

Persona Types in the Platform



System Administrator

The system administrator provides access to all platform features, applications, functions, and data



Specialized Administrator

Users with specialized administrator roles may manage specific functions or applications, including: Assignment Rules, Knowledge Base, Human Resources, Reports, and Web Services



Process User

Users with the process user role may fulfill ITIL activities associated with the ITIL workflow, including incident and change management



Approver

The approver can perform all requester actions and allows users to view or modify approval records directed to them



Requester

Also known as Employee Self Service (ESS) users, these users do not have roles but can submit and manage their own requests, access public pages, etc.

Users and Groups



Users are represented by a record on the **User [sys_user]** table.

Among other tasks, within a ServiceNow instance, **users** may:

- Update records
- Import data
- Request items
- Implement flows
- Approve knowledge content
- Run reports
- Develop applications



A **group** is represented by a record on the **Group [sys_user_group]** table.

A collection of users is a **group**.

Groups share a common purpose such as users approving change requests or users receiving e-mail notifications

Examples of Groups include:

- Service Desk
- Knowledge Base Authors
- HR Administrators

The ServiceNow Platform utilizes role-based access to ensure people have the information and workflows they need to fulfill their roles. It is crucial to protect sensitive data. Realize not every member of your organization needs access to all information at all times.

To understand how role-based access works in the ServiceNow Platform, it is important to first define its components.

Manage the individuals who can access ServiceNow by defining them as users in the platform. A **user** is an individual that has been granted access to your ServiceNow instance. User IDs are unique identifiers for the user's ServiceNow login user name.

A **group** is a set of users who share a common purpose. Members of groups perform similar tasks or need access to similar information for various purposes, such as approving change requests, resolving incidents, receiving email notifications, or administering the Service Catalog. Users working in ServiceNow are typically assigned to one or more groups. A group is part of the user hierarchy, and a user is part of a group.

Users and groups may be imported from a corporate directory (LDAP) or created manually in ServiceNow.

Add a user to your instance by navigating to All > User Administration > Users > and select New.

Add a group to your instance by navigating to All > User Administration > Groups > and select New.

To add a user to a group, select Edit in the Group Members related list and select a name of your choice in the List collector. Add the user by double-clicking the name or by selecting the Add arrow.

Once the user is added to the Group Members list, select Save.

Roles


A **role** is used to define access at the application, module, and/or Access Control List (ACL). A **user** can have **more than one role**.

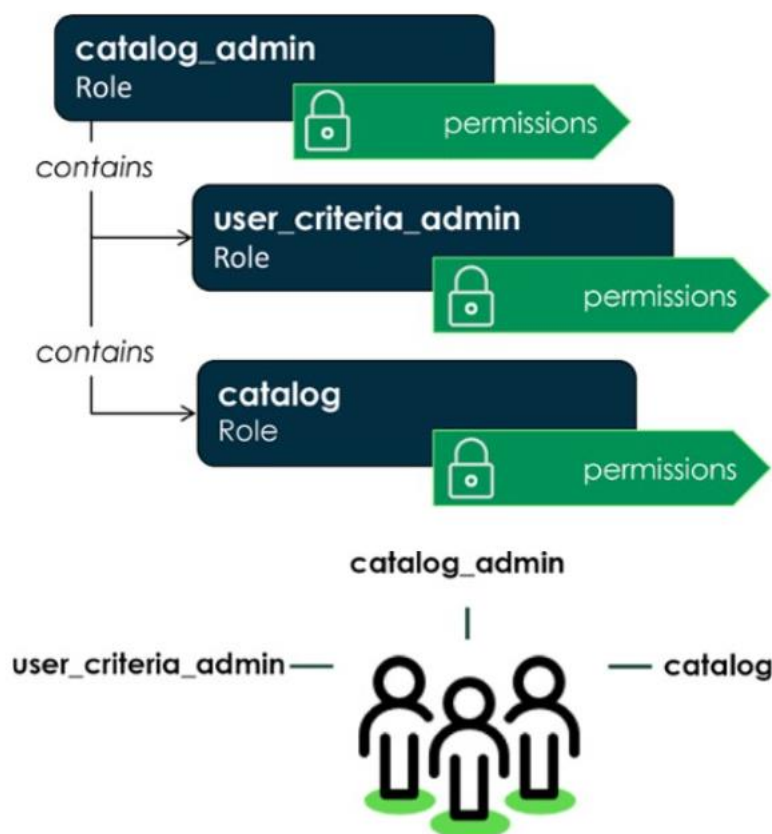
A **role** is used to:

- Grant access to the application/modules that a user has access to in the All menu
- Assign security rights.
- Access data in the tables via the ACL (read, write, update, or delete)

A **role** can:

- Be assigned to a group* or a single user
- Contain other roles.

