Chapter 1 Introduction

VilMinds ServiceNow Connector is a seamless and loosely coupled integration with ServiceNow IT SERVICE MANAGEMENT. Transform the Speed, Visibility, and Agility of ITSM through Liferay portal. This Connector helps to achieve the end to end digital transformation for your IT services and infrastructure through a single unified portal. ServiceNow Connector lets you interact with the below ServiceNow Features while automating service management processes. It's simple to configure and fast to deploy, so

You can go live quickly with confidence while scaling to your business needs.

Chapter 2 Key Features

- Service Portal: Create Incident, requests and view his requests, incidents
- Service Catalogue: Create an order for Asset Hardware or software which he needed
- Knowledge Base: View all the articles related to ITSM
- My Assets: View all his assets which are in use currently
- Notification: View all his notification
- LDAP Integration
- SSO Integration
- OAuth2 authentication
- Role Base access

Compatibility:

Liferay: liferay-ce-portal-7.0-ga7+ and DXP.
ServiceNow: Kingston, London

Chapter 3 Deployment Steps

Step 1.

Download the ServiceNow connector .lpkg file from Liferay marketplace.

Step 2.

Please create your own ServiceNow instance on https://developer.servicenow.com

Set the below properties into the portal-ext.properties file

```
servicenow.api=Your ServiceNow instance URL

snow.auth.oauth.clientid=Your app client id

snow.auth.oauth.clientsecret=Your app client secret

servicenow.authanticationtype=Provide your authentication type
```

For getting this values you have to follow the **Section C of Step 4**.

Step 3. Deploy the .lpkg or .war to Liferay Portal by either way

a. Login to Liferay with Admin credentials.
b. Go to Control Panel -> Apps-> App Manager
c. Click on Top Right Corner 3 vertical dots -> Upload.
d. Browse the files and select .lpkg or .war file.

OR

Copy the (war or .lpkg) file to the deploy folder of your liferay installation directory.

Step 4. ServiceNow configurations:

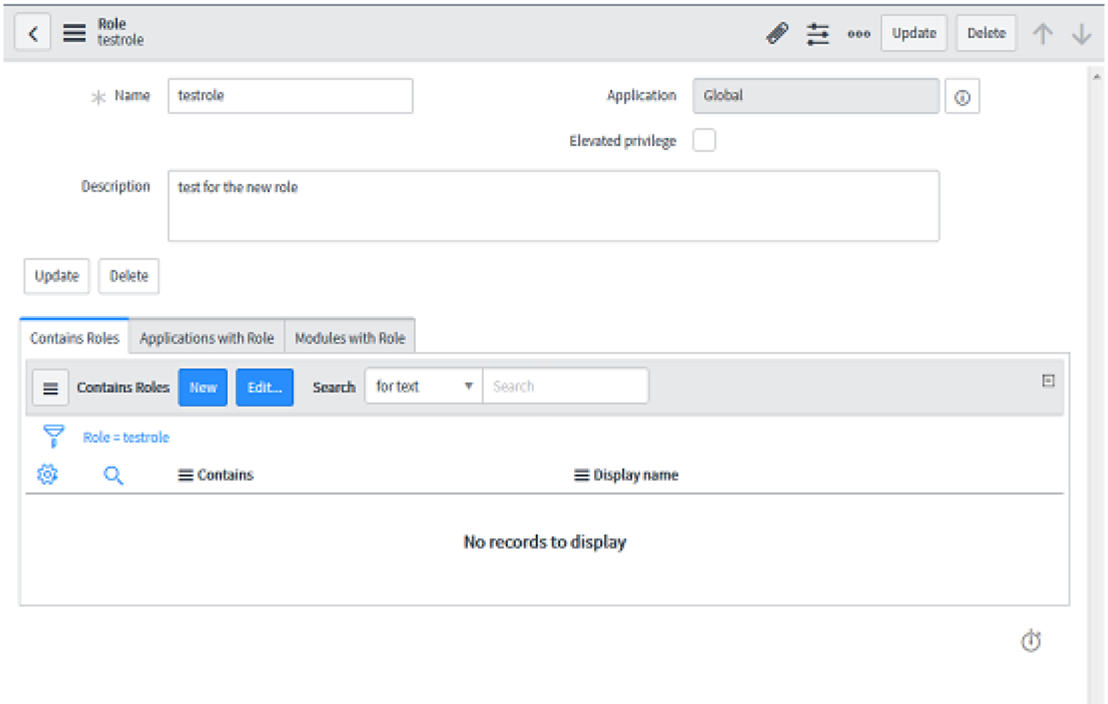
A) Make sure you have a ServiceNow User(other than admin) who have the following roles:

i) ITIL
ii) Rest service
iii) Rest api explorer

Please follow the below steps for assigning the roles for the role.

1. Log in as admin in ServiceNow instance.
2. Click on System Administrator ->Elevates role->check the security_admin check box ->OK.
3. Search for **Roles** in Filter Navigator in Left Side.

4. Click on **Roles** under User Administration.
5. Click on NEW (Blue)Button
6. Provide the name of the role in name field
7. Application field must contains the global scope.
8. Provide the description if require.
9. Click on submit button.
10. Select **Name** from **Go to** select list and provide the **role name** in search box and press enter button.
11. Click on your created role.
12. Select **Contains Roles** tab.
13. Click on **Edit** (Blue) Button.
14. Search **itil** role in Collection list, select **itil** role and click on Add arrow (>).
15. Do the step 14 for the roles **rest_api_explorer** and **rest_service**.
16. Click on save button. (Check Figure 1 for your reference.)



Role
testrole

Name: testrole

Application: Global

Elevated privilege: □

Description: test for the new role

Contains Roles

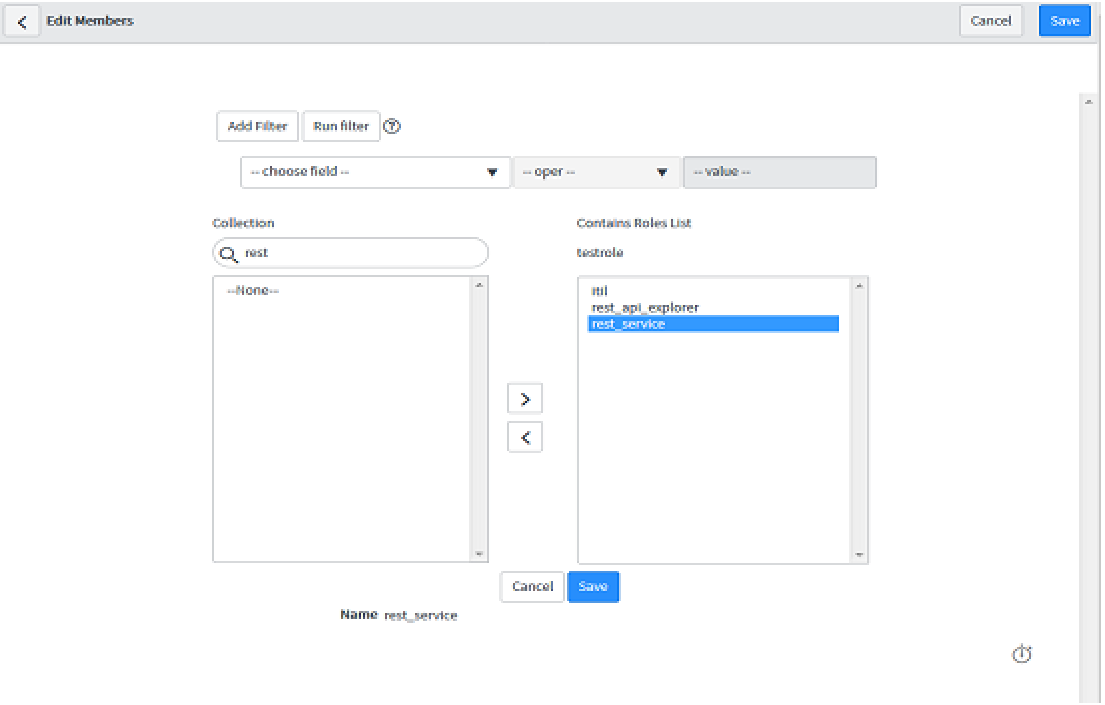
Role = testrole

Contains	Display name

No records to display

Figure 1

For assigning the role click on edit button of the Contains Role tab (Figure 2**).**



