



JULY 1, 2019

ADMIN TRAINING MODULE

A GUIDE FOR ADMINISTRATOR FOR USING ASDC

IMMAP AFGHANISTAN
KABUL
Afghanistan

Table Of Contents

INTRODUCTION	3
ACTIVATING AND DEACTIVATING USER	5
ACTIVATE ACCOUNT.....	5
DEACTIVATE USER	8
TYPES OF USER	8
STANDARDIZE ORGANIZATION NAME	9
SET LAYER PERMISSION	11
PERMISSION ON UPLOAD LAYER	11
SET LAYER PERMISSION	12
SET MULTIPLE LAYER PERMISSION	14
SET INTERACTIVE MAP PERMISSION	15
SET INTERACTIVE MAP PERMISSION	15
SET MULTIPLE INTERACTIVE MAPS PERMISSION.....	17
SET STATIC MAP PERMISSION.....	18
PERMISSION ON UPLOAD STATIC MAP	18
SET STATIC MAP PERMISSION	19
SET MULTIPLE STATIC MAP PERMISSION.....	21
CREATE AND SET GROUP PERMISSION.....	23
CHECKING SNAPSHOT.....	24

TABLE OF FIGURES

FIGURE 1	3
FIGURE 2	4
FIGURE 3	5
FIGURE 4	5
FIGURE 5	6
FIGURE 6	6
FIGURE 7	6
FIGURE 8	6
FIGURE 9	7
FIGURE 10	7
FIGURE 11	7
FIGURE 12	8
FIGURE 13	8
FIGURE 14	9
FIGURE 15	9
FIGURE 16	10
FIGURE 17	11
FIGURE 18	11
FIGURE 19	13
FIGURE 20	13
FIGURE 21	14
FIGURE 22	14
FIGURE 23	15
FIGURE 24	16
FIGURE 25	16
FIGURE 26	17
FIGURE 27	18
FIGURE 28	19
FIGURE 29	20
FIGURE 30	21
FIGURE 31	21
FIGURE 32	22
FIGURE 33	23
FIGURE 34	23
FIGURE 35	23
FIGURE 36	23
FIGURE 37	24

INTRODUCTION

Major learning objectives

At the end of this section the trainee should be able to:

1. Accessing the administrator panel interface

ASDC has an administration panel based on the Django admin which can be used to do some database operations. Although most of the operations can and should be done through the normal ASDC interface, the admin panel provides a quick overview and management tool over the database. Please note that only the staff users (including the superusers) can access the admin interface.

Accessing the admin panel

You could find the link access to administrator page at <http://asdc.immap.org/admin/> or by clicking in the upper right corner on the username and see under the dropdown menu with 'Admin' as a title (See Figure 1).

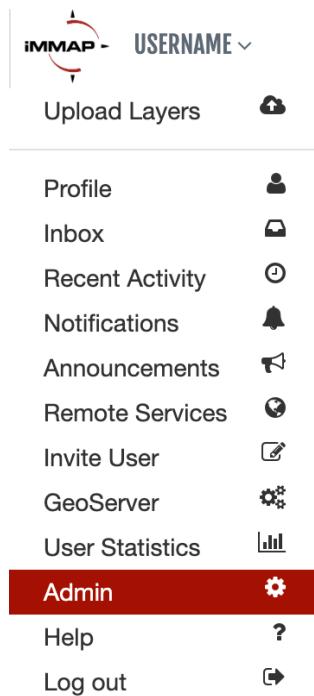


Figure 1

By clicking it, the following administrator interface will show up (Figure 2).

GeoNode administration

Site administration

Recent Actions		
My Actions		
 planinc3	User	
 abelle	User	
 elipp	User	
 elipp34	User	
 ssiawash	User	
 rahimi	User	
 Akbari	User	
 lee0486	User	
 har6518	User	
 amandaconsidine	User	

Account	Add	Change
Account deletions		
Accounts		
Email addresses		
Signup code extendeds		
Signup codes		

Actstream	Add	Change
Actions		
Follows		

Announcements	Add	Change
Announcements		
Dismissals		

Auth	Add	Change
Groups		

Avatar	Add	Change
Avatars		
Orglogos		

Base	Add	Change
Contact roles		
Licenses		
Links		
Metadata Regions		
Metadata Restriction Code Types		
Metadata Spatial Representation Types		
Metadata Topic Categories		

