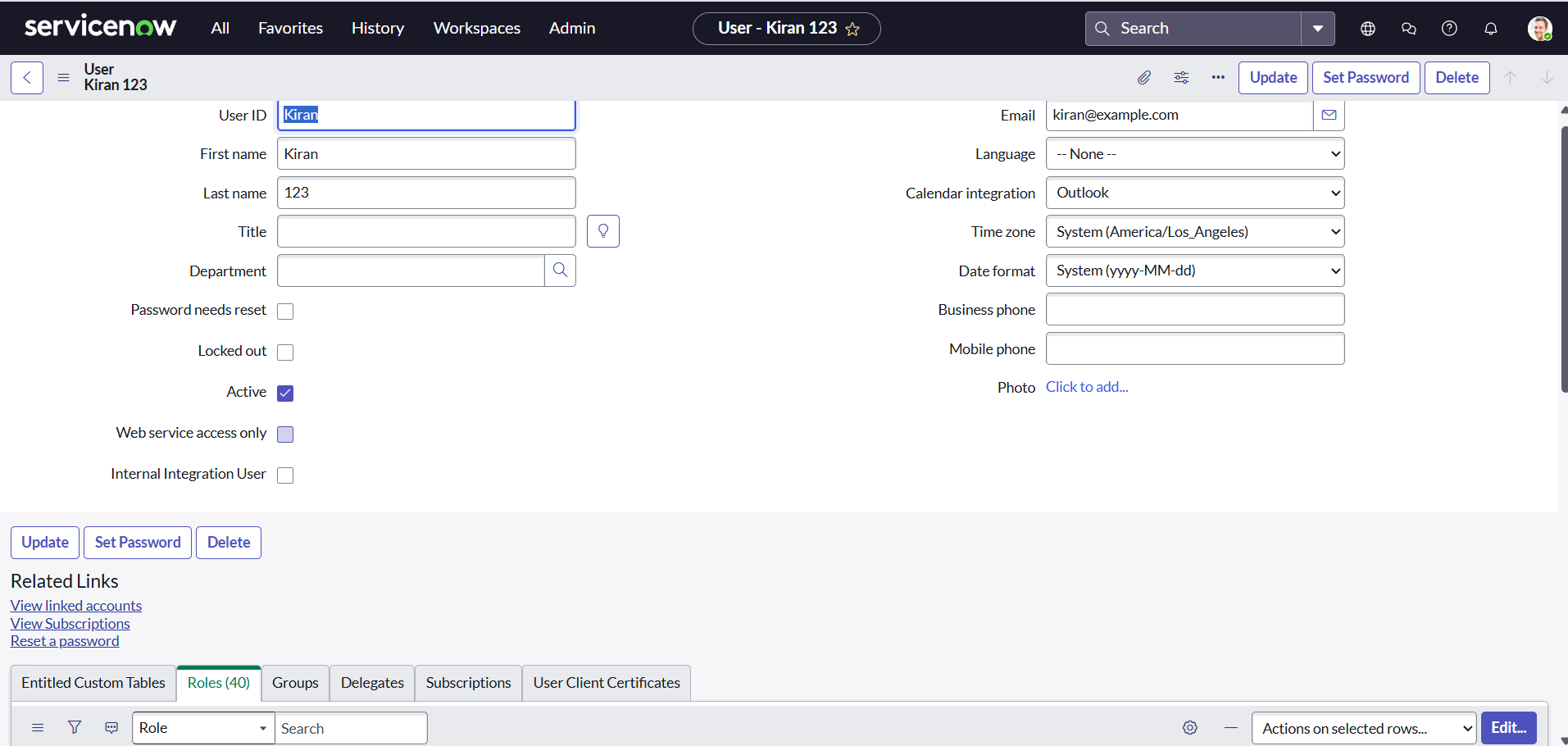
**User Creation**

1. Go to ServiceNow? All? Users (under System Security)
2. Click on New
3. Create two users (e.g., kiran kumar, ajaykumar)
4. Submit and verify user records.