Collection: rest

--None--

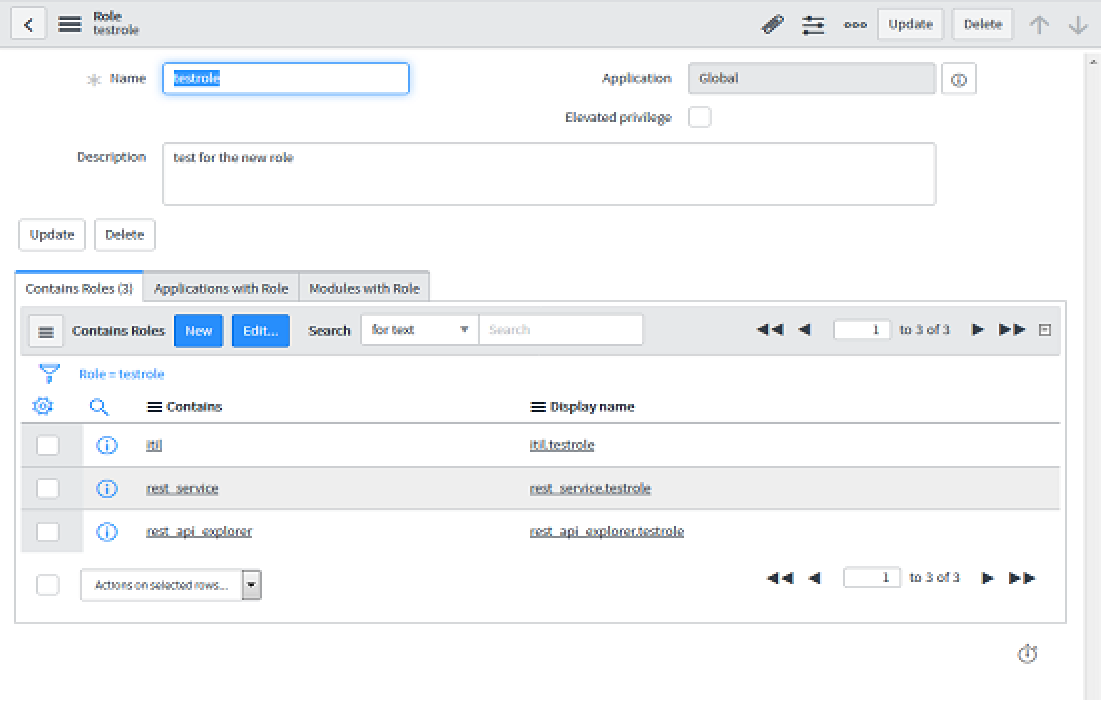
Contains Roles List: testrole

itil
rest_api_explorer
rest_service

Name rest_service

Figure 2

After click on the save you will see the below roles under role (Figure 3)**.**



Name: testrole

Application: Global

Elevated privilege: □

Description: test for the new role

Role = testrole

Contains	Display name
itil	itil.testrole
rest_service	rest_service.testrole
rest_api_explorer	rest_api_explorer.testrole

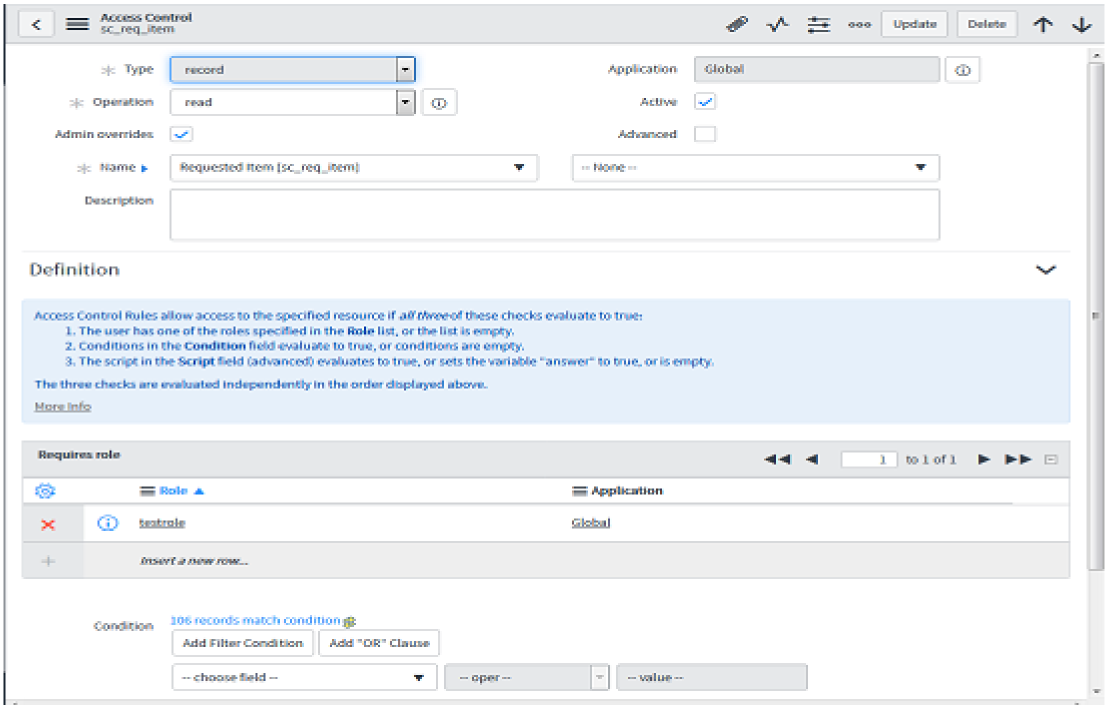
Figure 3

B) To run the ServiceNow connector app make sure that current user role having the following access control list entry and to create access control to newly created role please follow the below steps.

i) Table level read ACL for table “**sc_req_item**” for current user.
ii) Field level write ACL for table “**incident.company”** for current user.
iii) Field level read ACL (for all fields use *) for table “**sys_user_has_role”**.
iv) Row level (Table level) ACL for **“kb_knowledge”** table.

i) Please follow the steps for creating the table level ACL for sc_req_item.

1) Login to ServiceNow instance with Admin role.
2) Click on System Administrator ->Elevates role->check the security_admin check box ->OK.
3) Search for ACL in Filter Navigator in Left Side.
4) Click on **Access Control (ACL)**
5) Click on **NEW** button
6) Select Operation as read.
7) Select the table “**Requested Item [sc_req_item]”** from the name field.
8) Don’t select any column from the Field (remain it as none).
9) Double click on “**Insert a new row...*”*** of **Requires role** section and search your created new role from the list of roles.
10) Select your role and click on check mark.
11) Click on submit and after that click on continue button. Please see the Figure 4,



Type: record

Operation: read

Admin overrides: ☑

Application: Global

Active: ☑

Advanced: □

Name: Requested Item [sc_req_item] | -- None --

Description:

Definition

Access Control Rules allow access to the specified resource if *all three* of these checks evaluate to true:

1. The user has one of the roles specified in the **Role** list, or the list is empty.
2. Conditions in the **Condition** field evaluate to true, or conditions are empty.
3. The script in the **Script** field (advanced) evaluates to true, or sets the variable "answer" to true, or is empty.

The three checks are evaluated independently in the order displayed above.

More info

Requires role — 1 to 1 of 1

Role	Application
testrole	Global
Insert a new row...	

