GeoServer: User Security

Generally, when you first install GeoServer you will jump straight in…. creating Stores and Layers so that you can start to publish Web Map Services (WMS) as soon as possible. I am sure that many people still do this… and I know this is how I worked with GeoServer in the past.

However, it really should be good practice, instead of using the generic **ADMIN** user, to stop and think a little about better **Security** and **Roles**. This blog provides brief details of how we would recommend you manage your Users and Roles in a production environment for your GeoServer Installation.

In this blog we will perform two main tasks:

1 – Create a **New USER** and **ROLE** to limit the LAYERS, STORES, STYLES that you can see.

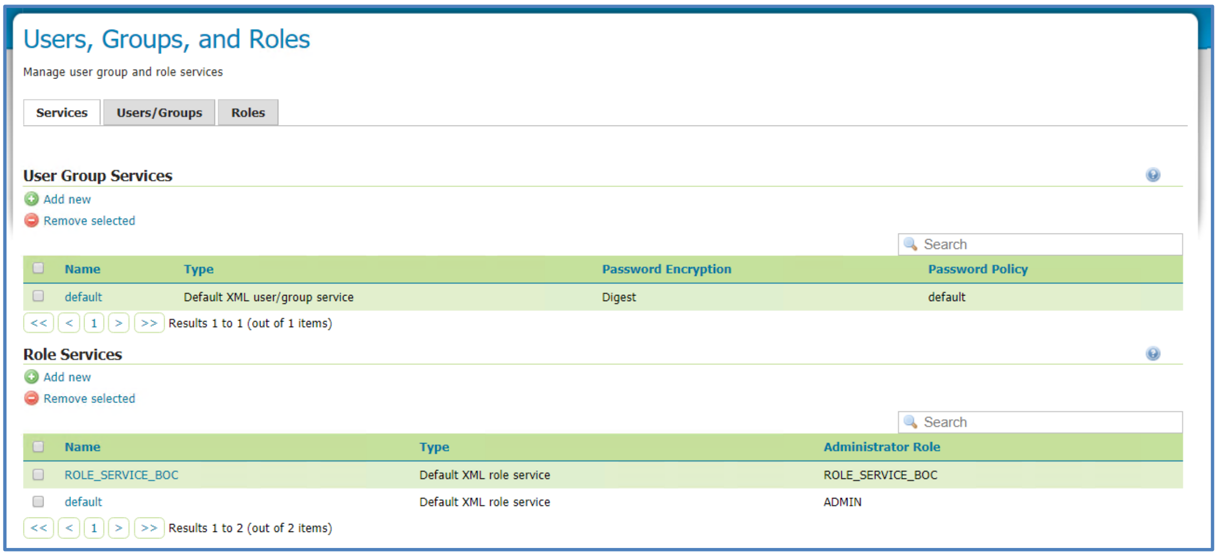
2 – Update the Default **Data Security Rule** so that layers exposed in the Layer Preview are again Role dependent.

This Blog discusses GeoServer Roles and Security with regards to the **GeoServer Admin Pages**. However, once the new Users have been created you can use those logins to manage which of your WMS layers are visible to users via client applications e.g. **QGIS.**

1 – CREATE NEW ROLE:

In order to work with Users in GeoServer you firstly need to define the **ROLE** that the User will have. In this instance we want to restrict the LAYERS, STORES and STYLES that can be accessed by a User in GeoServer to only one individual WORKSPACE. We have called this **Workspace – BOC.**

In the **Security** Pane, choose > **Users, Groups, Roles** > and in the **Role Services** select the ***Default*** record.



Users, Groups, and Roles

Manage user group and role services

User Group Services

□	Name	Type	Password Encryption	Password Policy
□	default	Default XML user/group service	Digest	default

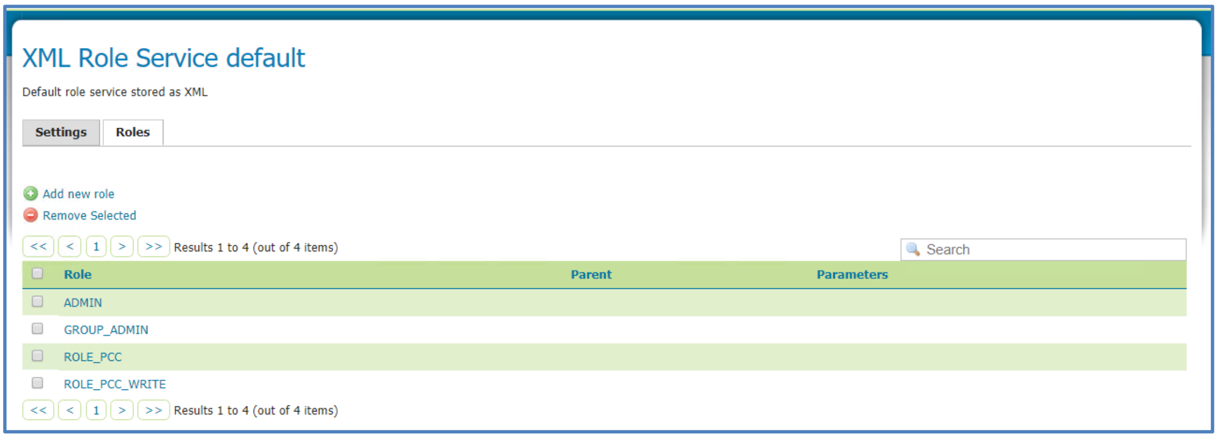
<< < 1 > >> Results 1 to 1 (out of 1 items)

Role Services

□	Name	Type	Administrator Role
□	ROLE_SERVICE_BOC	Default XML role service	ROLE_SERVICE_BOC
□	default	Default XML role service	ADMIN

<< < 1 > >> Results 1 to 2 (out of 2 items)

In the **XML Role Services Default** page, choose the **ROLES** tab.



XML Role Service default

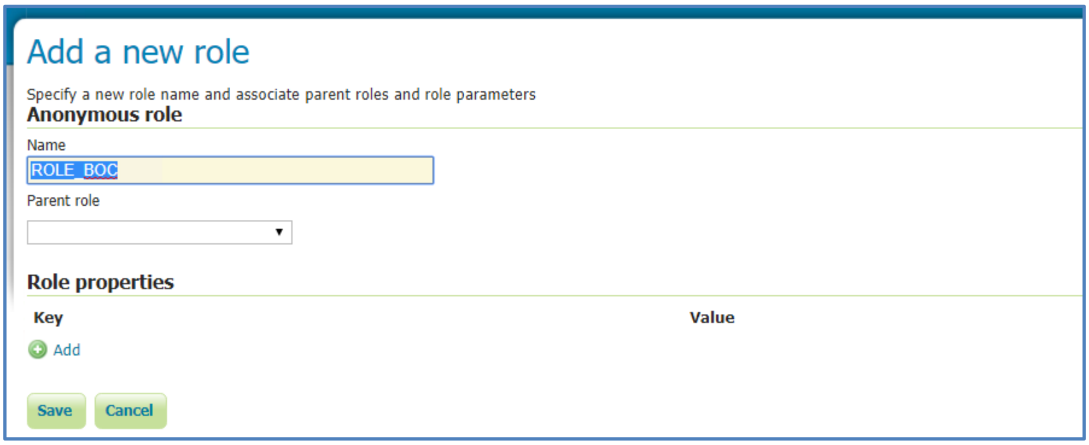
Default role service stored as XML

Results 1 to 4 (out of 4 items)

□	Role	Parent	Parameters
□	ADMIN		
□	GROUP_ADMIN		
□	ROLE_PCC		
□	ROLE_PCC_WRITE		

Results 1 to 4 (out of 4 items)

Now choose **Add New Role**, provide a suitable Role Name e.g. **ROLE_BOC** and then press **Save**.



Add a new role

Specify a new role name and associate parent roles and role parameters

Anonymous role

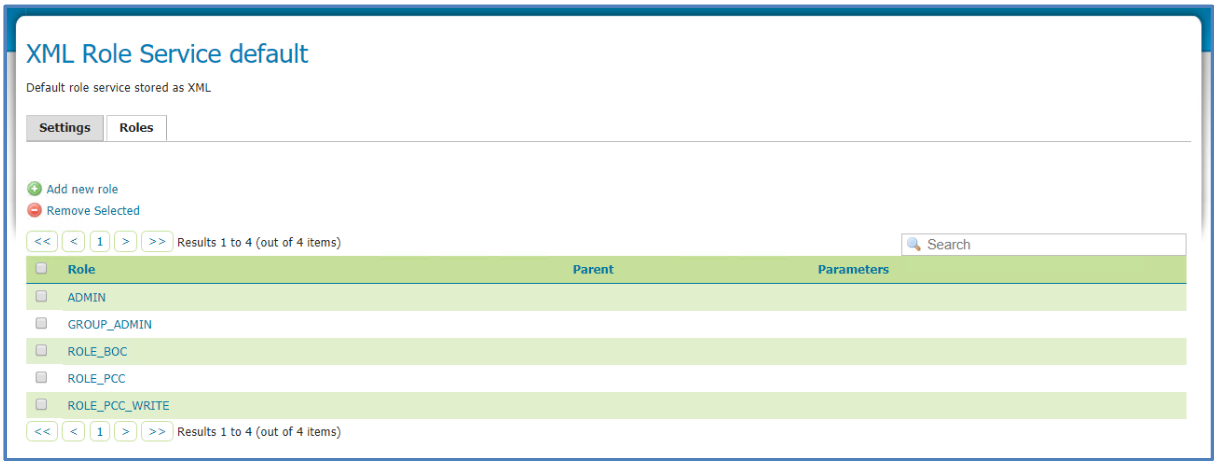
Name: ROLE_BOC

Parent role:

Role properties

Key	Value

The new ROLE (ROLE_BOC) will be added to the Role List.