1.Ajay Kumar(user)



2.Kiran kumar

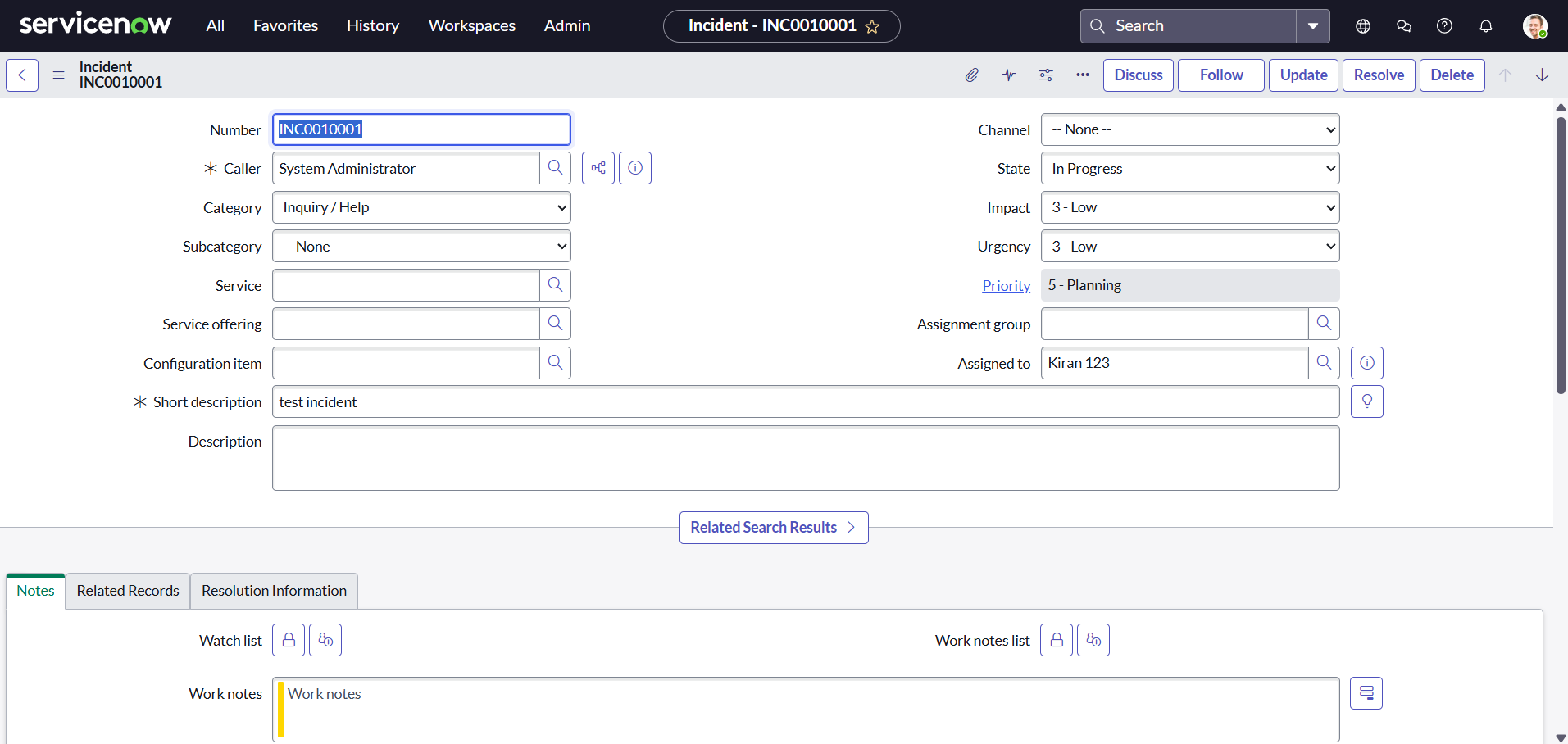


**Assign Incident to User**

1. Navigate to the Incident table.
2. Create a new incident and assign it to one of the created users (e.g.,kiran kumar)
3. Keep the incident Active = true and State = In Progress