Condition: 106 records match condition

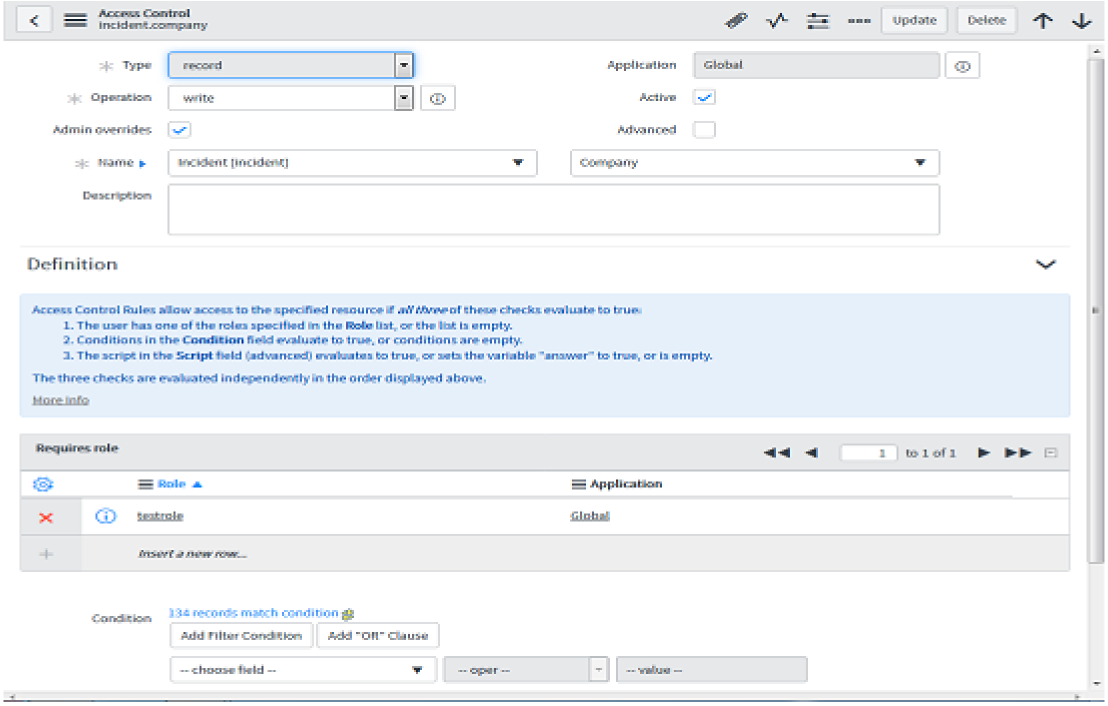
Add Filter Condition | Add "OR" Clause

-- choose field -- | -- oper -- | -- value --

Figure 4

ii) Please follow the steps for creating the Field level write ACL for table “incident”.

1. Login to ServiceNow instance with Admin role.
2. Click on System Administrator ->Elevates role->check the security_admin check box ->OK.
3. Search for ACL in Filter Navigator in Left Side.
4. Click on **Access Control (ACL)**
5. Click on **NEW**
6. Select **Operation** as “**write”**.
7. Select the table name “**Incident [incident]**” from the name field.
8. Select the column name “**Company**” from the “**Fields**” section.
9. Double click on “**Insert a new row...**” of **Requires role** section and search your created new role from the list of roles.
10. Select your role and click on check mark.
11. Click on submit and after that click on continue button. Please see the Figure 5.



Type	record	Application	Global
Operation	write	Active	☑
Admin overrides	☑	Advanced	□
Name	incident [incident]	Company	
Description			

Definition

Access Control Rules allow access to the specified resource if *all three* of these checks evaluate to true:

1. The user has one of the roles specified in the **Role** list, or the list is empty.
2. Conditions in the **Condition** field evaluate to true, or conditions are empty.
3. The script in the **Script** field (advanced) evaluates to true, or sets the variable "answer" to true, or is empty.

The three checks are evaluated independently in the order displayed above.

More info

Requires role — 1 to 1 of 1

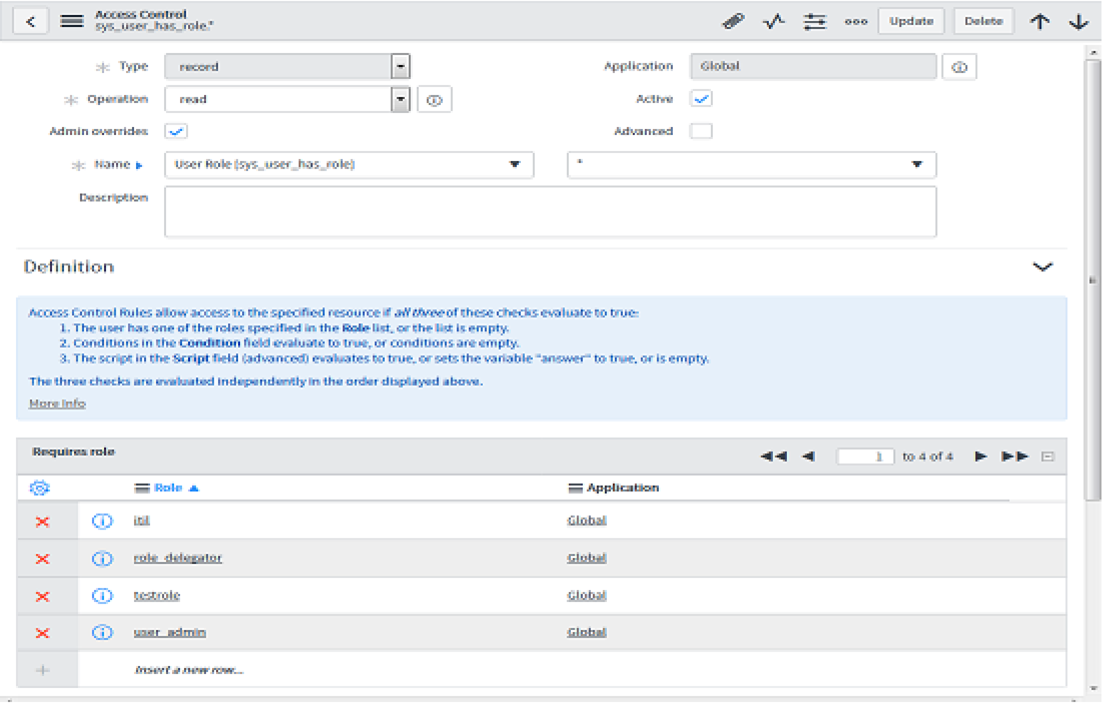
Role	Application
testrole	Global
Insert a new row...	

Condition: 134 records match condition

Figure 5

iii) Please follow the steps for creating the Field level read ACL (for all fields use *) for table sys_user_has_role.

1. Login to ServiceNow instance with Admin role.
2. Click on System Administrator ->Elevates role->check the security_admin check box ->OK.
3. Search for ACL in Filter Navigator in Left Side.
4. Click on **Access Control (ACL)**
5. Click on **NEW**
6. Select Operation as read.
7. Select the table name "**User Role [sys_user_has_role]**" from the name field.
8. Select the column name as * from the Field section (for all fields use *).
9. Double click on "**Insert a new row...**" of **Requires role** section and search your created new role from the list of roles.
10. Select your role and click on check mark.
11. Click on submit and after that click on continue button. Please see the Figure 6,



Type: record

Operation: read

Admin overrides: ☑

Name: User Role (sys_user_has_role) | *

Description:

Application: Global

Active: ☑

Advanced: □

Definition

Access Control Rules allow access to the specified resource if *all three* of these checks evaluate to true:

1. The user has one of the roles specified in the **Role** list, or the list is empty.
2. Conditions in the **Condition** field evaluate to true, or conditions are empty.
3. The script in the **Script** field (advanced) evaluates to true, or sets the variable "answer" to true, or is empty.

The three checks are evaluated independently in the order displayed above.