XML Role Service default

Default role service stored as XML

Results 1 to 4 (out of 4 items)

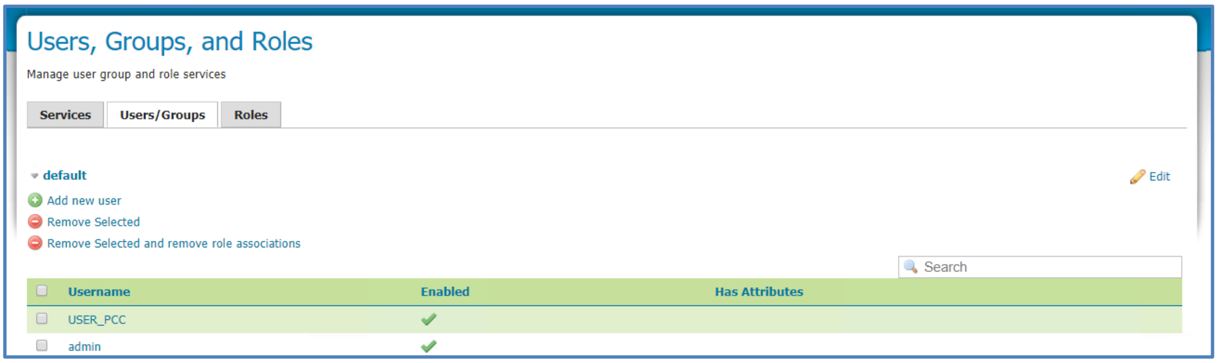
□	Role	Parent	Parameters
□	ADMIN		
□	GROUP_ADMIN		
□	ROLE_BOC		
□	ROLE_PCC		
□	ROLE_PCC_WRITE		

Results 1 to 4 (out of 4 items)

2 – CREATE NEW USER:

Now that we have created a new Role, we can create a New User to associate to that Role.

In the **Security** Pane, choose > **Users, Groups, Roles** > and in the **Users/Groups** tab choose **Add New User**.

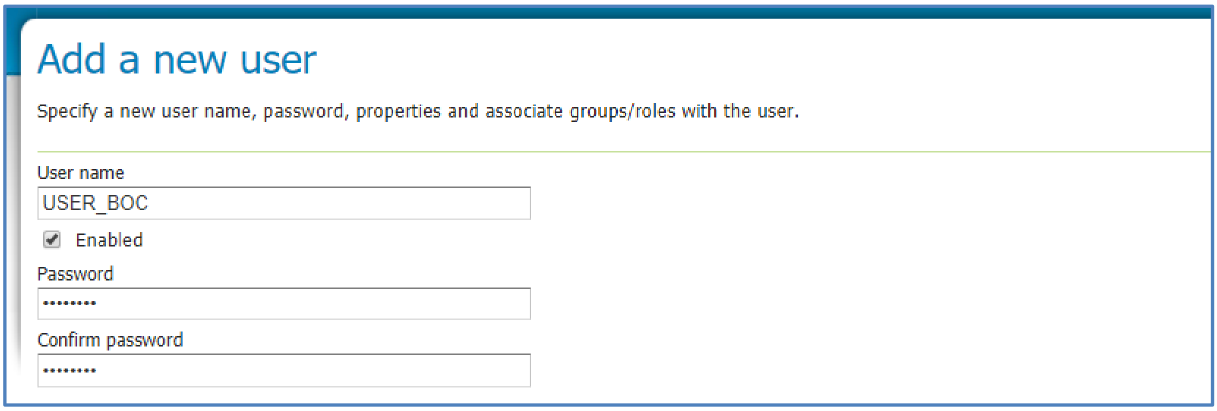


Users, Groups, and Roles

Manage user group and role services

□	Username	Enabled	Has Attributes
□	USER_PCC	✓	
□	admin	✓	

In the **Add a New User** window, provide a User_Name e.g. **USER_BOC** and define a **password.**



Add a new user

Specify a new user name, password, properties and associate groups/roles with the user.

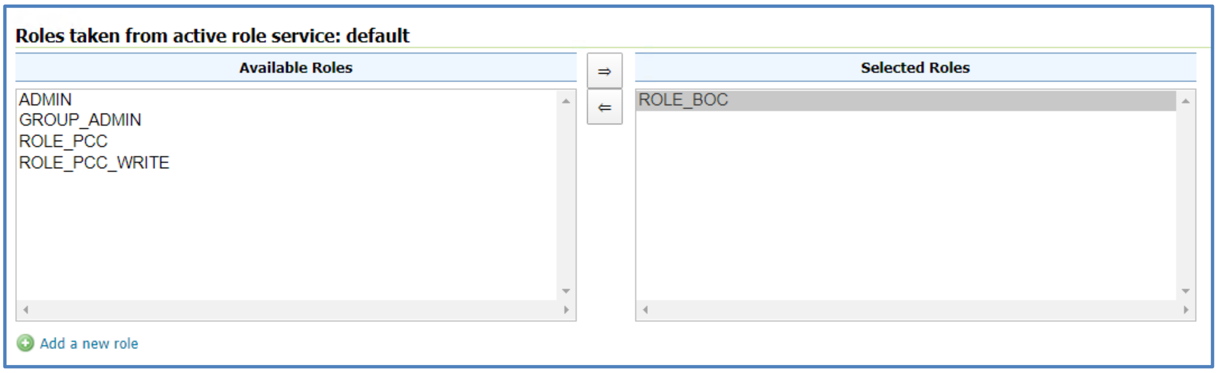
User name: USER_BOC

☑ Enabled

Password: ••••••••

Confirm password: ••••••••

In the bottom half of the page choose the **ROLE** to be associated with the new User. Here you should select the **ROLE_BOC** record and use the **Right Arrow** to move the Role to the **Selected Roles** pane.



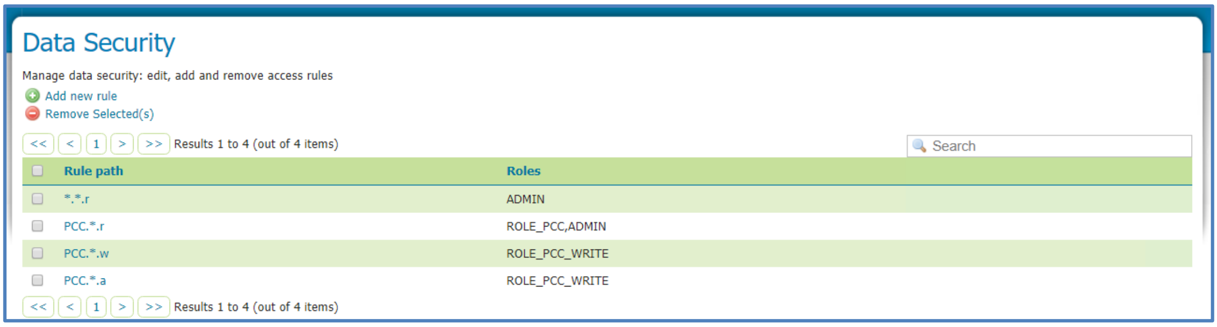
Roles taken from active role service: default

Available Roles	Selected Roles
ADMIN	ROLE_BOC
GROUP_ADMIN	
ROLE_PCC	
ROLE_PCC_WRITE	

3 – DATA SECURITY

Now that we have created a new Role and new User, we need to define the **Data Security** for that ROLE. This will enable you to create and edit RULES that define the Workspaces that ROLES can see and their **Actions** associated to that Workspace e.g. Read, Write or Admin. These permissions are not only important for a GeoServer Web Admin User, but the Security will also determine which WMS layers can be seen in a client application such as QGIS or WebGIS.

In the **Security** Pane, choose > the **Data** menu and the Data Security page opens.