To assign any user to the incident user should have at least one role.

so assigned a role to the user kiran kumar before assigning incident



**Business Rule Creation**

1. Go to System Definition? Business Rules
2. Click on New
3. Fill in:
4. Name: Prevent User Deletion if Assigned to an Incident
5. Table: sys\_user
6. When: Before
7. Delete: Checked
8. **Script:**

(function executeRule (current, previous /\*null when async\*/) {

var incGr = new GlideRecord('incident');

    incGr.addQuery('assigned\_to', current.sys\_id);

    incGr.setLimit(1); // Just need to check existence

    // incGr.addQuery('active', true); we can use  the above or this line of code to check where the user is assigned with any incident

    incGr.query();

    if (incGr.next()) {

        gs.addErrorMessage('This user cannot be deleted because they are assigned to one or more incidents.');

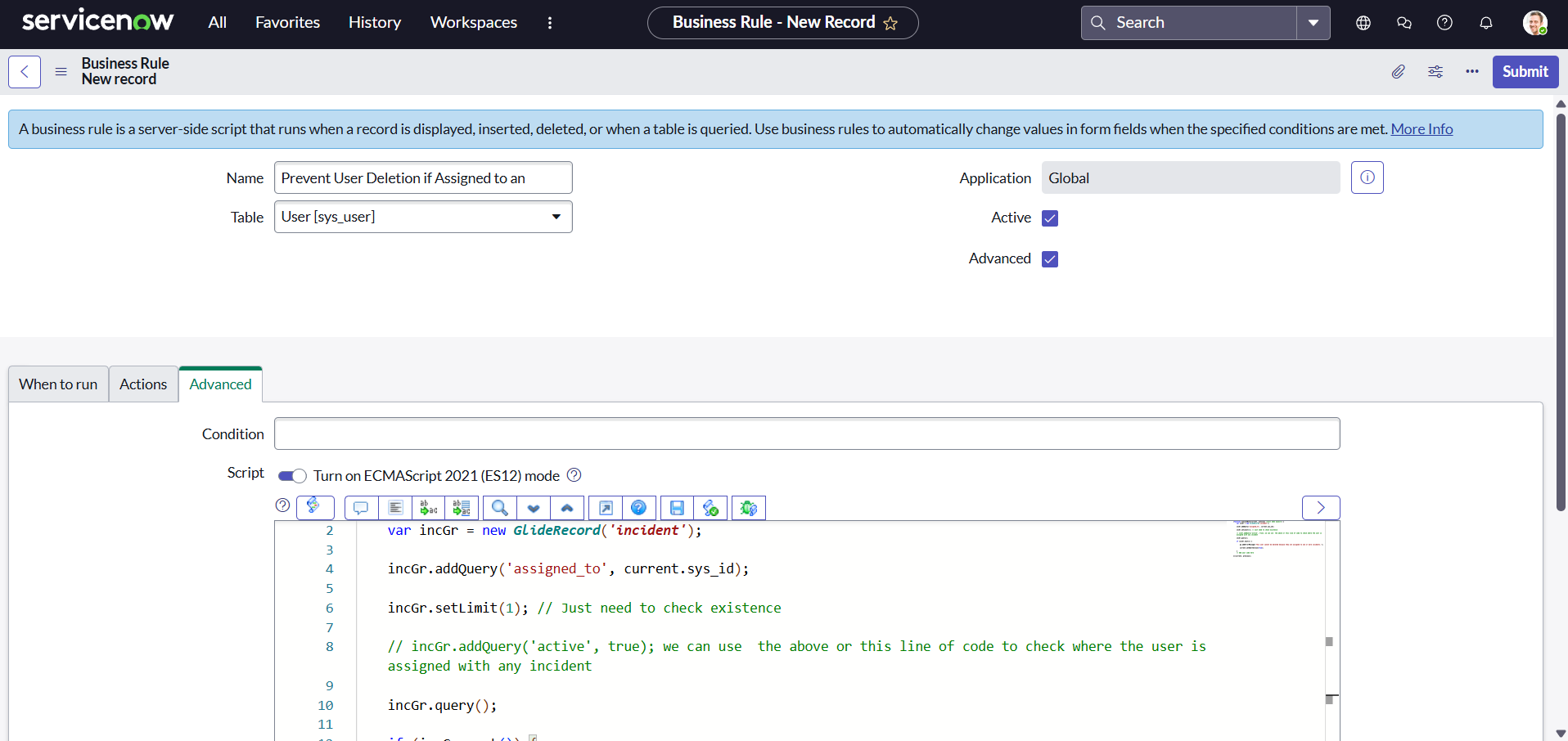
        current.setAbortAction(true);