More info

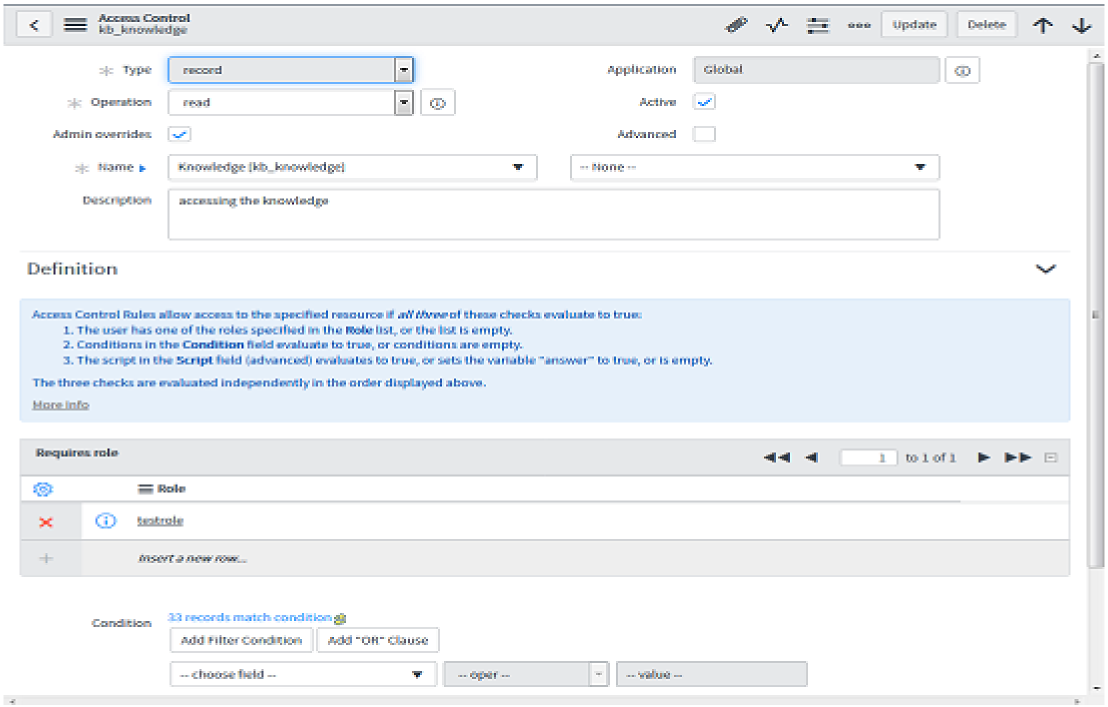
Requires role — 1 to 4 of 4

Role ▲	Application
itil	Global
role_delegator	Global
testrole	Global
user_admin	Global
Insert a new row...	

Figure 6

iv) Please follow the steps for creating the row level read ACL for table kb_knowledge.

1. Login to ServiceNow instance with Admin role.
2. Click on System Administrator ->Elevates role->check the security_admin check box ->OK.
3. Search for ACL in Filter Navigator in Left Side.
4. Click on **Access Control (ACL)**
5. Click on **NEW**
6. Select Operation as read.
7. Select the table name “**Knowledge [kb_knowledge]**” from the name field.
8. Don’t select any column from the Field (remain it as none).
9. Double click on “**Insert a new row...**” of **Requires role** section and search your created new role from the list of roles.
10. Select your role and click on check mark.
11. Click on submit and after that click on continue button. Please see the Figure 7,



Access Control
kb_knowledge

Type: record
Operation: read
Admin overrides: ☑
Name: Knowledge [kb_knowledge] | -- None --
Description: accessing the knowledge
Application: Global
Active: ☑
Advanced: □

Definition

Access Control Rules allow access to the specified resource if *all three* of these checks evaluate to true:

1. The user has one of the roles specified in the **Role** list, or the list is empty.
2. Conditions in the **Condition** field evaluate to true, or conditions are empty.
3. The script in the **Script** field (advanced) evaluates to true, or sets the variable "answer" to true, or is empty.

The three checks are evaluated independently in the order displayed above.

Requires role — 1 to 1 of 1

Role
testrole

Condition: 33 records match condition
-- choose field -- | -- oper -- | -- value --

Figure 7

As we have completed Section "C" already please go to step 5

C) Create OAuth 2.0 server in ServiceNow for end points

For providing the token based authentication we need to create OAuth 2.0 server in ServiceNow. The following steps are required to create an endpoints for clients to access the instance.

Before you begin we required role: admin

Procedure

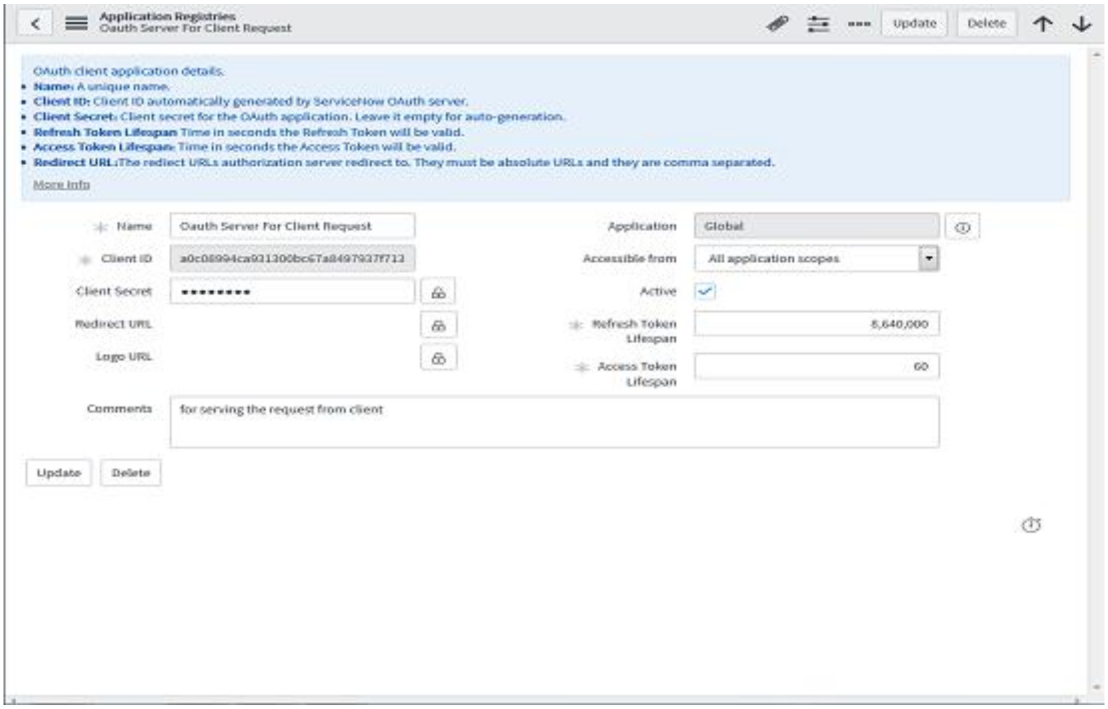
1. Login as an Admin
2. Search for "**application registry"** in Filter Navigator in Left Side.
3. Click on New button in application registry for creating new OAuth server.
4. On the interceptor page, click create an "**OAuth API endpoint for external clients"** and then fill in the form.

Field	**Description**
Name	A unique name that identifies the application that you require OAuth access for.

Client ID	[Read-Only] The auto-generated unique ID of the application. The instance uses the client ID when requesting an access token.
Client Secret	[Required] The shared secret string that both the instance and the client application or website use to authorize communications with one another. The instance uses the client secret when requesting an access token. Leave this field blank to have the instance auto-generate a client secret. To display existing client secrets, click the lock icon. For example, client Secret= test.
Redirect URL	[Optional] The *callback URL* that the authorization server redirects to. Enter the full URLs of the clients requesting access to the resource, appended by /oauth_redirect.do. For example, http://token_consumer:port/oauth_redirect.do. Enter as many URLs as needed for all possible token consumers. The instance matches the URL of the incoming request to one of the redirect URLs. If no match is made, the instance uses the first redirect URL.
Logo URL	[Optional] The URL that contains an image to use as the application logo. The logo appears on the approval page when the user receives a request to grant a client application access to a restricted resource on the instance.
Active	[Optional] Select the check box to make the application registry active.
Refresh Token Lifespan	[Optional] The number of seconds that a refresh token is valid. The instance uses the lifespan value when requesting a refresh token. By default, refresh tokens expire in 100 days (8640000 seconds).
Access Token Lifespan	[Optional] The number of seconds that an access token is valid. The instance uses the lifespan value when requesting an access token. By default, access tokens expire in 30 minutes (1800 seconds).
Comments	[Optional] Additional information to associate with the application.

5. Click Submit. The record is saved in the Application Registries [oauth_entity] table.

Please see the following entry in Figure 8



Application Registries
Oauth Server For Client Request

OAuth client application details.