Deliverynotes	Add	Change
Notess		

Dialogos	Add	Change
Comments		

Djcelery	Add	Change
Crontabs		
Intervals		
Periodic tasks		
Tasks		
Workers		

Documents	Add	Change
Documents		

Figure 2

ACTIVATING AND DEACTIVATING USER

Major learning objectives

At the end of this section the trainee should be able to:

1. Activate new user
2. Deactivate existing user
3. Differentiate types of user in ASDC
4. Giving role permission accordingly

ACTIVATE ACCOUNT

Method 1

Through the section called People (See Figure 3), it has the link to access all the users that exist at the moment by clicking "Users" (People -> Users).

The screenshot shows a web-based application interface. At the top, there's a blue header bar with the word 'People'. Below it, a white navigation bar has 'Users' highlighted in blue. On the right side of the navigation bar are two buttons: a green plus sign labeled 'Add' and a pencil icon labeled 'Change'. The main content area is currently empty, showing a light gray background.

Figure 3

To modify an existing user, click on "Users" then on a "username" in the list (Figure 4).

This screenshot shows a detailed list of users within the 'People' section. At the top left is a search bar with a magnifying glass icon and a 'Go' button. To its right, a message says '0 of 100 selected'. On the far right, there's a 'Filter' sidebar with several sections:

- By staff status:** All (selected), Yes, No
- By superuser status:** All (selected), Yes, No
- By active:** All (selected), Yes, No
- By groups:** anonymous, securityEditor, securityEditorUsers, staff_user_approve, IMMAP, MSH, Aidsdata, SMDMHA, NPA, DutchArmy, DOLO, OFDA, Akts, TeacherTraining, DoRR, WAW, CARITAS-G, ORNL, IMC, USGS, EDU-Brunswick, EDU-CALU, EDU-CHICAGO, EDU-JHU, EDU-CAU, EDU-AWEC, RMO, MEW, SERVE, EDU-Colorado, CAS, AMU, EDU-JHU, IDLO, CPAU, EDU-U-Tokyo, ASDF, EDU-WRI, Alcis, REACH

The main table lists numerous users with columns for Username, Email address, First name, Last name, Organization Name, Organisation acronym, Staff status, and a small red circular icon. The 'Staff status' column contains mostly red circles, indicating inactive users.

Figure 4

You can also filter the list by the active status on the right side (Figure 5).

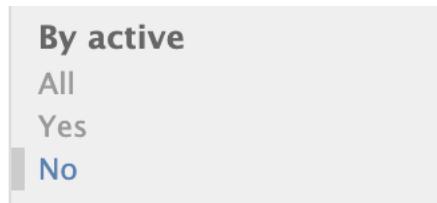


Figure 5

After clicking the “username”, tick the “Active”, “Staff Status” or “Superuser Status” checkboxes accordingly (Figure 6). Then, confirm with “save” button at the bottom left (Figure 7).

The image shows a user permission configuration screen. At the top, a blue header bar contains the text 'Permissions'. Below this, there are three sections, each with a checkbox and a subtitle:

- Active**: The checkbox is checked (indicated by a blue checkmark). The subtitle says: "Designates whether this user should be treated as active. Unselect this instead of deleting accounts."
- Staff status**: The checkbox is unchecked (indicated by a gray outline). The subtitle says: "Designates whether the user can log into this admin site."
- Superuser status**: The checkbox is unchecked (indicated by a gray outline). The subtitle says: "Designates that this user has all permissions without explicitly assigning them."

Figure 6



Figure 7

Method 2

Open your registered mailing address. You will get a notification of new registered user in ASDC if your account has been set up as an admin (Figure 8).



Figure 8

Open the message and click the link provided to enable access of the new registered account (Figure 9).