    }

// Add your code here

})(current, previous);

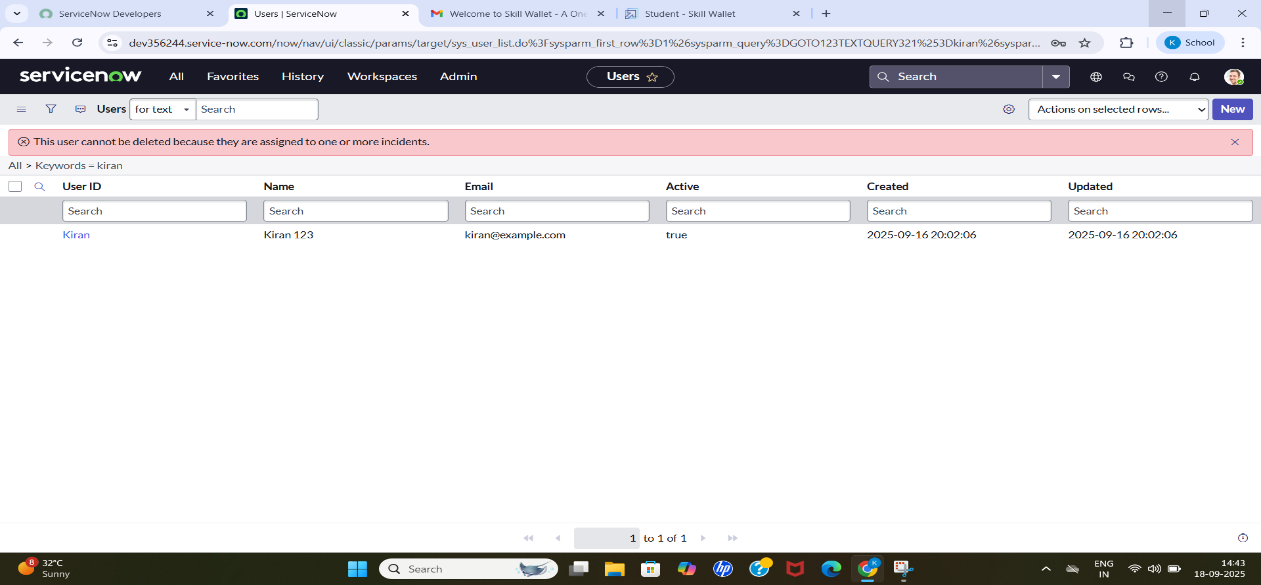
9.Click on submit.