- **Name:** A unique name.
- **Client ID:** Client ID automatically generated by ServiceNow OAuth server.
- **Client Secret:** Client secret for the OAuth application. Leave it empty for auto-generation.
- **Refresh Token Lifespan** Time in seconds the Refresh Token will be valid.
- **Access Token Lifespan:** Time in seconds the Access Token will be valid.
- **Redirect URL:**The rediect URLs authorization server redirect to. They must be absolute URLs and they are comma separated.

Name	Oauth Server For Client Request	Application	Global
Client ID	a0c08994ca931300bc67a8497937f713	Accessible from	All application scopes
Client Secret	••••••••	Active	☑
Redirect URL		Refresh Token Lifespan	8,640,000
Logo URL		Access Token Lifespan	60
Comments	for serving the request from client		

Figure 8

6. After creating the authentication server for the end points, please enter the application main **URL**, **client id** and **client secret** into the portal-ext.properties. (If portal-ext.properties file is not exist then create new portal-ext.properties file in liferay home location)
    1. servicenow.api={base-url of servicenow instance}
       (e.g. https://devsomenumber.service-now.com)
    2. snow.auth.oauth.clientid= your app client id
    3. snow.auth.oauth.clientsecret= your app client secret
    4. servicenow.authanticationtype = provide your authentication type(either BasicSecurity or Auth2.0)

Please go to step 3.

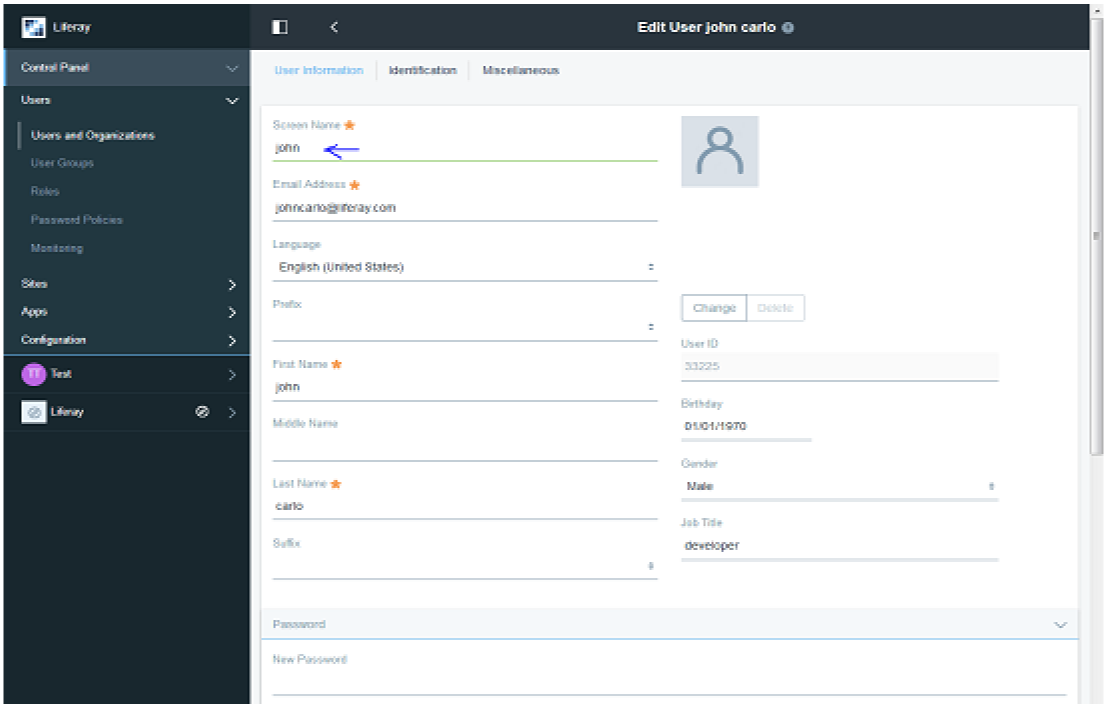
Step 5.

Creating the user account in ServiceNow incident.
The account must have same **user id** as **screen name** in liferay account. Assign your newly created role which is containing the roles like **itil, rest service, rest API explorer**.

Note: User id (ServiceNow) **=** Screenname (Liferay)

Please see the Figure 9 for reference,

We have created one user with screen name = “**john”** in liferay and in the following second images we are creating the service now user account with user id = “**john**” only. After that we are assigning the role for that newly created ServiceNow user.



Edit User john carlo

Screen Name * john
Email Address * johncarlo@liferay.com
Language English (United States)
Prefix
First Name * john
Middle Name
Last Name * carlo
Suffix
User ID 33225
Birthday 01/01/1970
Gender Male
Job Title developer
New Password

Figure 9

For creating the account in ServiceNow please follow the below steps,

1. Search for “**Users**” in “**Filter Navigator”** in Left Side.
2. Click on “Users” which are under the “**Organization”**.
3. Click on the **New** (with blue colour) button.
4. Please enter the liferay screen name of user account which you are going to sync with ServiceNow. To get the liferay screen name please follow the below steps,

   4.1 Log in with your credentials in liferay portal.

   4.2 Click on the menu icon ◧

   4.3 Click on User Name tab.

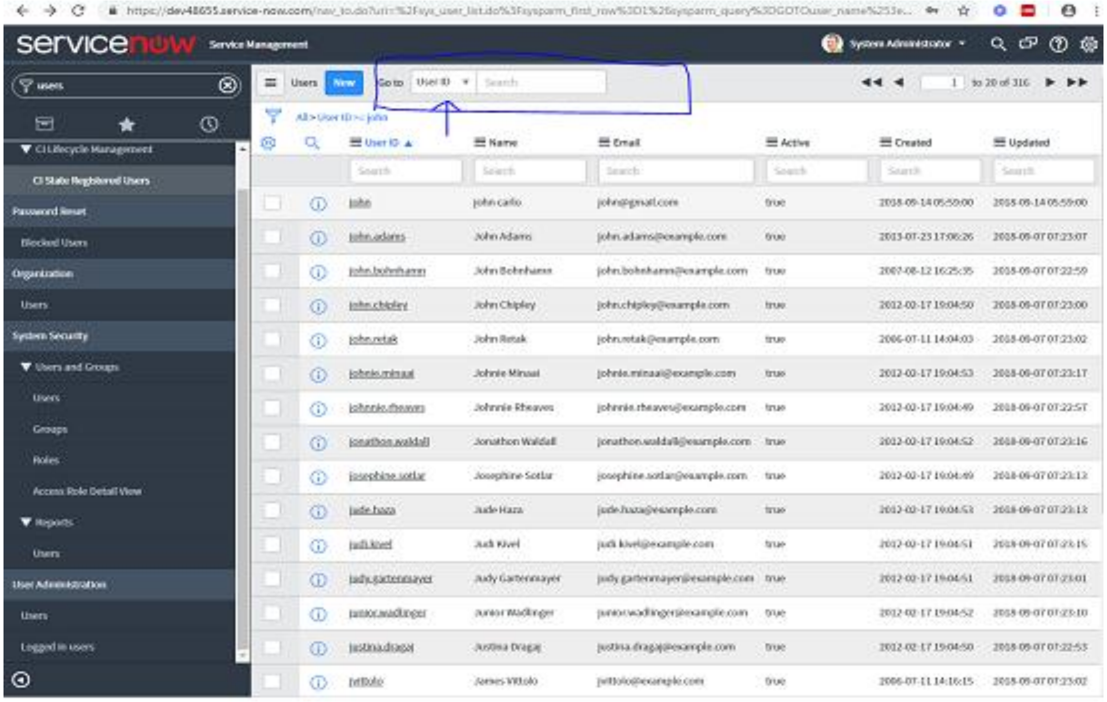
   4.4 Click on Account Settings.

   4.5 Copy the Screen Name field value from the form and paste into the user id field of the ServiceNow user account form.

5. Insert the necessary information and provide the password for this account (this password is further need to be insert into the **portlet preferences** in liferay for the first time login) click on the submit button.

Now user is created and you need to assign role which you have created in **Step 4**.