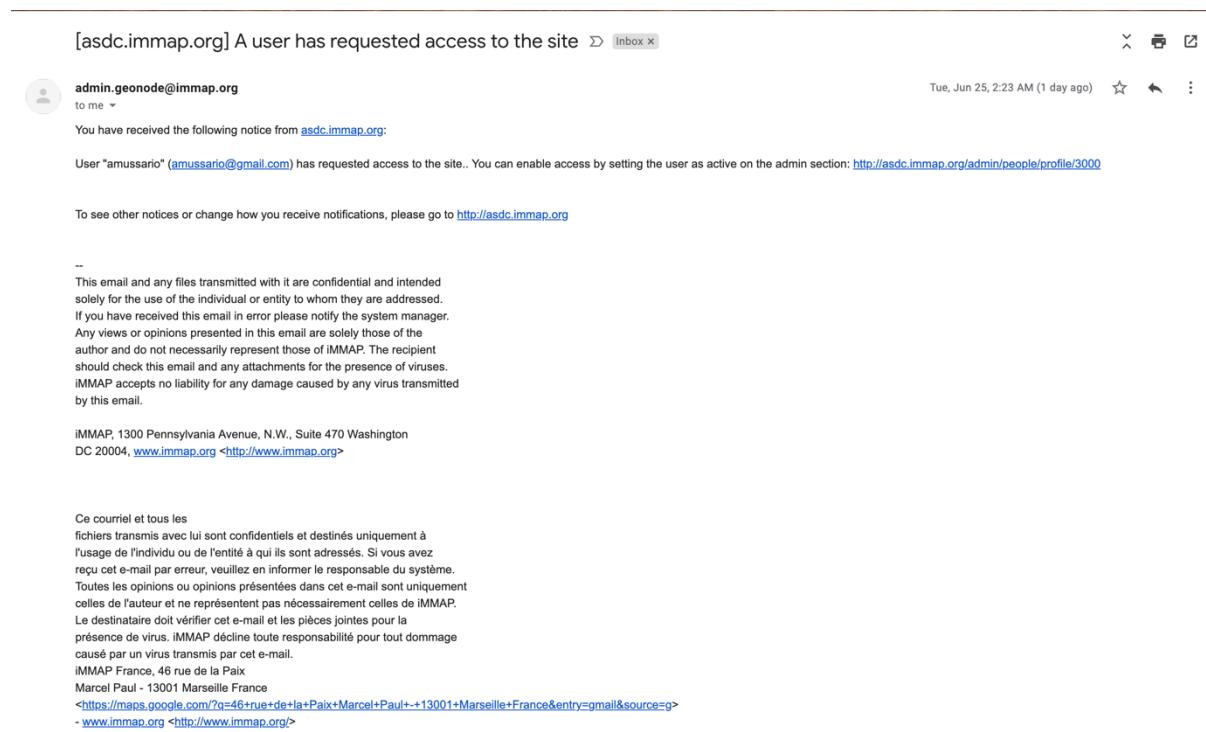


Figure 9

Tick the “Active”, “Staff Status” or “Superuser Status” checkboxes accordingly (Figure 10). Then, confirm with “save” button at the bottom left (Figure 11).

Permissions	
<input checked="" type="checkbox"/> Active	Designates whether this user should be treated as active. Unselect this instead of deleting accounts.
<input type="checkbox"/> Staff status	Designates whether the user can log into this admin site.
<input type="checkbox"/> Superuser status	Designates that this user has all permissions without explicitly assigning them.

Figure 10



Figure 11

DEACTIVATE USER

If you want to deactivate an existing account, you can do it by uncheck the “Active” checkbox (Figure 12) and confirm it with “save” button at the bottom left (Figure 13).

Permissions

Active
Designates whether this user should be treated as active. Unselect this instead of deleting accounts.

Staff status
Designates whether the user can log into this admin site.

Superuser status
Designates that this user has all permissions without explicitly assigning them.

Figure 12



Figure 13

TYPES OF USER

There are two types of user in ASDC:

- Superuser is able to access the Django Admin Interface and he has all permissions on the data uploaded to ASDC.
- Ordinary user (created from the ASDC interface) only has active permissions by default. The user will not have the ability to access the Django Admin Interface and certain permissions have to be added for him/her.

You should now have an overview over the different kinds of users.

STANDARDIZE ORGANIZATION NAME

Major learning objectives

At the end of this section the trainee should be able to:

1. Modify existing organization in certain profile at ASDC

To standardize the organization name, we need to modify at each of the existing user profile. Click on “Users” at “People” section (Figure 14) then, click on a “username” in the list (Figure 15).