Data Security

Manage data security: edit, add and remove access rules

Add new rule

Remove Selected(s)

<< < 1 > >> Results 1 to 4 (out of 4 items)

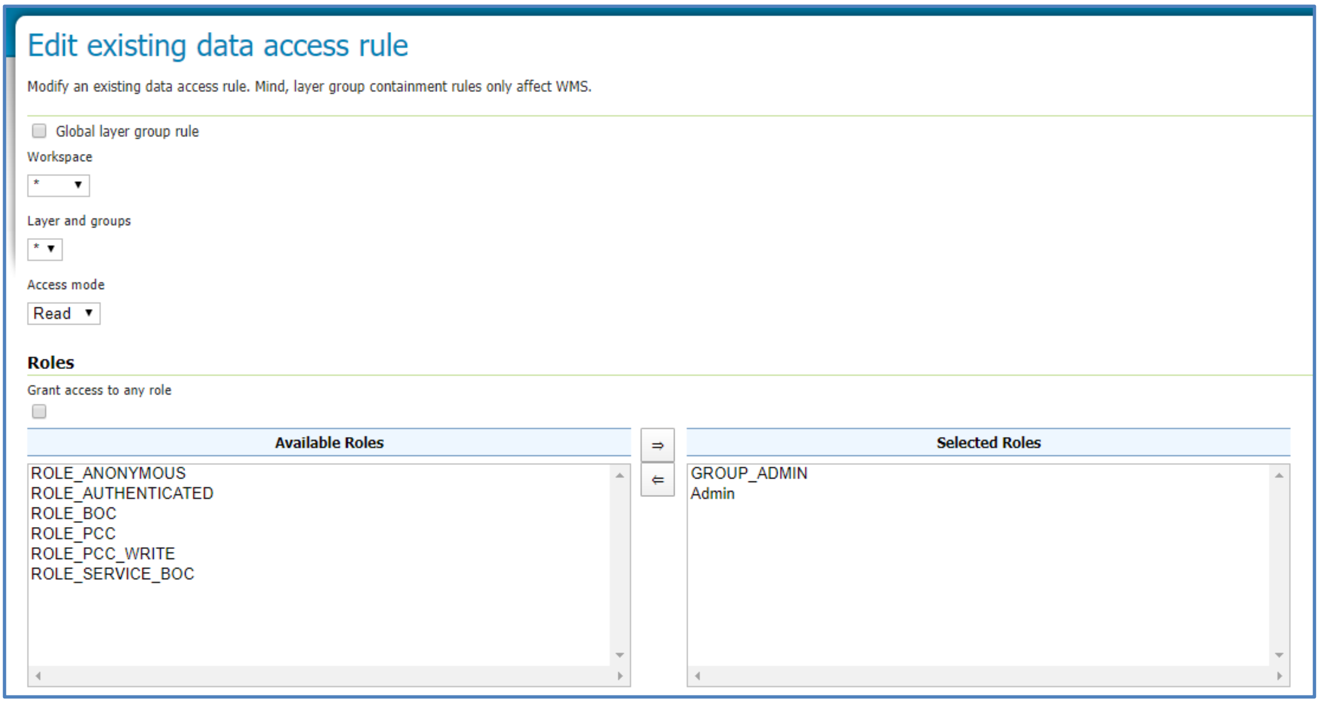
□	Rule path	Roles
□	*.*.r	ADMIN
□	PCC.*.r	ROLE_PCC,ADMIN
□	PCC.*.w	ROLE_PCC_WRITE
□	PCC.*.a	ROLE_PCC_WRITE

<< < 1 > >> Results 1 to 4 (out of 4 items)

3.1 DATA SECURITY - ADMIN:

There will already be a RULE defined in GeoServer called ***.*.r.** This Rule is pre-set so that the ADMIN Role can view ALL **(*)** Workspaces, Layers, Groups, Styles etc…

So, if you wish to restrict the viewing of records per ROLE, choose to **edit** the *.*.r rule and check that only **ADMIN** and Group_Admin are listed in the **selected Role** for this Rule.



Edit existing data access rule

Modify an existing data access rule. Mind, layer group containment rules only affect WMS.

□ Global layer group rule

Workspace: *

Layer and groups: *

Access mode: Read

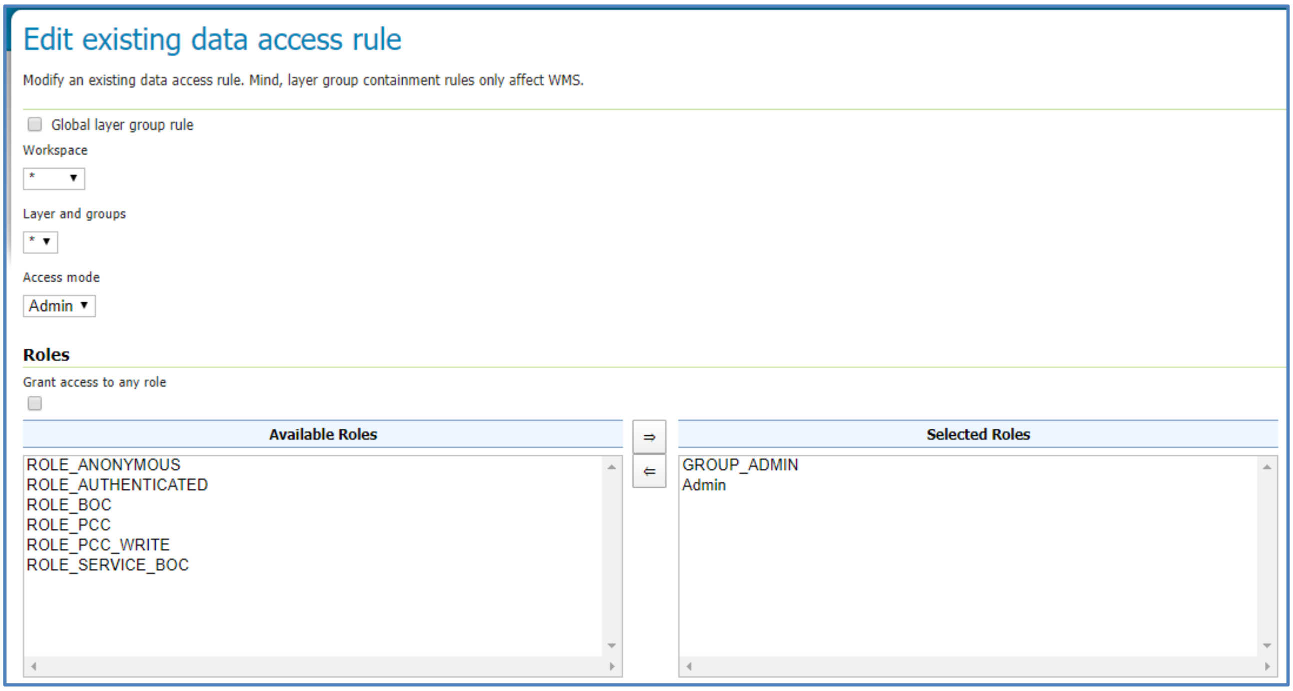
Roles

Grant access to any role □

Available Roles	Selected Roles
ROLE_ANONYMOUS ROLE_AUTHENTICATED ROLE_BOC ROLE_PCC ROLE_PCC_WRITE ROLE_SERVICE_BOC	GROUP_ADMIN Admin

Repeat this for the WRITE and ADMIN Rules so that the ADMIN user has rights to all Workspaces, Layers and Stores.

Admin Access:



Edit existing data access rule

Modify an existing data access rule. Mind, layer group containment rules only affect WMS.

☐ Global layer group rule

Workspace: *

Layer and groups: *

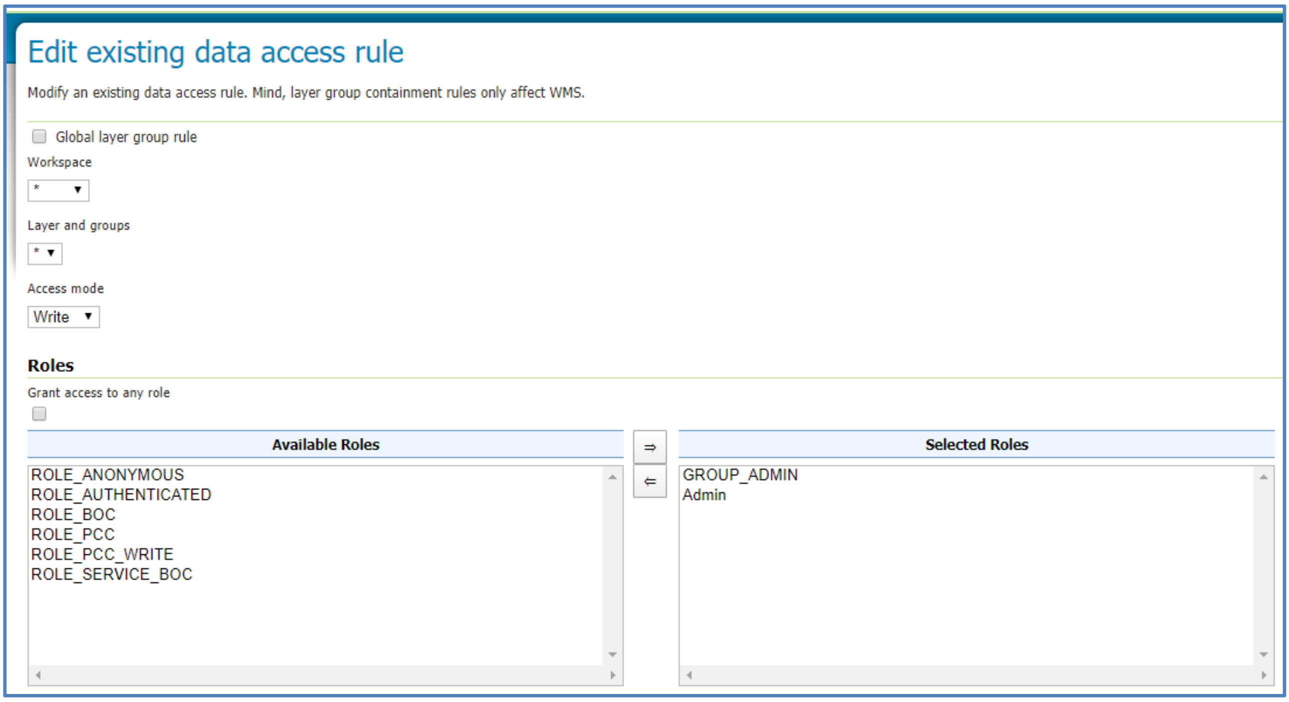
Access mode: Admin

Roles

Grant access to any role ☐

Available Roles	Selected Roles
ROLE_ANONYMOUS ROLE_AUTHENTICATED ROLE_BOC ROLE_PCC ROLE_PCC_WRITE ROLE_SERVICE_BOC	GROUP_ADMIN Admin

Write Access:



Edit existing data access rule

Modify an existing data access rule. Mind, layer group containment rules only affect WMS.