6. After submitting the new user, select user id from **Go to** select list which is shown below.

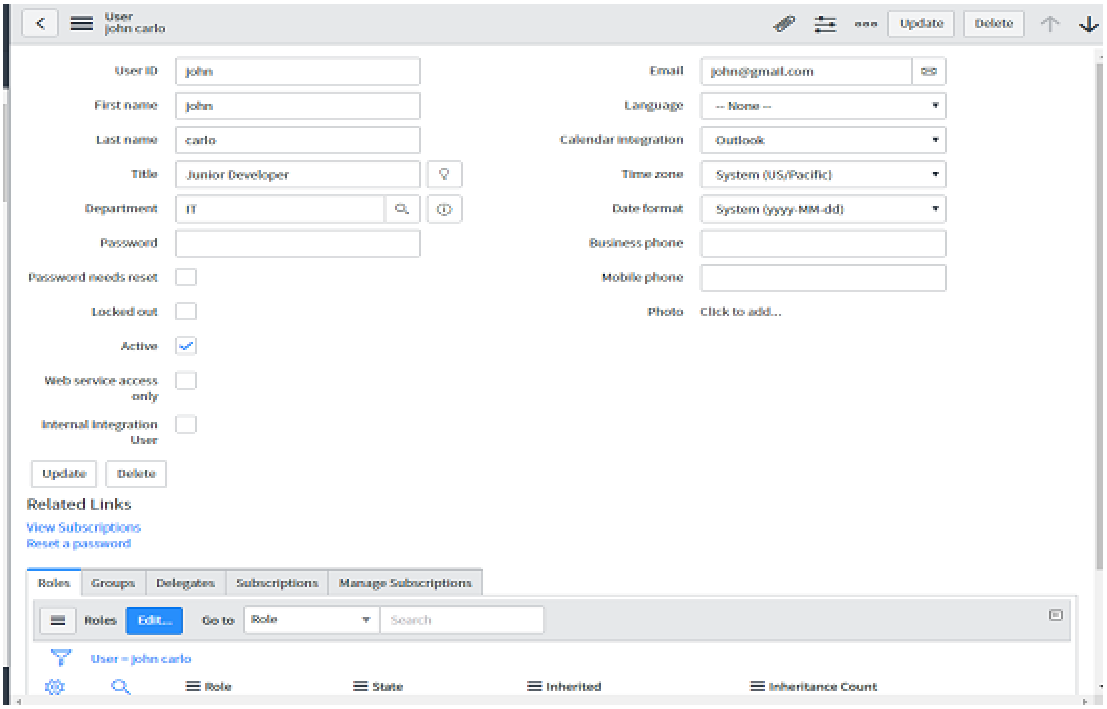


User ID ▲	Name	Email	Active	Created	Updated
john	john carlo	john@gmail.com	true	2018-09-14 05:59:00	2018-09-14 05:59:00
john.adams	John Adams	john.adams@example.com	true	2013-07-23 17:06:26	2018-09-07 07:23:07
john.bohnhamm	John Bohnhamm	john.bohnhamm@example.com	true	2007-08-12 16:25:35	2018-09-07 07:22:59
john.chipley	John Chipley	john.chipley@example.com	true	2012-02-17 19:04:50	2018-09-07 07:23:00
john.retak	John Retak	john.retak@example.com	true	2006-07-11 14:04:03	2018-09-07 07:23:02
johnie.minaai	Johnie Minaai	johnie.minaai@example.com	true	2012-02-17 19:04:53	2018-09-07 07:23:17
johnnie.rheaves	Johnnie Rheaves	johnnie.rheaves@example.com	true	2012-02-17 19:04:49	2018-09-07 07:22:57
jonathon.waldall	Jonathon Waldall	jonathon.waldall@example.com	true	2012-02-17 19:04:52	2018-09-07 07:23:16
josephine.sotlar	Josephine Sotlar	josephine.sotlar@example.com	true	2012-02-17 19:04:49	2018-09-07 07:23:13
jude.haza	Jude Haza	jude.haza@example.com	true	2012-02-17 19:04:53	2018-09-07 07:23:13
judi.kivel	Judi Kivel	judi.kivel@example.com	true	2012-02-17 19:04:51	2018-09-07 07:23:15
judy.gartenmayer	Judy Gartenmayer	judy.gartenmayer@example.com	true	2012-02-17 19:04:51	2018-09-07 07:23:01
junior.wadlinger	Junior Wadlinger	junior.wadlinger@example.com	true	2012-02-17 19:04:52	2018-09-07 07:23:10
justina.dragaj	Justina Dragaj	justina.dragaj@example.com	true	2012-02-17 19:04:50	2018-09-07 07:22:53
jvittolo	James Vittolo	jvittolo@example.com	true	2006-07-11 14:16:15	2018-09-07 07:23:02

Figure 10

And enter the latest created user id in search box, in our case it is john and hit enter button.

7. Select the proper record from shown user records and click on it, after clicking the view nothing but as following,



User ID	john	Email	john@gmail.com
First name	john	Language	-- None --
Last name	carlo	Calendar integration	Outlook
Title	Junior Developer	Time zone	System (US/Pacific)
Department	IT	Date format	System (yyyy-MM-dd)
Password		Business phone	
Password needs reset	☐	Mobile phone	
Locked out	☐	Photo	Click to add...
Active	☑		
Web service access only	☐		
Internal Integration User	☐		

Figure 11

8. Please select the Roles tab from the menu which is located below the related links portion.
9. After selecting the Roles tab please click on the Edit (blue colour) button.
10. Search for the new role you created in **step 4** in collection search box, Please see the Figure 12,

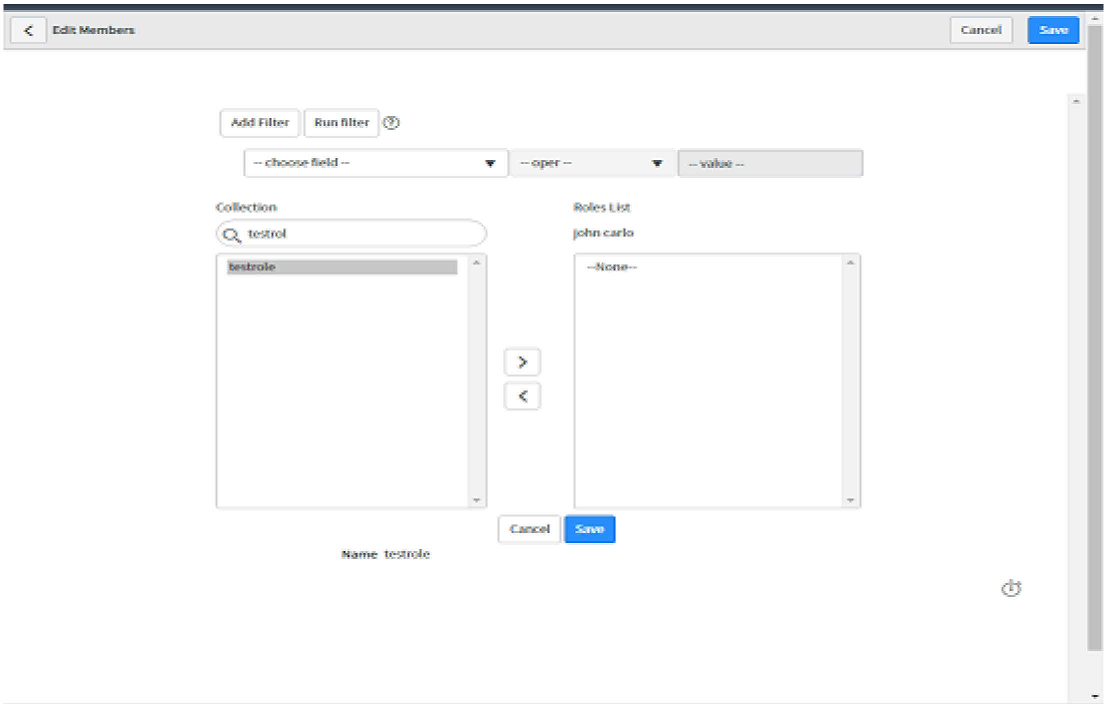


Figure 12

11. Select the role in our case that is nothing but testrole and click on the add button which is denoted by > symbol. Please see the Figure 13,