The screenshot shows a web-based application interface for managing users. At the top, there's a blue header bar with the word 'People'. Below it, a sub-header says 'Users'. On the right side of the header, there are two buttons: a green plus sign labeled 'Add' and a pencil icon labeled 'Change'. The main area contains a table with several columns: 'Username', 'Email address', 'First name', 'Last name', 'Organization Name', 'Organisation acronym', and 'Staff status'. There are many rows of data, each representing a different user account.

Figure 14

This screenshot shows a detailed view of user management. The top navigation bar includes 'GeoNode administration', 'Home', 'People', and 'Users'. A search bar is at the top left. To the right, there are links for 'Welcome', 'Rafinkanisa', 'Change password / Log out', and 'Add user'. A sidebar on the right provides filtering options: 'By staff status' (All, Yes, No), 'By superuser status' (All, Yes, No), 'By active' (All, Yes, No), and 'By groups' (All, anonymous, securityEditor, securityEditorUsers, staff_user_approve, IMMAP, MEW-Balkh, Addata, SMDMHA, NPA, DutchArmy, USAID - OFDA, Akhla, TeacherTraining, DoRR, WAW, CARITAS-G, ORNL, HCR, USGS, EDU-Brunswick, EDU-CALU, ENEA, AWEC, PWD, MOW, SERVE, EDU-Colorado, CAPS, AMO, EDU-JHU, IDLO, CPAU, EDU-U-Tokyo, ASIF, EDU-WRI, Alcis, REACH). The main table lists users with columns for 'Action', 'Username', 'Email address', 'First name', 'Last name', 'Organization Name', 'Organisation acronym', and 'Staff status'. Each row contains a checkbox for 'Action' and a link to 'Edit' for each user entry.

Figure 15

Look at the “Extended Profile” section (Figure 16) and modify the organization details accordingly.

Extended profile

Organization Name:	German International Cooperation	name of the responsible organization
Organisation acronym:	GIZ	Organisation acronym
Organisation Type:	Government Int.	Organisation Type
Organisation Name Status:	OCHA	Organisation Name Status
Profile:	<div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div> introduce yourself	
Position Name:	employee	role or position of the responsible person

Figure 16

SET LAYER PERMISSION

Major learning objectives

At the end of this section the trainee should be able to:

1. Restrict the access of new uploaded layer data in ASDC
2. Restrict the access of certain layer data in ASDC
3. Restrict the access of multiple layer data in ASDC

PERMISSION ON UPLOAD LAYER

This section will guide you through the steps that can be done in order to restrict the access on any layer data uploaded to ASDC.

As already mentioned before, it is important to know that a superuser does have unrestricted access to all your uploaded data. That means you cannot ban a superuser from viewing, downloading or editing a layer.

The permissions on a certain layer can already be set when uploading files. Once you click "Upload Layer" button (Figure 17) on Layers page (Layers -> Upload Layer), an upload form will appear (Figure 18).

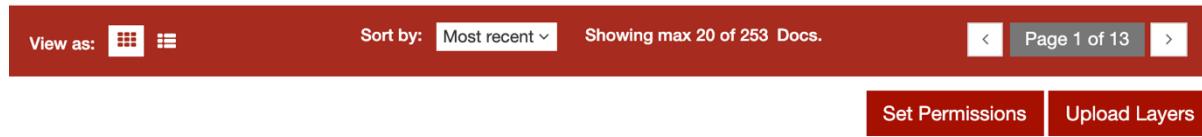


Figure 17

When the upload form appears (Layers -> Upload Layer) you will see the permission section on the right side (Figure 18).

A screenshot of the 'Upload Layers' form. On the left, there's a large area for file upload with a 'Drop files here' placeholder and a 'Choose Files' button. Below it is a dropdown for 'Files to be uploaded' (set to 'UTF-8/Unicode') and buttons for 'Clear' and 'Upload files'. On the right, there's a 'Permissions' section with several dropdown menus:

- 'Who can view it?': 'Anyone' (selected)
- 'The following users': 'Choose users...' (button)
- 'The following groups': 'Choose groups...' (button)
- 'Who can download it?'
- 'Who can change metadata for it?'
- 'Who can edit data for this layer?'
- 'Who can edit styles for this layer?'
- 'Who can manage it? (update, delete, change permissions, publish/unpublish it)'

A blue 'Explore Layers' button is located at the top right of the form.