☐ Global layer group rule

Workspace: *

Layer and groups: *

Access mode: Write

Roles

Grant access to any role ☐

Available Roles	Selected Roles
ROLE_ANONYMOUS ROLE_AUTHENTICATED ROLE_BOC ROLE_PCC ROLE_PCC_WRITE ROLE_SERVICE_BOC	GROUP_ADMIN Admin

We can now define the ROLES that are associated to the new **BOC Workspace.**

3.2 DATA SECURITY - BOC ROLE

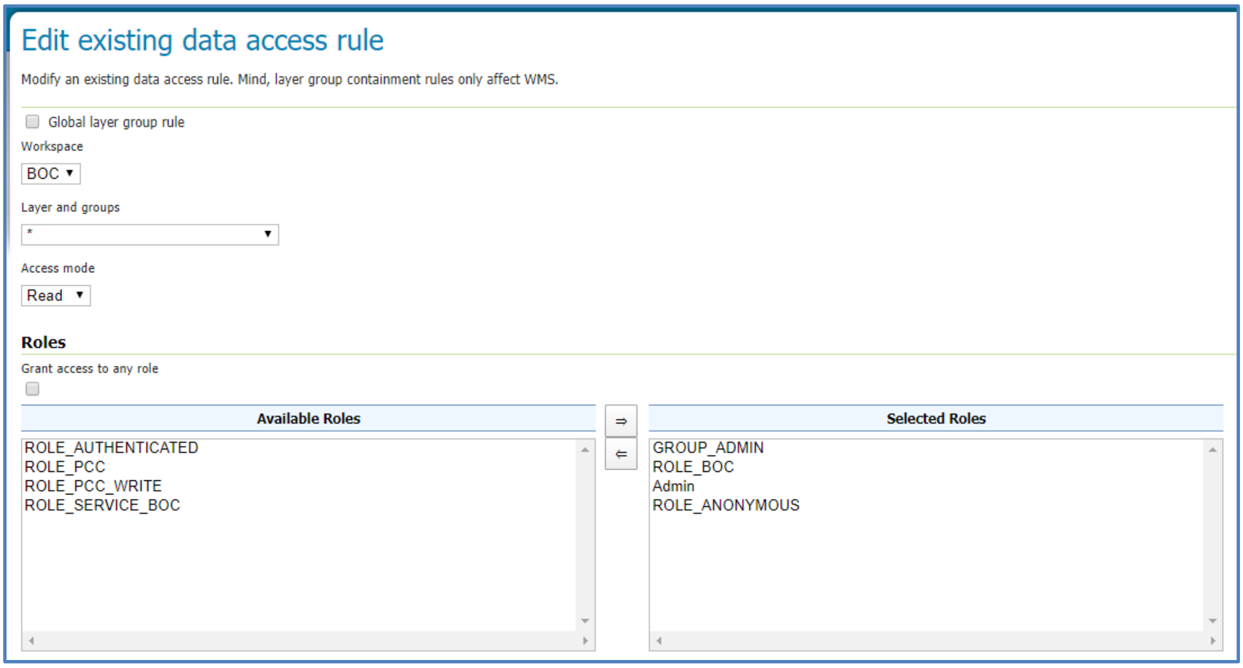
We will now need to add **Data Security RULES** which relate to the Workspace that the new BOC ROLE will be associated to. In this case the ROLE_BOC should only have access to the **BOC Workspace.** We will need to configure RULES for ADMIN (A), WRITE (W) and READ (R) Access to the BOC Workspace.

3.2.1 BOC – READ RULE:

From the **Data Security** page, choose **New Rule**.

- Choose the **BOC Workspace**
- Choose ***** for - ALL LAYERS (which will include all Layers in the BOC Workspace)
- Choose Access Mode = **READ**
- Assign the Admin, Anonymous and the new **ROLE_BOC** as the only ROLES to have READ Access to this Workspace by moving the Roles to the right (Selected Roles).

***NB.** Without the **ROLE_ANONYMOUS** being a Selected Role for the BOC Workspace, client applications such as a WebGIS will not be able to render any WMS layers from the BOC Workspace. This is because a client application may not utilise a LOGIN/ROLE when accessing the WMS layer. So, in order to view the WMS, the ROLE_ANONYMOUS must have access to the layer. However, you won't need the ROLE_ANONYMOUS for the ADMIN or WRITE Access Modes.*



Edit existing data access rule

Modify an existing data access rule. Mind, layer group containment rules only affect WMS.

☐ Global layer group rule

Workspace: BOC

Layer and groups: *

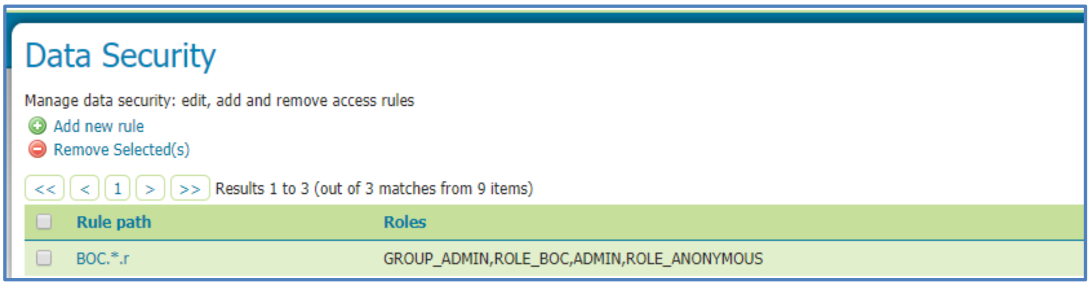
Access mode: Read

Roles

Grant access to any role ☐

Available Roles	Selected Roles
ROLE_AUTHENTICATED	GROUP_ADMIN
ROLE_PCC	ROLE_BOC
ROLE_PCC_WRITE	Admin
ROLE_SERVICE_BOC	ROLE_ANONYMOUS

Save the changes and a new RULE will be created called **BOC.*.r**



Data Security

Manage data security: edit, add and remove access rules

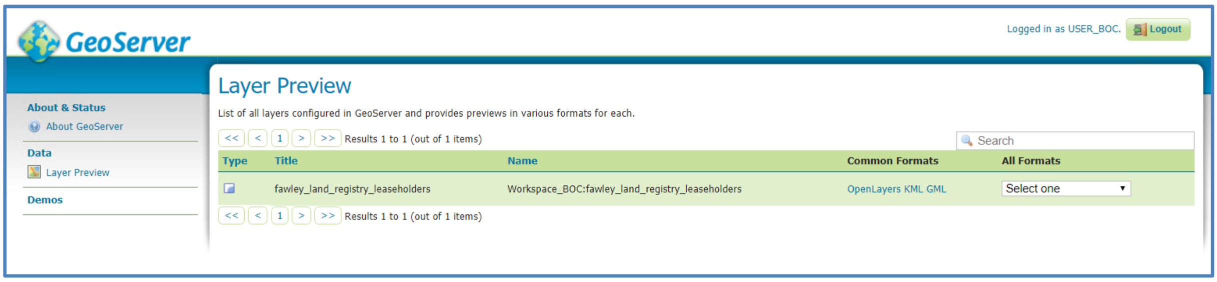
Add new rule

Remove Selected(s)

<< < 1 > >> Results 1 to 3 (out of 3 matches from 9 items)

□	Rule path	Roles
□	BOC.*.r	GROUP_ADMIN,ROLE_BOC,ADMIN,ROLE_ANONYMOUS

To test the new User, Role and Rule, logout as the Admin User and **login** as the **USER_BOC**. Once logged in you will see that all Panes apart from the **DATA Pane** are now hidden. Within the DATA Pane the only option we have is **Layer Preview.** This is because the User/ROLE BOC only has **read** privileges (defined by the Rule we created).



Layer Preview

List of all layers configured in GeoServer and provides previews in various formats for each.