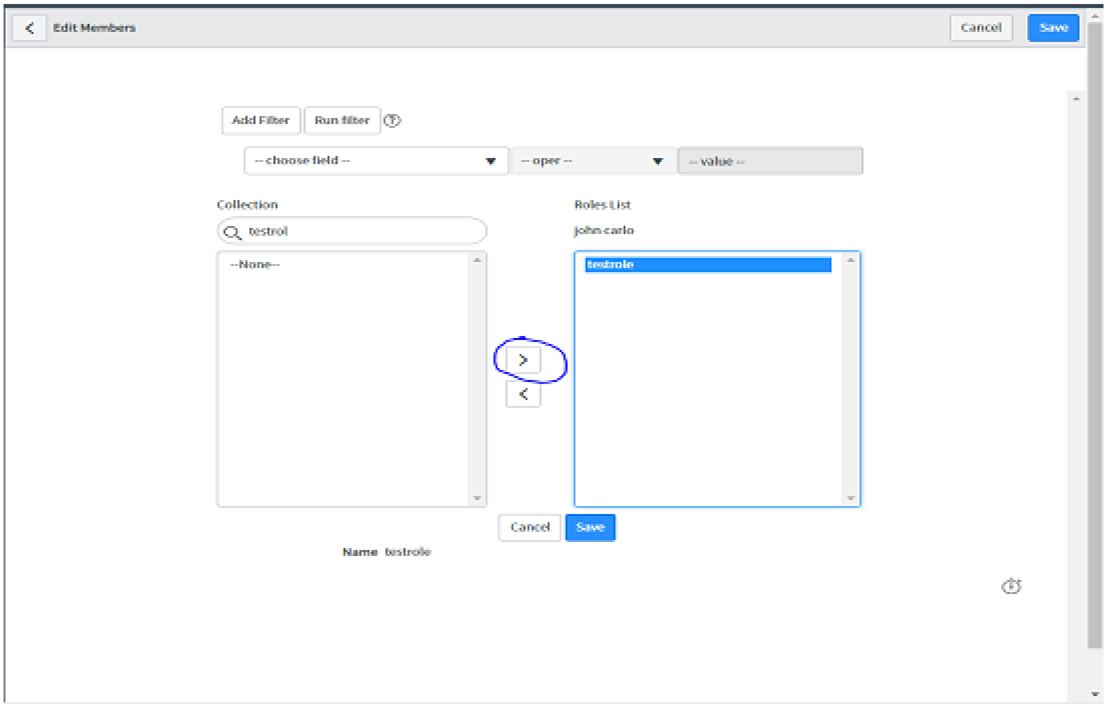
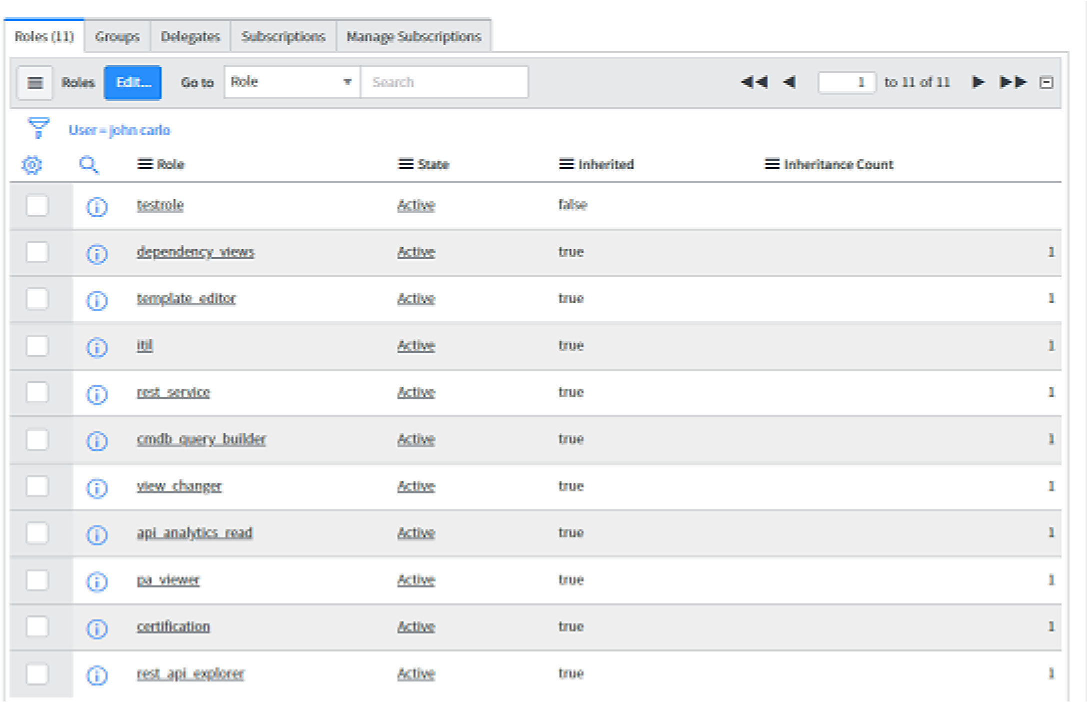


Figure 13

That is going to move your role from left search box in to the role list box for john carlo and click on the save button.
Your newly created user contains list of roles shown below in Figure 14,



User = john carlo

		Role	State	Inherited	Inheritance Count
□	ⓘ	testrole	Active	false	
□	ⓘ	dependency_views	Active	true	1
□	ⓘ	template_editor	Active	true	1
□	ⓘ	itil	Active	true	1
□	ⓘ	rest_service	Active	true	1
□	ⓘ	cmdb_query_builder	Active	true	1
□	ⓘ	view_changer	Active	true	1
□	ⓘ	api_analytics_read	Active	true	1
□	ⓘ	pa_viewer	Active	true	1
□	ⓘ	certification	Active	true	1
□	ⓘ	rest_api_explorer	Active	true	1

Figure 14

Now your user is ready with all the permissions.

Step 6. Liferay Configuration:

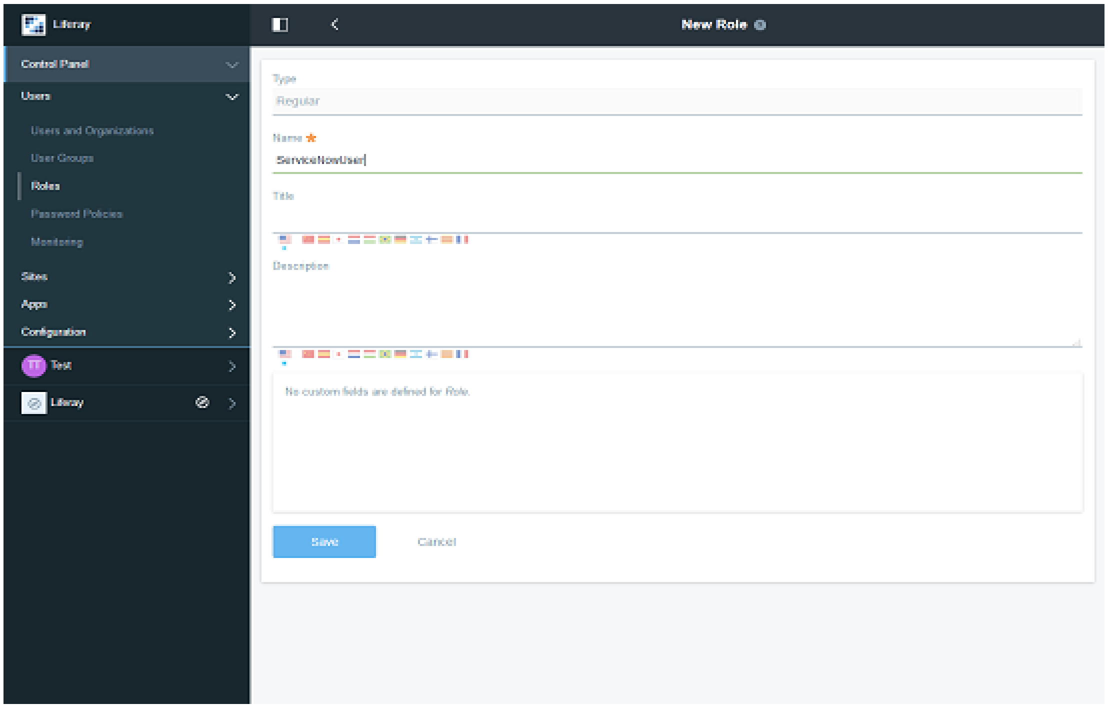
6.1 Restart the Liferay server.

