User Administration in ServiceNow

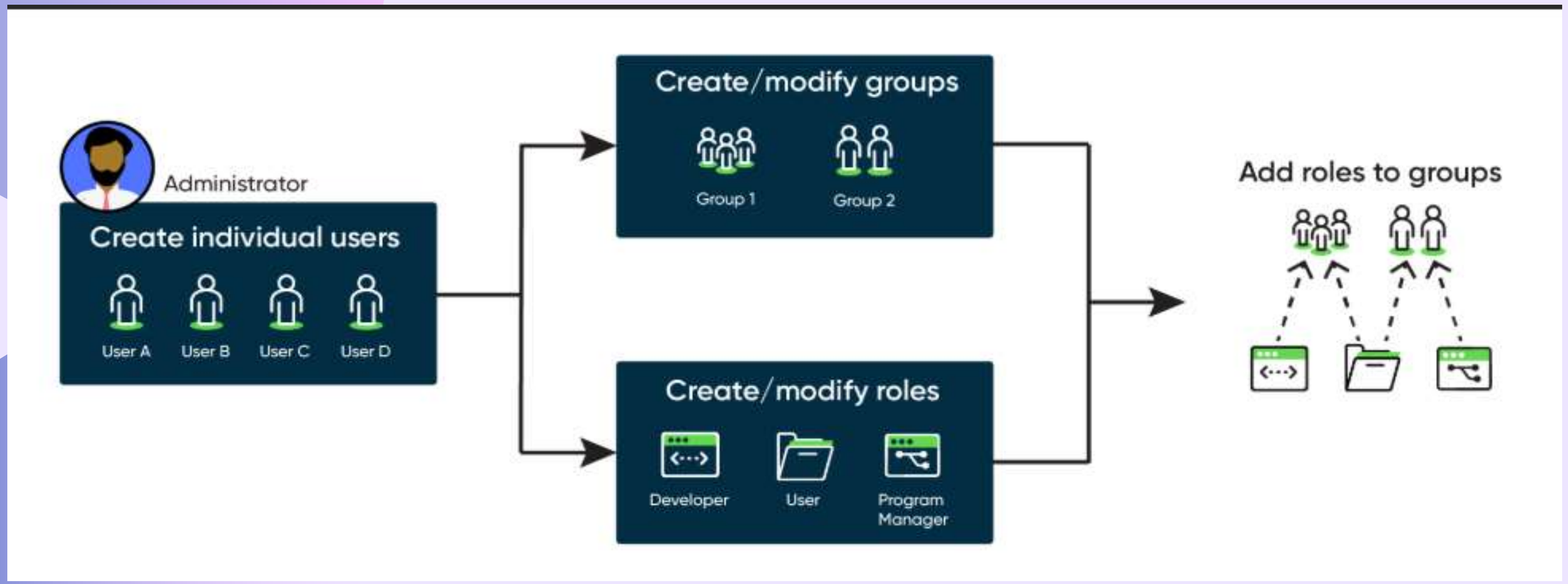
SYSNOW Software PVT.LTD.
Plot No- 297 , District Center,
Bhubaneswar , Odisha. INDIA
Pin – 751016
Mail- ***info@sysnowsoftware.com,***
hr@sysnowsoftware.com

EXPLORING USER ADMINISTRATION:-

OVERVIEW:-

Creating users, groups, and roles provide a flexible and scalable way to manage access to features on the ServiceNow AI Platform. By creating user accounts, assigning users to groups, and defining roles and permissions, administrators can ensure that users have the appropriate level of access to applications and data. This enables organizations to control access to sensitive data, maintain conformance with regulatory requirements, and improve overall security. Additionally, users, groups, and roles can be easily managed and modified over time as organizational needs change.

User Administration Workflow:-



WORK FLOW:-

1. SUBSCRIPTION MANAGEMENT:-

Understand your subscriptions. Subscription management enables you to manage your subscriptions proactively and monitor subscription usage on your instances. Subscriptions may include per-user subscriptions. For more information, see Managing per-user subscriptions in Subscription Management

2. CREATING USERS, COMPANIES, AND DEPARTMENTS:-

Create an account record for the individuals who have access to your instance. Each user account has a unique login ID, password, and set of permissions (roles) that define what they can do and access within the platform.

3.CREATING GROUPS:-

Define groups that have similar roles or permissions. Groups enable you to apply permissions (roles) to multiple users at the same time. When a user is a member of a group, that user has the same permissions that have been defined for the group.
You can view group members by navigating to All > User Administration > Groups. Select a group name and view the members in the Group Members related list.

4.MANAGING ROLES:-

Roles describe the types of activities that a user can perform on the instance. Each role has a set of permissions that can govern what the users and groups can do, such as read, write, create, or delete records. Roles can be assigned to users and groups. Users can have multiple roles.

5.MONITORING INSTANCE USAGE:-

Users with the admin or usage_admin role can view the Application usage overview and ServiceNow Store usage overview dashboards to track instance usage.