<< < 1 > >> Results 1 to 1 (out of 1 items)

Search

Type	Title	Name	Common Formats	All Formats
▨	fawley_land_registry_leaseholders	Workspace_BOC:fawley_land_registry_leaseholders	OpenLayers KML GML	Select one

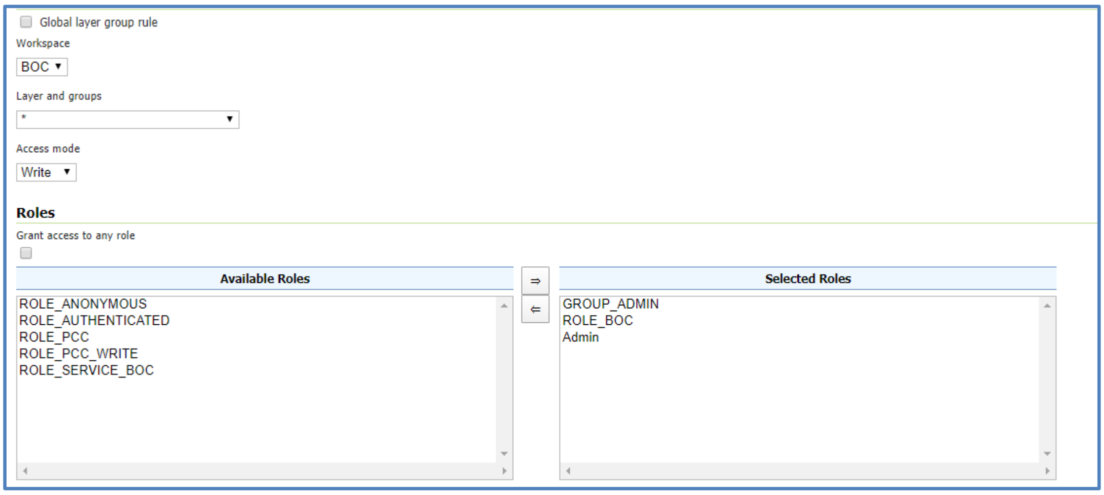
<< < 1 > >> Results 1 to 1 (out of 1 items)

3.2.2 BOC – WRITE RULE:

Logout and login as the **ADMIN User.**

From the **Data Security** page, choose **New Rule.**

- Choose the **BOC Workspace**
- Choose ***** for - ALL LAYERS
- Choose Access Mode = **WRITE**
- Assign the Admin and the new **ROLE_BOC** as the only ROLES to have WRITE Access to this Workspace by moving the Roles to the right (Selected Roles).



□ Global layer group rule

Workspace: BOC

Layer and groups: *

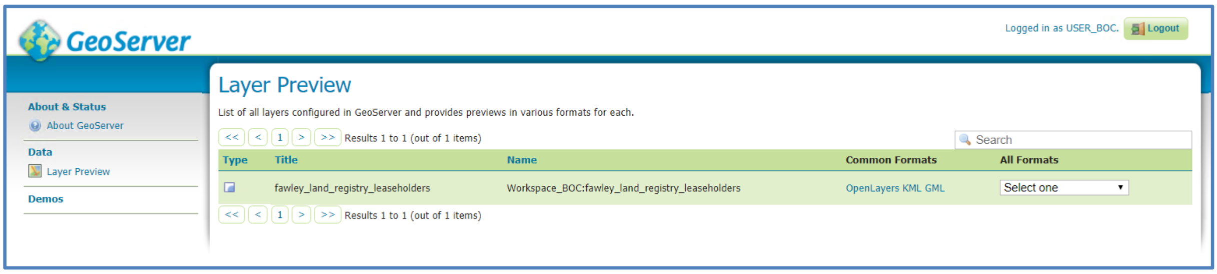
Access mode: Write

Roles

Grant access to any role □

Available Roles	Selected Roles
ROLE_ANONYMOUS ROLE_AUTHENTICATED ROLE_PCC ROLE_PCC_WRITE ROLE_SERVICE_BOC	GROUP_ADMIN ROLE_BOC Admin

Again, this RULE will only allow you to see the Layer Preview option in the DATA PANE.



Layer Preview

List of all layers configured in GeoServer and provides previews in various formats for each.

Results 1 to 1 (out of 1 items)

Type	Title	Name	Common Formats	All Formats
	fawley_land_registry_leaseholders	Workspace_BOC:fawley_land_registry_leaseholders	OpenLayers KML GML	Select one

Results 1 to 1 (out of 1 items)

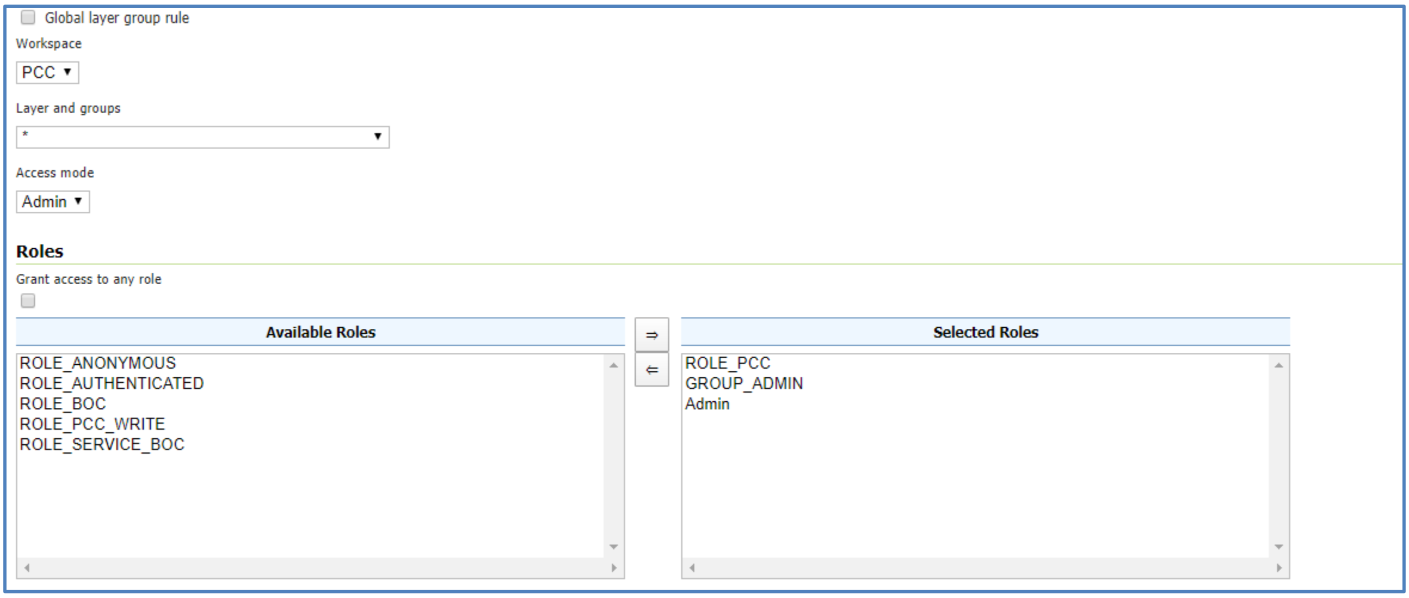
So, add a third RULE.

Logout and login as the ADMIN User.

3.2.3 BOC – ADMIN RULE:

From the **Data Security** page, choose **New Rule.**

- Choose the **BOC Workspace**
- Choose * for - ALL LAYERS
- Choose Access Mode = **ADMIN**
- Assign the Admin and the new **ROLE_BOC** as the only ROLES to have ADMIN Access to this Workspace by moving the Roles to the right (Selected Roles).



☐ Global layer group rule

Workspace
PCC

Layer and groups
*

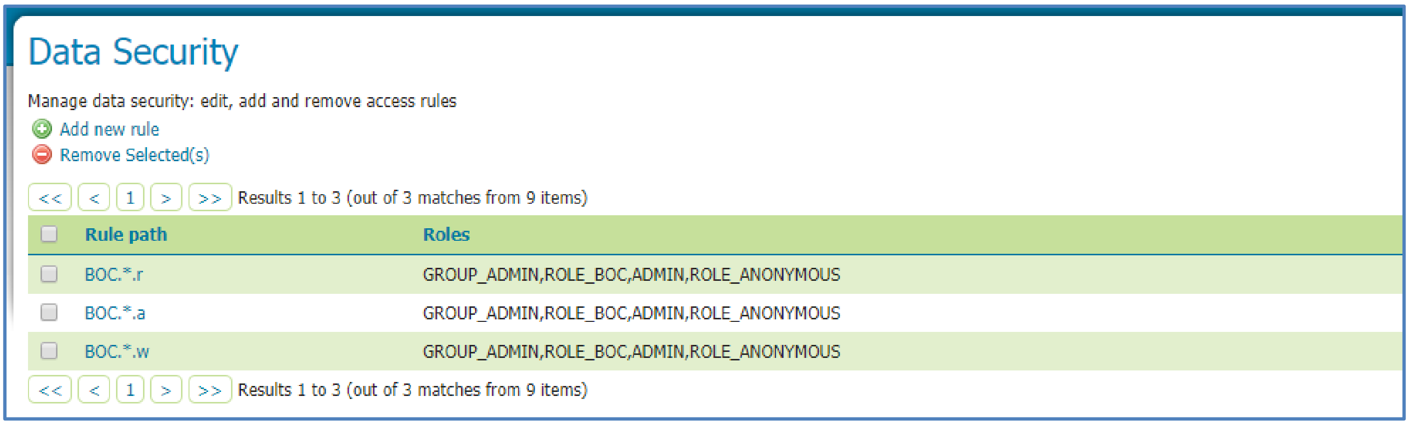
Access mode
Admin

Roles

Grant access to any role
☐

Available Roles	Selected Roles
ROLE_ANONYMOUS ROLE_AUTHENTICATED ROLE_BOC ROLE_PCC_WRITE ROLE_SERVICE_BOC	ROLE_PCC GROUP_ADMIN Admin

You will now have **3 RULES** for the BOC ROLE.