Figure 18

As it can be seen here, the access on your layer is split up into:

- view data
- download data
- change metadata, edit data and edit styles
- manage data

The difference between manage and edit layer is that a user assigned to edit layer is not able to change the permissions on the layer whereas a user assigned to manage and edit layer can change the permissions.

You can now choose whether you want your layer to be viewed and downloaded by:

- anyone
- any registered user
- a certain user (or group)

If you want a layer only to be viewed by certain users or a group, you have to choose only users who can edit column in the part Who can view and download this data and do not tick the "Anyone" checkbox. In the section Who can edit this data you write down the names of the users you want to have admission on this layer.

Please remember when you assign a user to be able to edit your data, this user is allowed to execute all of the following actions:

- edit metadata
- edit styles
- manage styles
- replace layer
- remove layer

SET LAYER PERMISSION

To set the permissions on specific layer, click on the layer and you will see the same menu as shown in Figure 19. Click Change Permission of this Map located at the right-hand side (Figure 20) and a pop-up menu (Figure 21) will appear to set the access of the specified layer.

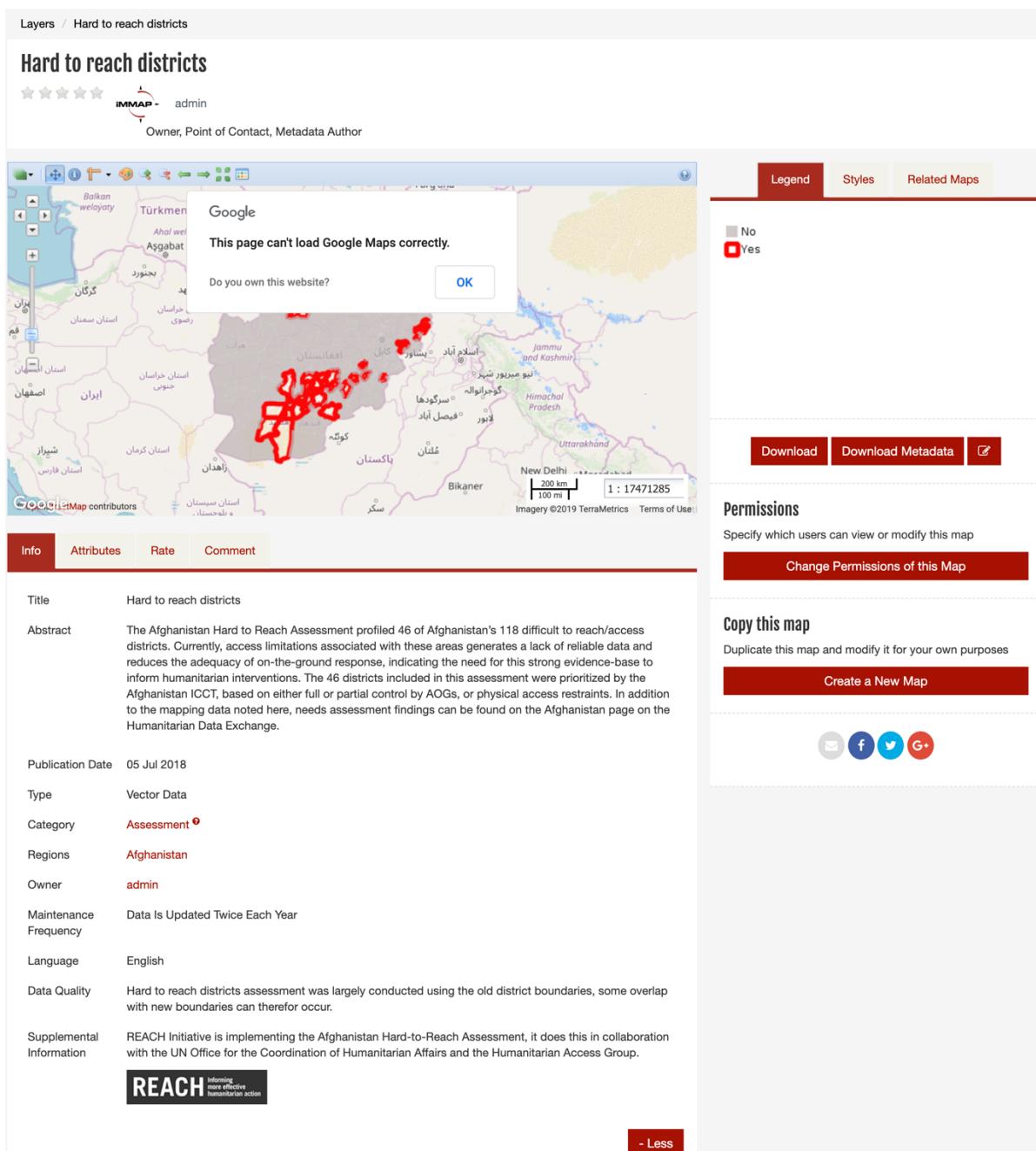


Figure 19

Permissions

Specify which users can view or modify this map

[Change Permissions of this Map](#)

Figure 20

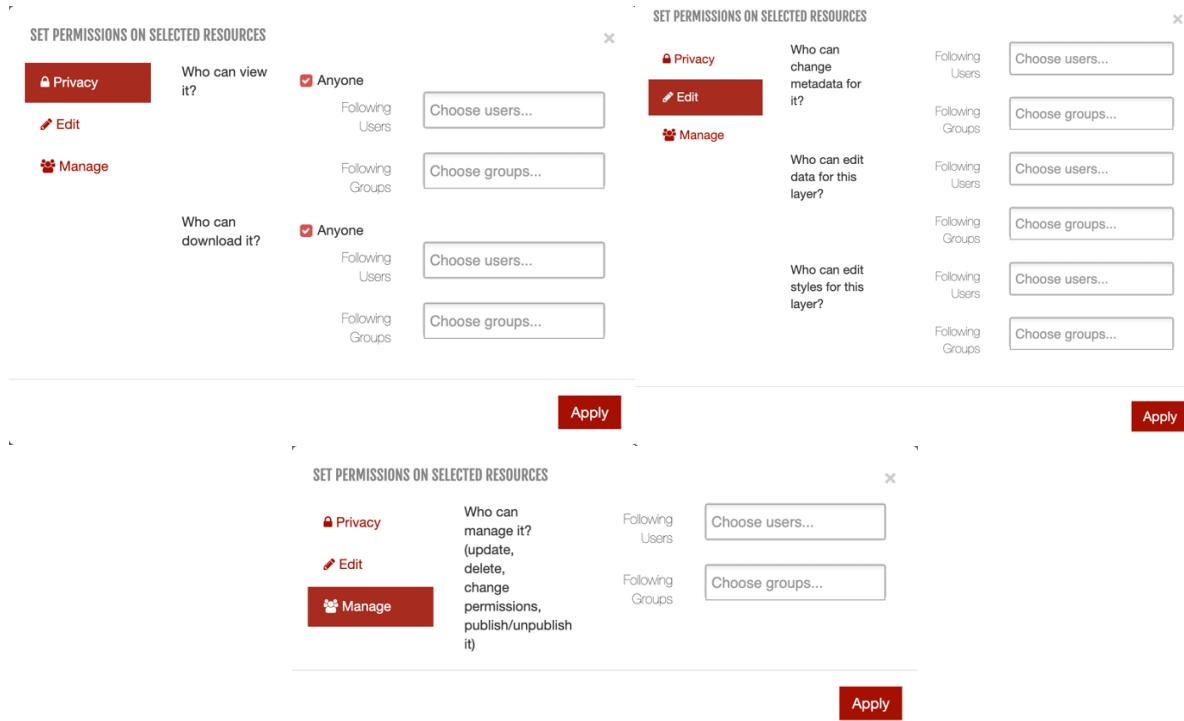


Figure 21

SET MULTIPLE LAYER PERMISSION

You could also set up the access by selecting multiple layer at once by clicking the checklist button that appear on the upper left side in each of the layer thumbnail in layer list. Click Set Permission button on the upper right side (Figure 22) and a pop-up (Figure 21) menu will appear to set the access of these layers.