 **Roles** are represented by a record on the **Role [sys_user_role]** table



Roles control access to features and capabilities in applications, modules, and/or Access Control List (ACL). These roles define which applications a user or group will and will not be able to access and which actions the user can take on records within the applications.

In the example, the catalog admin role contains the user_criteria_admin and catalog roles. If a user or group was assigned the catalog-admin role, they would be granted the permissions of all three roles. Once access has been granted to a role, all of the groups or users assigned to that role are granted the same access.

Generally, when you think about your "role" in the workplace, you are thinking about your specific position or title, such as project manager or developer. In the ServiceNow Platform, the word "role" defines your capabilities in the application. Therefore, it is important to distinguish between the different

definitions.

Later in the course, you will learn how roles are used in conjunction with users and groups as the second level of security for accessing data in Service Now.

Assigning Roles

Application/Module access is controlled by roles. Roles may contain other roles.

Application > Module access	catalog role	user_criteria_admin role	catalog_admin role
Service Catalog	✓		✓
Service Catalog > User Criteria		✓	✓
Knowledge > User Criteria		✓	✓
Contextual Search			✓
Item Designer			✓
Service Creator			✓

The table illustrates the following:

- A user who is assigned the catalog role only has access to the Service Catalog application and its associated modules.
- A user with the user_criteria_admin role only has access to two modules: All > Service Catalog > User Criteria and Knowledge > User Criteria.
- A user with the catalog admin role has access to all of the applications and modules of both roles plus any permissions specific to the catalog admin role.

Note: Users without any assigned role permissions can still log in to ServiceNow and access common actions, such as viewing a dashboard, accessing the Service Catalog, viewing knowledge articles, and taking surveys. These users will have access to anything the System Administrator has configured, that doesn't require any specific role to access. These are often referred to as self-service users.

User Impersonation

Impersonate user

1. Open the user menu
2. Select **Impersonate user**
3. Select a user
4. Select **Impersonate user**

End impersonation

1. Open the user menu
2. Select **End impersonation**
3. You can also select **impersonate another user** or **Log out**.

When you impersonate a user with an application-specific admin role (for example, an application admin for Human Resources or Security Incident Response), you cannot access features granted by the application admin role, including security incidents, profile information, or other scope-protected features, unless you already have those roles. Access to modules and applications in the Filter navigator is also restricted. Admins cannot change the password of any user with an application admin role.

Tip: It is recommended to create logins for the following roles to effectively test the system:

- admin - to do work
- itil - to test as a process user
- ess (employee self service) - to test as an end user

Note: Impersonations are logged in the System Log. The `sys_property glide.sys.log impersonation` needs to be added and set to true in order to see impersonation events in the System Log. This log file enables (true) or disables (false) impersonation logging for interactive sessions.

ServiceNow - Intelligent platform for end-to-end digital transformation

To start off, ServiceNow is the intelligent platform for end-to-end digital transformation. The ServiceNow Platform is an Application Platform-as-a-Service. This means the platform resides in the cloud. Companies no longer have to buy and manage the equipment necessary to host these applications.

ServiceNow provides services to its users from a configurable web-based user interface, built on top of a flexible database schema.

The Platform and the applications that run on it use a single system of record to consolidate an organization's business processes.

- The single data model allows sharing of data between applications and departments.
- The Platform integrates with other enterprise systems and supports a wide variety of plug-and-play applications.
- With ServiceNow, you can also build custom applications.

Any company of any size across any industry can accelerate end-to-end transformation with our platform.

It's a single platform with automation, engagement, and AI built in and serves as the foundation for our Workflow solutions, which are pre-built, intelligent, and easily configurable work solutions.