Data Security

Manage data security: edit, add and remove access rules

Add new rule

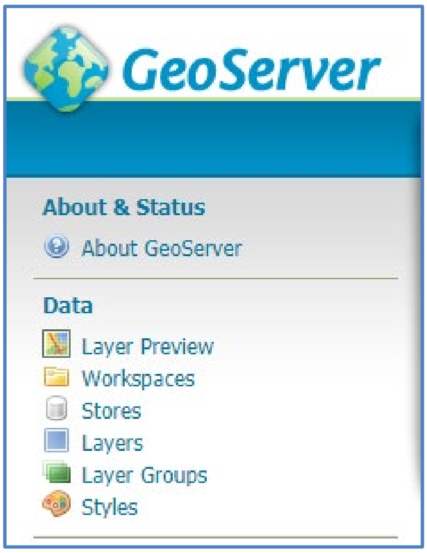
Remove Selected(s)

<< < 1 > >> Results 1 to 3 (out of 3 matches from 9 items)

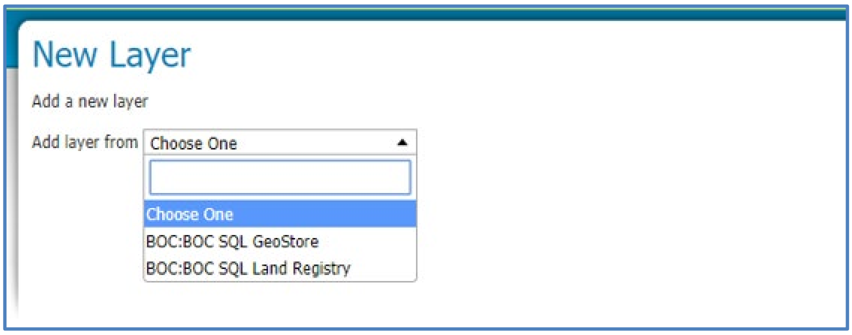
□	Rule path	Roles
□	BOC.*.r	GROUP_ADMIN,ROLE_BOC,ADMIN,ROLE_ANONYMOUS
□	BOC.*.a	GROUP_ADMIN,ROLE_BOC,ADMIN,ROLE_ANONYMOUS
□	BOC.*.w	GROUP_ADMIN,ROLE_BOC,ADMIN,ROLE_ANONYMOUS

<< < 1 > >> Results 1 to 3 (out of 3 matches from 9 items)

If you now logout and **login** as **USER_BOC**, you will see that all options are available in the **DATA** Pane, including **LAYERS, STORES, STYLES**.



If you try to Add a New Layer, the list of STORES is now filtered to only show the **STORES** that are within the **BOC Workspace.**

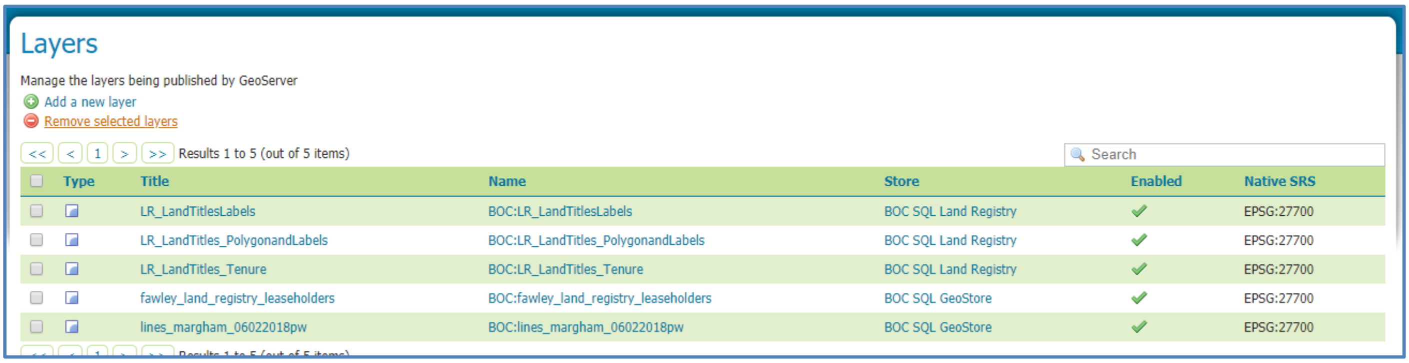


New Layer

Add a new layer

Add layer from: Choose One

The Layers list will only show those **Layers** that were created in a **BOC Store/Workspace.**



Layers

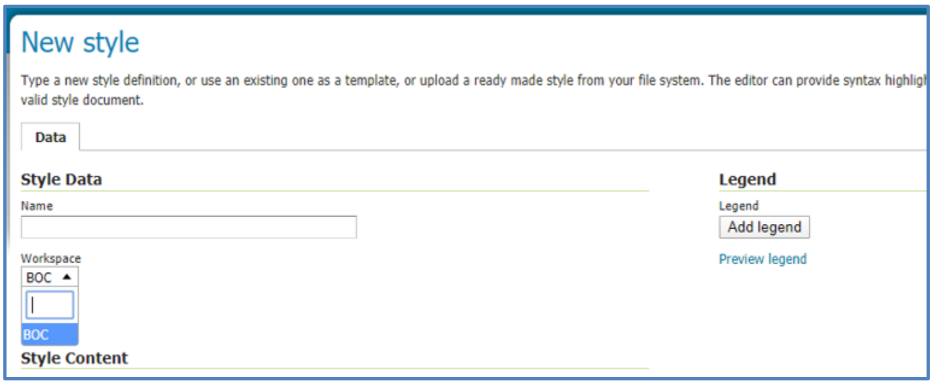
Manage the layers being published by GeoServer

Add a new layer
Remove selected layers

<< < 1 > >> Results 1 to 5 (out of 5 items)

□	Type	Title	Name	Store	Enabled	Native SRS
□		LR_LandTitlesLabels	BOC:LR_LandTitlesLabels	BOC SQL Land Registry	✓	EPSG:27700
□		LR_LandTitles_PolygonandLabels	BOC:LR_LandTitles_PolygonandLabels	BOC SQL Land Registry	✓	EPSG:27700
□		LR_LandTitles_Tenure	BOC:LR_LandTitles_Tenure	BOC SQL Land Registry	✓	EPSG:27700
□		fawley_land_registry_leaseholders	BOC:fawley_land_registry_leaseholders	BOC SQL GeoStore	✓	EPSG:27700
□		lines_margham_06022018pw	BOC:lines_margham_06022018pw	BOC SQL GeoStore	✓	EPSG:27700

And if you try to create something new e.g. a new **STYLE**… you can only save the Style into the **BOC Workspace.**

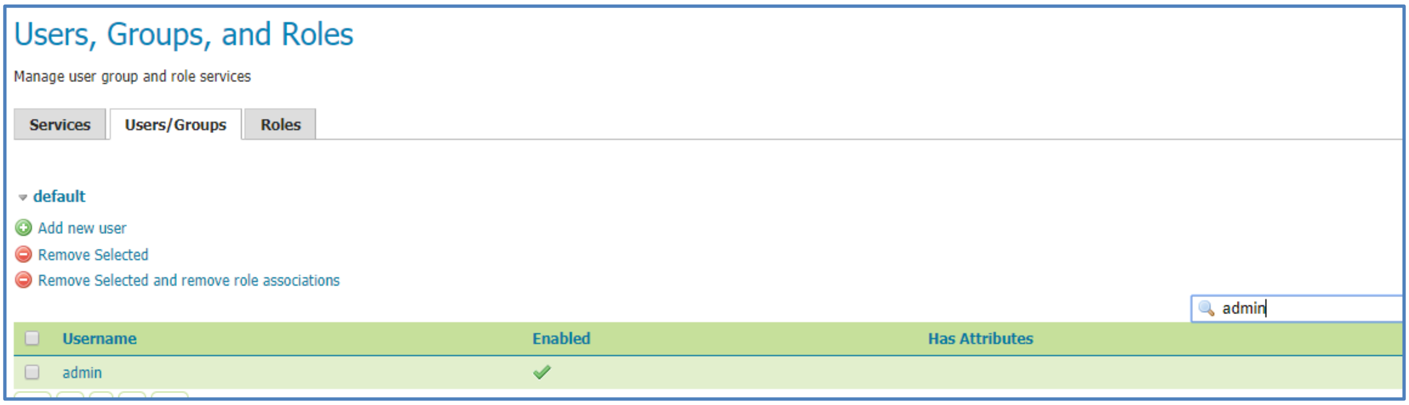


New style

Type a new style definition, or use an existing one as a template, or upload a ready made style from your file system. The editor can provide syntax highligl valid style document.

