

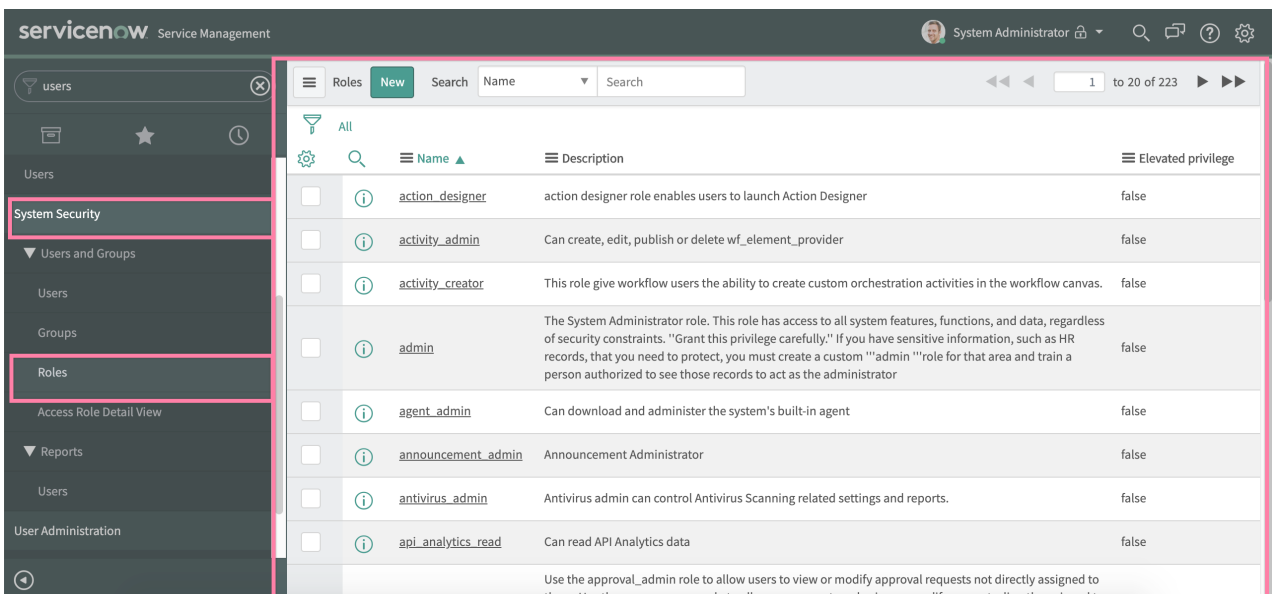
ServiceNow - Metadata and User Roles

Last Modified on 03/16/2020 3:32 pm EDT

When creating new users in ServiceNow UI, the users should have certain permissions to access metadata and, implicitly, have access to the SAP Cloud Platform Open Connectors CO feature. To have access to this feature, the user should be a **sys_user** with permission rights to access the **sys_dictionary** table. The **sys_user** permission is usually by default part of the following roles: *admin*, *delegated_developer*, *user_admin*, *catalog*, and *cloud_admin*.

To see the definitions of the roles directly in the Service Now account, you can navigate to the

Security tab and access the **Roles** :



The screenshot shows the ServiceNow interface for managing roles. The left sidebar is expanded to the 'Roles' section. The main content area displays a table of roles with columns for Name, Description, and Elevated privilege. The roles listed are:

Name	Description	Elevated privilege
action_designer	action designer role enables users to launch Action Designer	false
activity_admin	Can create, edit, publish or delete wf_element_provider	false
activity_creator	This role give workflow users the ability to create custom orchestration activities in the workflow canvas.	false
admin	The System Administrator role. This role has access to all system features, functions, and data, regardless of security constraints. "Grant this privilege carefully." If you have sensitive information, such as HR records, that you need to protect, you must create a custom "admin" role for that area and train a person authorized to see those records to act as the administrator	false
agent_admin	Can download and administer the system's built-in agent	false
announcement_admin	Announcement Administrator	false
antivirus_admin	Antivirus admin can control Antivirus Scanning related settings and reports.	false
api_analytics_read	Can read API Analytics data	false

Also, ServiceNow offers the possibility of defining a new role and apply ACL rules (Access Control Rules) which means one can create a custom role with custom permissions.