6.Monitoring user activity:-

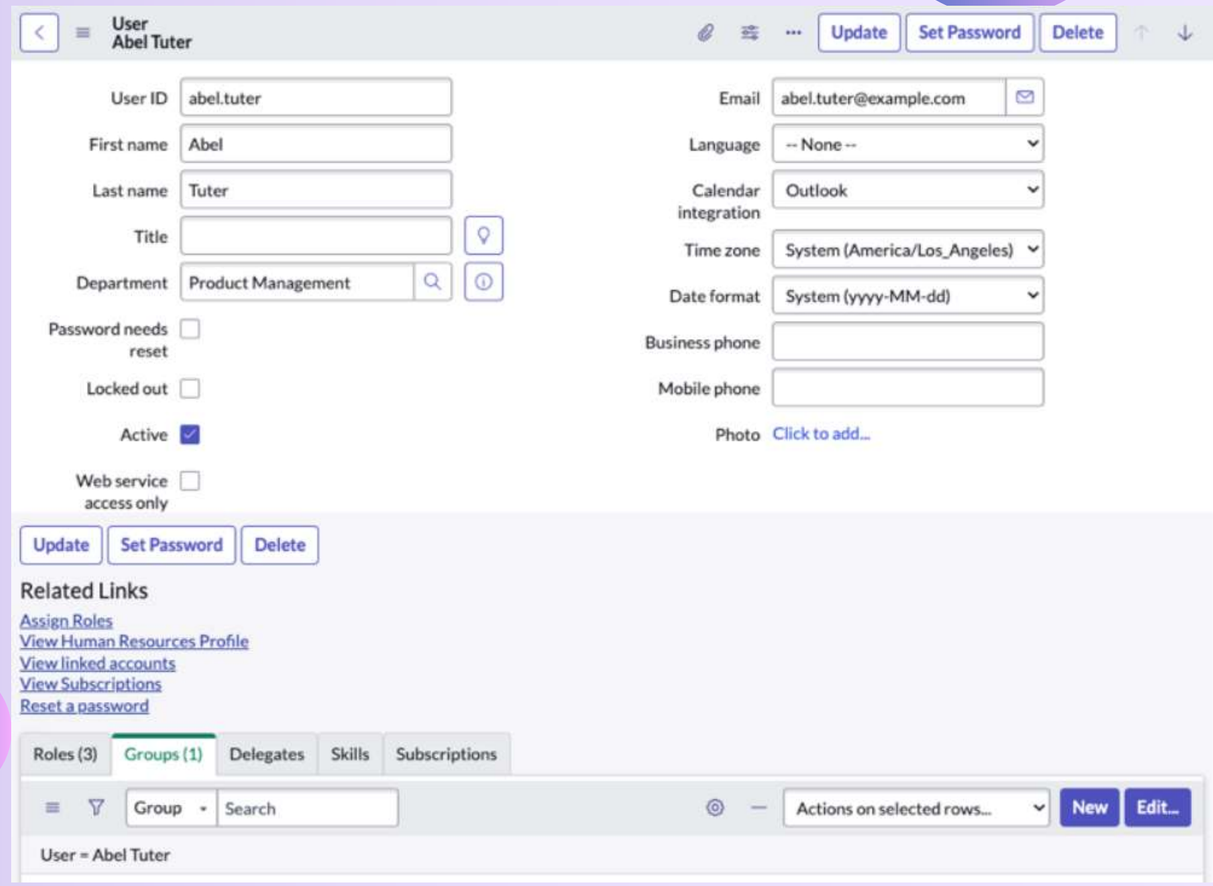
Users with the admin role can impersonate users, manage user sessions, and leverage non-interactive sessions.

USER ACCOUNT RECORDS:-

User records establish a relationship between an individual and your ServiceNow instance. User records consist of a user name, a password, and information relating to the individual, such as contact information, location, and job title.

RELATED RECORDS:-

User records are associated with records on several other tables to control permissions, preferences, and other features.



Roles

User Roles:-

- Definition: A user role defines specific permissions that a user can access.
- Assignment: System Administrators assign user roles to individual users.
- Examples: Common user roles include admin, itil, knowledge_manager, etc.

Group Roles:-

- Definition:A group role assigns permissions to a group of users, rather than individual users.
- Assignment:When a user is added to a group that has a specific role, the user automatically inherits those permissions.
- Benefits:This simplifies access management, as you can manage permissions for a group of users rather than individually.

CREATING USERS, COMPANIES, AND DEPARTMENTS:-

Create user records for the individuals who access your instance. Users can be assigned to groups with defined roles to determine what records and actions they can access.

1.Creating users:-

Users are typically added through Lightweight Directory Access Protocol (LDAP) directory integrations. Admins can also manually add users to the instance, enable self-registration for new users, and impersonate users to ensure that they have the proper access privileges.

2.Add a new company:-

You can add companies that represent vendors, manufacturers, or customers with whom you do business. These companies provide a way to categorize users, groups, and assets.

3.Normalization data services:-

The Normalization Data Services plugin helps maintain consistency for table fields that refer to a company name.

4.Add a department:-

Departments provide another way to categorize users, groups, and assets. You can add departments and assign them to users.

CREATING GROUPS:-

Admins can add users to one or more groups.

1.Create a user group:-

Create groups and assign roles to them. Users assigned to the group inherit the roles.

2.Add a user to a group:-

Add a user to a group so that the user inherits all the roles assigned to the group.

3.Configure assignment group types:-

Use the Type field to define categories of groups. Once defined, you can use these categories to filter assignment groups based on the group type using a reference qualifier.

ADD A USER TO A GROUP:-

Add a user to a group so that the user inherits all the roles assigned to the group.

->Before you begin

Role required: user_admin

->About this task

If you’re a non-admin user, you can’t add a user to a group that contains the admin role. Likewise, if you don’t have a security_admin role, you can’t add a user to a group that contains the security_admin role.

->Procedure

Navigate to All > User Administration > Groups.
Select a group Name.
In the Group Members related list, select Edit.
Select one or more names in the Collection list.
Select Add and Save.
(Optional) Remove a user from a group when they change roles.
Navigate to All > User Administration > Groups.
Select a group Name.
In the Group Members related list, select the check box next to each group member name you want to remove.
From the Actions on selected rows menu, select Delete.

Thank You!

FOR YOUR ATTENTION