4 – USER PASSWORDS:

Finally, ensure that you update the generic **GeoServer password** to one that isn't shared with other Users/Roles. To do this choose **Security** > **Users, Groups, Roles** > and click on the **Users/Groups** Tab.



Users, Groups, and Roles

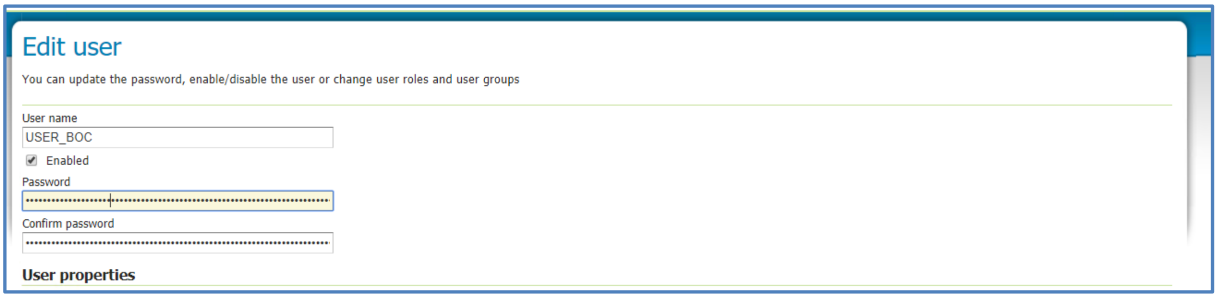
Manage user group and role services

admin

□	Username	Enabled	Has Attributes
□	admin	✓	

Select the User that you wish to update, in this case the **ADMIN User.**

Edit the **existing password** (this will be masked out), **confirm** the new password and choose **Save** to commit the changes.



Edit user

You can update the password, enable/disable the user or change user roles and user groups

User name: USER_BOC

☑ Enabled

Password: ••

Confirm password: ••

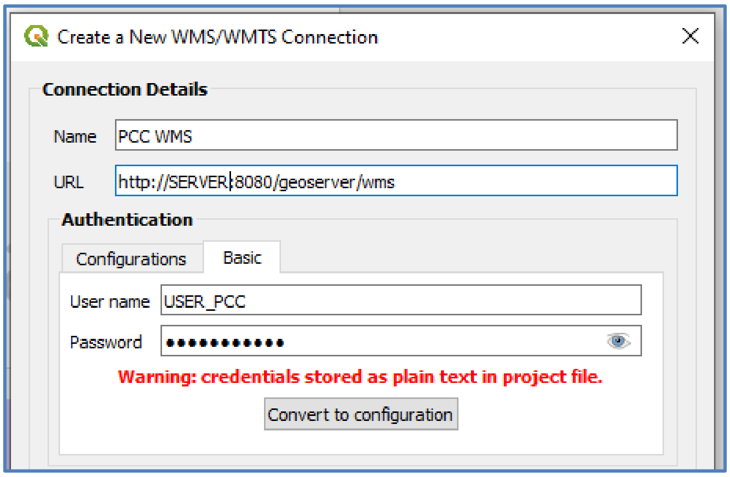
User properties

You have now successfully created a New ROLE, New User and defined the Rules for that Role/User so that they only have access to the Layers, Stores, Styles associated to their Workspace when working in the GeoServer Admin Pages. This ensures that team members or clients that share servers can only see and edit the GeoServer configuration for their Roles.

5 – QGIS and GEOSERVER:

Now that we have created a new User/Role with restricted access to Layers in our GeoServer instance, this will also be beneficial for when you share your WMS layers. For example, in **QGIS** instead of providing all Users with the generic GeoServer Admin details, you can now provide Clients, Teams, Users with their **own login.**

Let's edit the **WMS Connection** in QGIS and use a specific Users login. In this case we will use another User called **USER_PCC** and insert their login details into the WMS connection.



Create a New WMS/WMTS Connection

Connection Details

Name: PCC WMS

URL: http://SERVER:8080/geoserver/wms

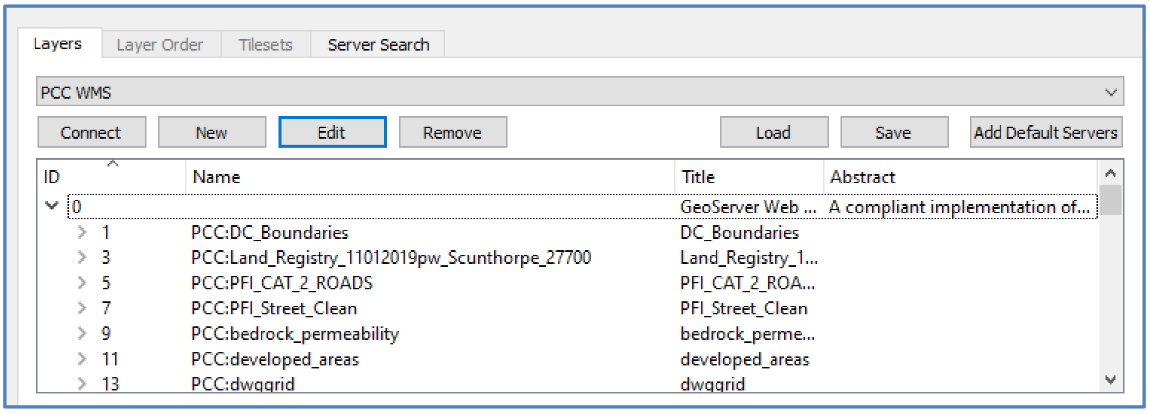
Authentication

User name: USER_PCC

Password: ●●●●●●●●●●●

Warning: credentials stored as plain text in project file.

With the WMS Connection updated to connect via the **USER_PCC** the end user (QGIS user) can now only access and open the WMS layers associated to that User/Role.. with layers filtered accordingly.

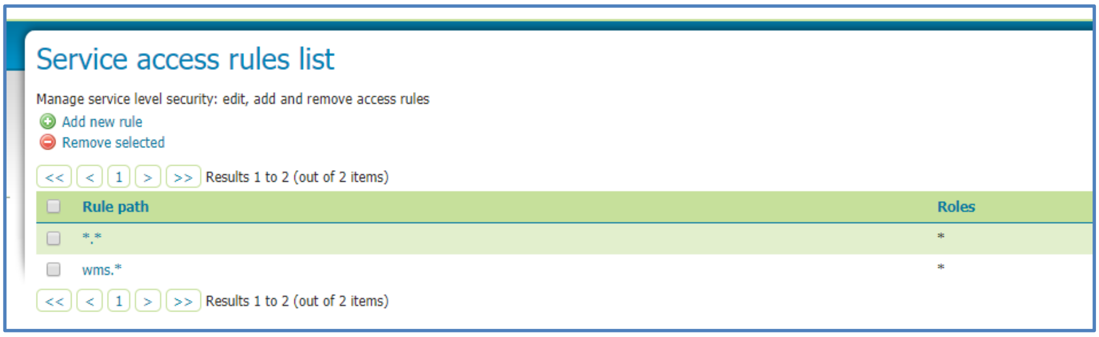


ID	Name	Title	Abstract
0		GeoServer Web ...	A compliant implementation of...
1	PCC:DC_Boundaries	DC_Boundaries	
3	PCC:Land_Registry_11012019pw_Scunthorpe_27700	Land_Registry_1...	
5	PCC:PFI_CAT_2_ROADS	PFI_CAT_2_ROA...	
7	PCC:PFI_Street_Clean	PFI_Street_Clean	
9	PCC:bedrock_permeability	bedrock_perme...	
11	PCC:developed_areas	developed_areas	
13	PCC:dwggrid	dwggrid	

6 – More options….. WFS and DATA DOWNLOAD:

You may wish to also restrict what DATA can be downloaded from your GeoServer Instance. To do this you should setup **WFS Rules.**

If in your GeoServer Instance you haven't setup a Service Access Rule for WFS yet… check this in the **Security** > **Services** Pane.