**Test Deletion**

**Attempt to Delete Assigned User**

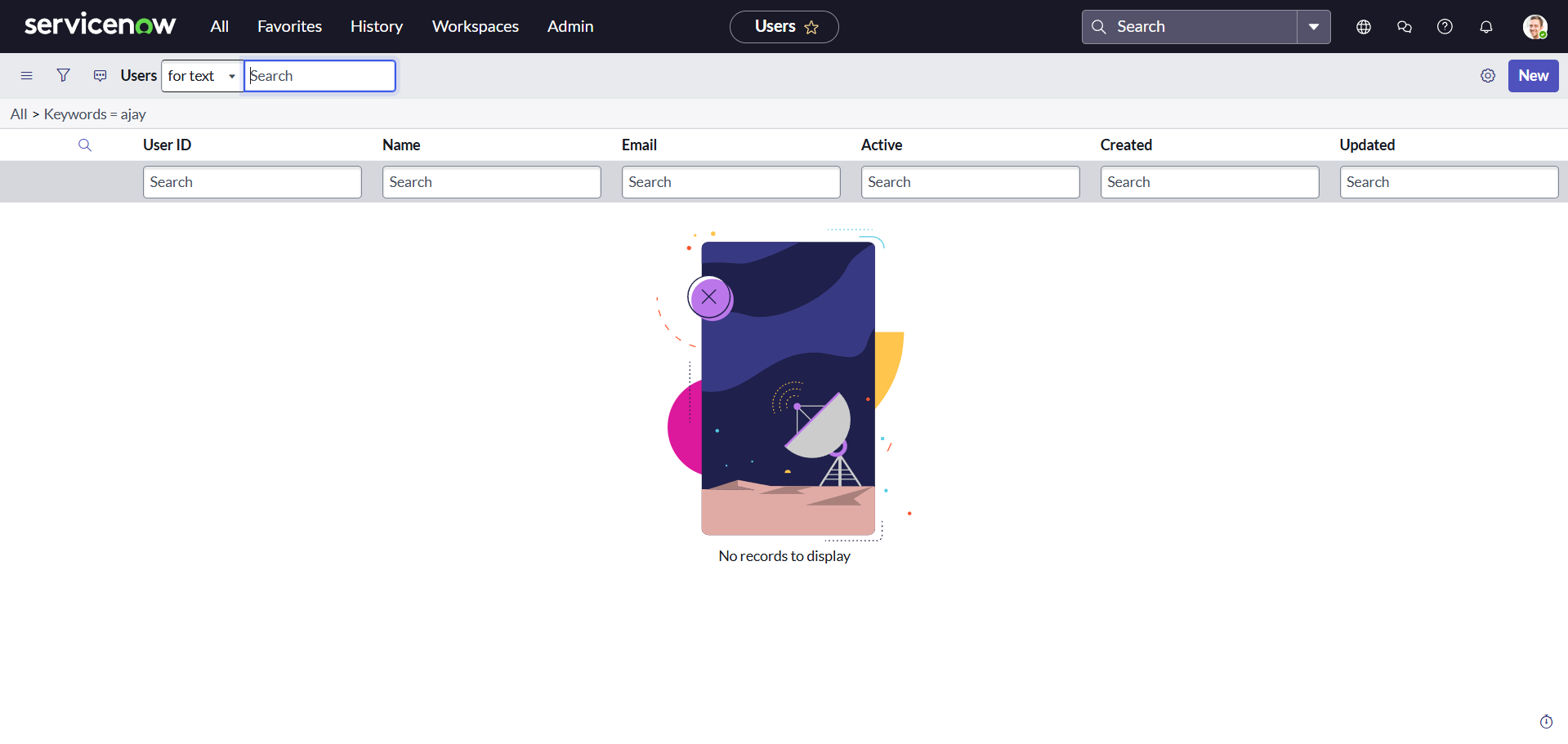
1. Go to the user record (kiran123)
2. Click Delete
3. Verify that deletion is blocked with an error message



**Test With Unassigned User**

**Attempt to Delete Unused User**

1. Try deleting the second user (Ajaykumar) who is not assigned to any active incidents.
2. Deletion should succeed.



**Conclusion**

Implementing a restriction on user deletion when they are assigned to an active incident strengthens accountability, data integrity, and compliance within the system. By ensuring that users remain linked to their assigned incidents until proper reassignment or closure, organizations can prevent workflow disruptions, avoid data inconsistencies, and maintain a complete audit trail. This control not only enhances operational efficiency but also upholds security and governance standards, making the incident management process more reliable and trustworthy.