6.2 To make the **Portlet Preferences** available for user we have to assign the particular role to the user. You can select the existing Power User Role or create the custom role and assign it to the Liferay user.

For creating the custom role please see the following steps,
In Liferay portal log in as **admin**,

1. Go to control panel -> click on **Users** tab -> click on **Roles**
2. Click on the + button located at right-bottom-corner (for creating the regular role).
3. After clicking the + button role creation form will be available.

4. Please keep the type field as it is (by default **Regular**) and provide the name for your custom role here we have given the name = ServiceNowUser. The Title, Description, Custom field are optional. Please see the Figure 15,



Type
Regular

Name *
ServiceNowUser

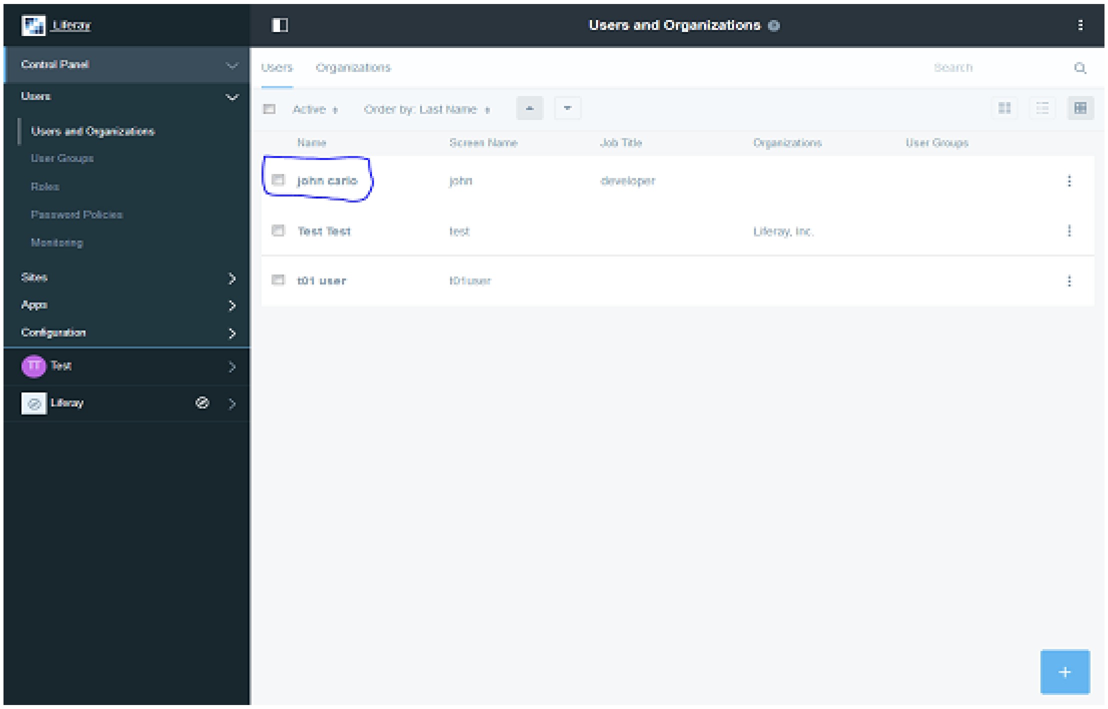
Title

Description

No custom fields are defined for Role.

Figure 15

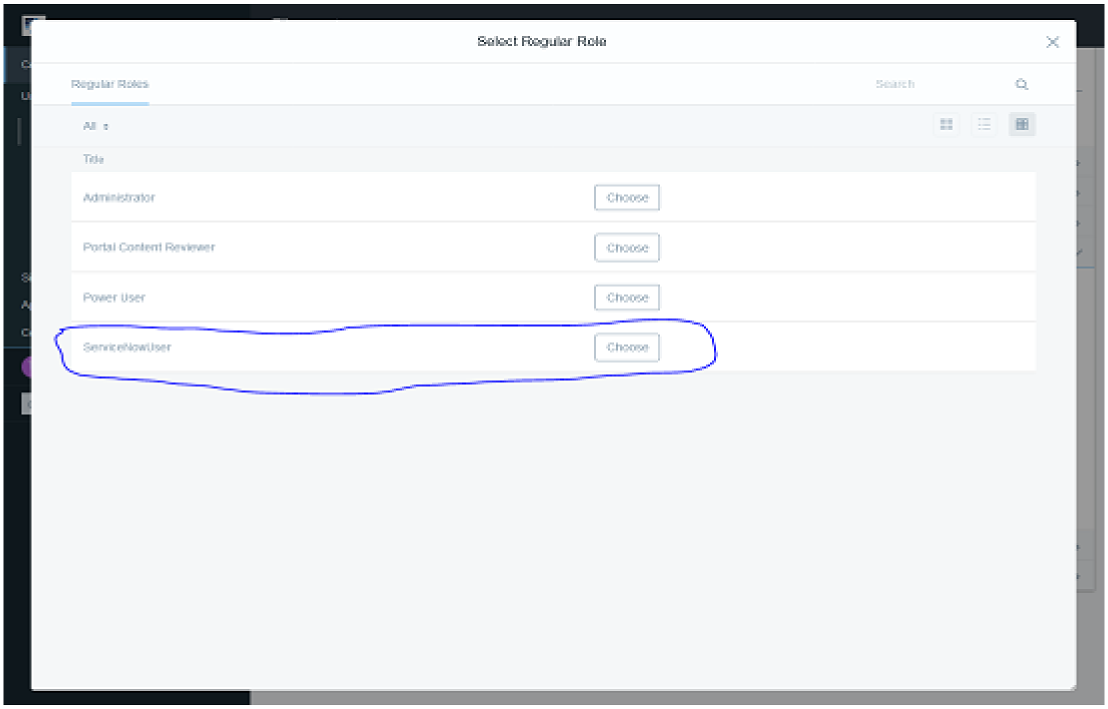
5. Click on the save button.
6. Go to **Control Panel** -> click on **Users** -> click on **Users and Organization** -> click on user account in our case the user account name = john carlo. Please see Figure 16,



Name	Screen Name	Job Title	Organizations	User Groups
john carlo	john	developer		
Test Test	test		Liferay, Inc.	
t01 user	t01user			

Figure 16

7. After clicking the account name scroll the page and you can able to see the **Roles** tab
8. Click on the Roles tab -> click on **Select** button -> choose your custom role or you can select the already existing role e.g. **user**, **power user** by clicking on the choose button front of your custom role name shown in the below Figure 17.



Select Regular Role

Regular Roles

Title	
Administrator	Choose
Portal Content Reviewer	Choose
Power User	Choose
ServiceNowUser	Choose

Figure 17

9. After choosing the role for your account click on the save button.

6.3 Permission for user to use Portlet Preferences:

Note: For **Admin** user in Liferay Portlet Preferences permission is already define by default**.**

6.3.1 Go to **Control Panel** -> **Users** -> **Roles** -> Click on the 3 vertical dots for the role which you have created in **Step 6.2** -> **Define permission**

6.3.2 Now under Summary Click on **Site Administration** -> **Applications** -> select **ServiceNow Dashboard** app -> scroll to the top and check the check box for **Preferences** ->click on save.

Step 7. Once done with all configurations, to find portlet go to add -> **Applications** -> **VilMinds** and add portlet on relevant page.

Step 8. Logout from **Admin** account and Login as the user account.

Note: If your sync user is not default Admin User of Liferay then you need to log out from current account and log In with your account credentials

Step 9. If User is using this portlet for first time then user needs to change password from portlet configuration (click on three vertical dot's available on top right corner of portlet) and go to preferences to change password. Enter your **ServiceNow account password**.

You are ready to use portlet.