Service access rules list

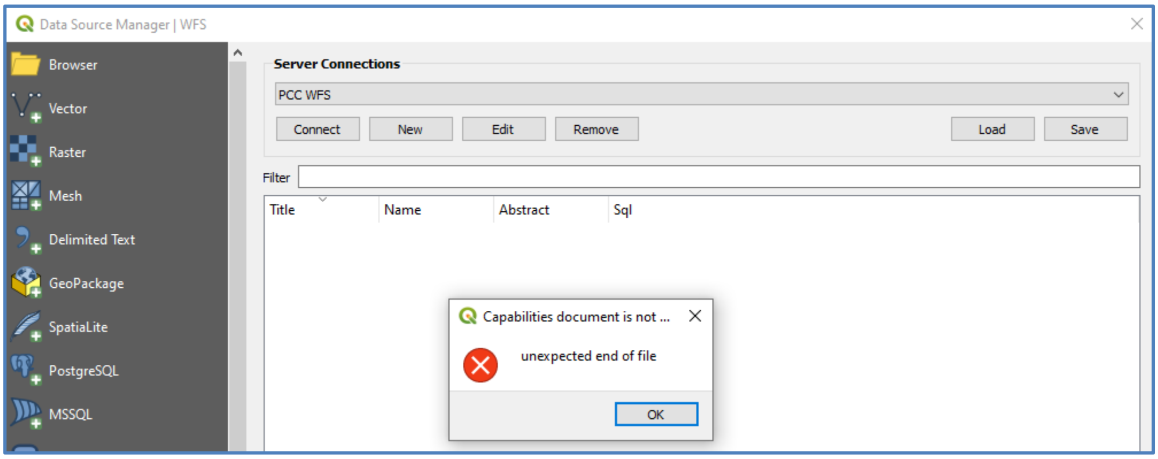
Manage service level security: edit, add and remove access rules

Results 1 to 2 (out of 2 items)

□	Rule path	Roles
□	*.*	*
□	wms.*	*

Results 1 to 2 (out of 2 items)

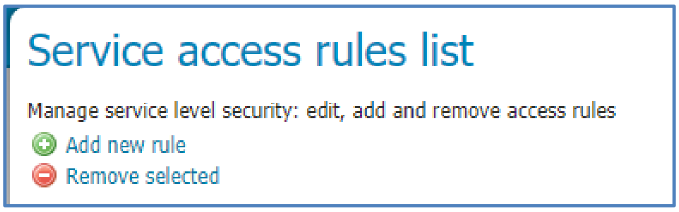
When you try and connect a client application (e.g. QGIS) to your GeoServer WFS, you will receive a failure notice:



Capabilities document is not ...

unexpected end of file

In order for client applications (e.g. QGIS) to access WFS, in GeoServer choose **Security** > **Services** > and choose to **Add a New Rule**.

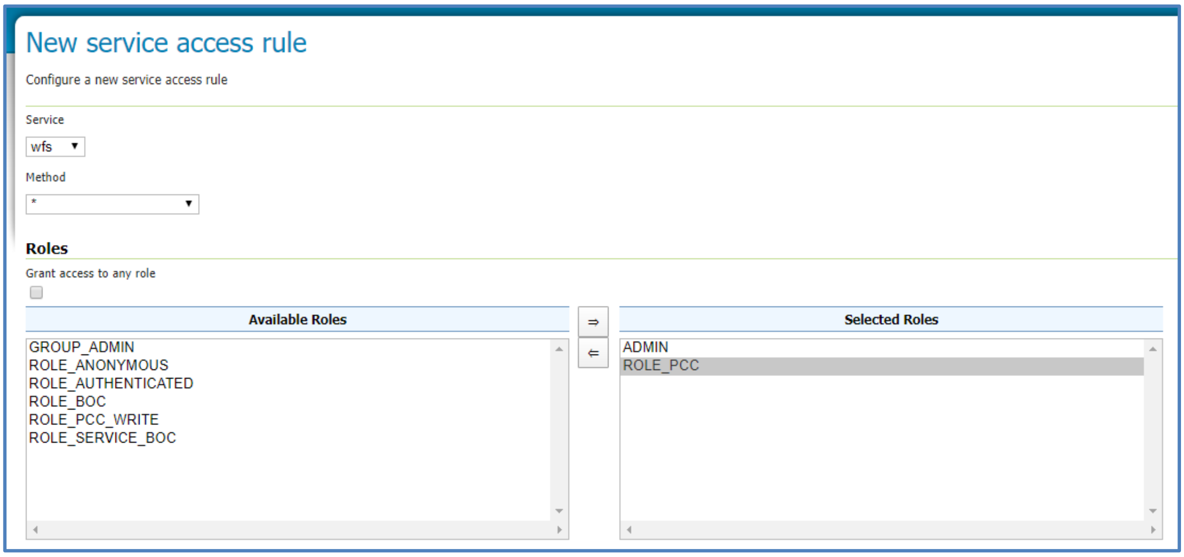


Service access rules list

Manage service level security: edit, add and remove access rules

In the Add New Rule choose:

- Choose the Service = **WFS**
- The Method = ***** (all)… there are other Methods to individually only allow certain calls
- Grant Access to the **ADMIN** and the **ROLE_PCC**



New service access rule

Configure a new service access rule

Service: wfs

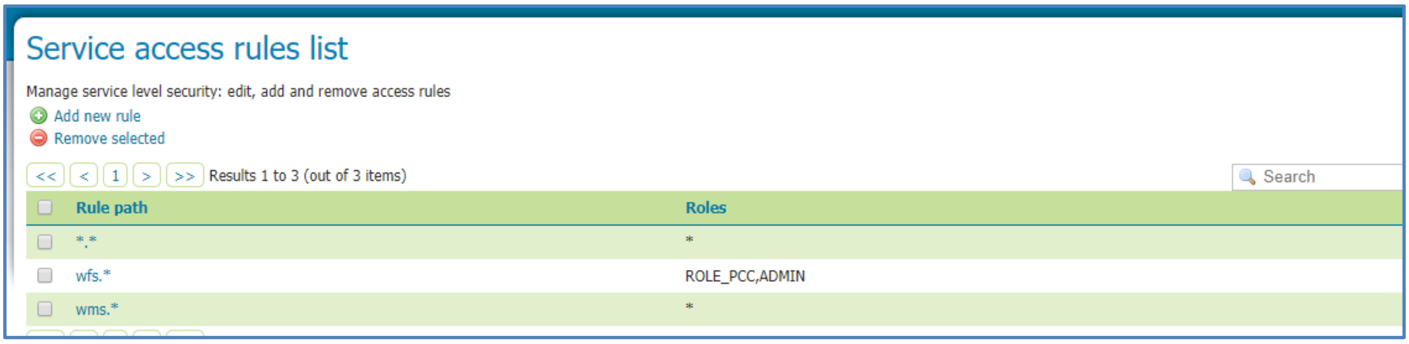
Method: *

Roles

Grant access to any role ☐

Available Roles	Selected Roles
GROUP_ADMIN	ADMIN
ROLE_ANONYMOUS	ROLE_PCC
ROLE_AUTHENTICATED	
ROLE_BOC	
ROLE_PCC_WRITE	
ROLE_SERVICE_BOC	

You will now have a 3rd **Service Access Rule** where the Admin and ROLE_PCC User can access **WFS**/Data Download.



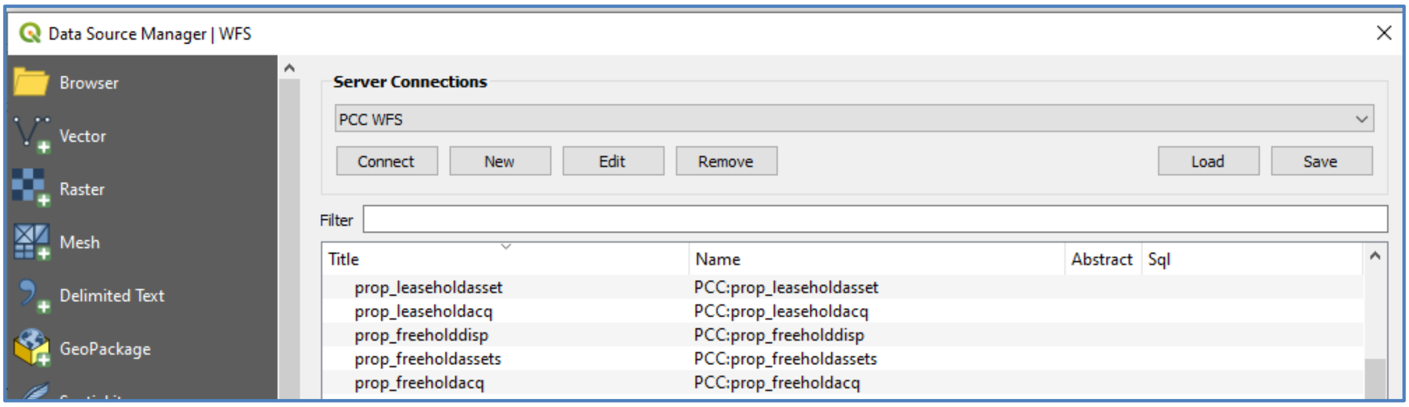
Service access rules list

Manage service level security: edit, add and remove access rules

Results 1 to 3 (out of 3 items)

□	Rule path	Roles
□	*.*	*
□	wfs.*	ROLE_PCC,ADMIN
□	wms.*	*

Back in QGIS, if you check the WFS Connection the USER_PCC can now access their Layers (only those defined by their Workspace) in **WFS format** for data download.



PCC WFS

Title	Name	Abstract	Sql
prop_leaseholdasset	PCC:prop_leaseholdasset		
prop_leaseholdacq	PCC:prop_leaseholdacq		
prop_freeholddisp	PCC:prop_freeholddisp		
prop_freeholdassets	PCC:prop_freeholdassets		
prop_freeholdacq	PCC:prop_freeholdacq		

This blog successfully details how to start managing your Users, Roles and Data Security within your GeoServer Instance, so you no longer need to rely on the generic ADMIN user!