Figure 22

SET INTERACTIVE MAP PERMISSION

Major learning objectives

At the end of this section the trainee should be able to:

1. Restrict the access of certain interactive map in ASDC
2. Restrict the access of multiple interactive maps in ASDC

SET INTERACTIVE MAP PERMISSION

To set the permissions on specific interactive map, click on the map and you will see the same menu as shown in Figure 23. Click "Change Permission of this Map" located at the right-hand side (Figure 24) and a pop-up menu (Figure 25) will appear to set the access of the specified interactive map.

The screenshot shows the 'Current Drought Risk - Vegetation Health' map interface. At the top, there are five star ratings and a user icon labeled 'IMMAP - admin'. Below the map, there are tabs for 'Info', 'Rate', and 'Comment'. The map itself displays a grayscale vegetation health index over Afghanistan, with major cities like Kabul, Herat, and Mazar-i-Sharif marked. A legend on the left identifies various provinces and districts. On the right, there's a 'Map Layers' sidebar listing land cover, drought prediction, elevation, rivers, roads, districts, provinces, and water wells. Below the map are sections for 'Permissions' (with a 'Change Permissions of this Map' button), 'Copy this map' (with a 'Create a New Map' button), and 'Map WMS' (with a 'Publish Map WMS' button). At the bottom, there are social sharing icons for email, Facebook, Twitter, and Google+.

Figure 23

Permissions

Specify which users can view or modify this map

Change Permissions of this Map

Figure 24

SET PERMISSIONS ON SELECTED RESOURCES

Privacy

Who can view it? Anyone
Following Users
Following Groups

Who can download it? Anyone
Following Users
Following Groups

SET PERMISSIONS FOR THIS RESOURCE

Privacy

Who can change metadata for it? Anyone
Following Users admin
Following Groups

Edit

Manage

Apply **Cancel** **Apply Changes**

SET PERMISSIONS ON SELECTED RESOURCES

Privacy

Who can manage it? (update, delete, change permissions, publish/unpublish it)
Following Users
Following Groups

Edit

Manage

Apply

Figure 25

Please keep in mind that administrators can choose who can do what for each map. Users can manage only the maps they own or the maps which they are authorized to manage.

By default, only owners can edit and manage maps, anyone can view and download them. Through the Permissions Settings Panel you can add or remove permissions for users and groups. Using this panel, you can set the following types of permissions:

- **View** allows to view the map
- **Download** allows to download the map
- **Change Metadata** allows to change the map metadata
- **Manage** allows to update, delete, change permissions, publish and unpublish the map.

For each of the above type permission, you can choose whether you want your map to be viewed and downloaded by:

- anyone
- any registered user
- a certain user (or group)

Please remember when assigning permissions to a group, all the group members will have those permissions. Be careful in case of editing permissions.

SET MULTIPLE INTERACTIVE MAPS PERMISSION

You could also set up the access by selecting multiple interactive maps at once by clicking the checklist button that appear on the upper left side in each of the layer thumbnail in layer list. Click Set Permission button on the upper right side (Figure 26) and a pop-up (Figure 25) menu will appear to set the access of these layers.

The screenshot shows a user interface for managing map layers. At the top, there are navigation controls: 'View as:' (grid and list icons), 'Sort by: Most recent', 'Showing max 20 of 29 Docs.', and 'Page 1 of 2'. Below these are two buttons: 'Set Permissions' and 'Create a New Map'. The main area displays four map thumbnails, each with a checked checkbox in the top-left corner, indicating they are selected:

- Kabul River Basin** by Hassibullah, 7 months ago (2 views)
- Current Drought Risk - Vegetation Health** by admin, about a year ago (676 views)
- REACH Initiative - Service Units / Informal Settlements** by admin, about a year ago (290 views)
- IOM - Gabion Walls - Mitigated - 2013-2017** by admin, about a year ago (133 views)

Each thumbnail has a 'View' and an 'i' button below it.

Figure 26

SET STATIC MAP PERMISSION

Major learning objectives

At the end of this section the trainee should be able to:

1. Restrict the access of new uploaded static map data in ASDC
2. Restrict the access of certain static map data in ASDC
3. Restrict the access of multiple static map data in ASDC

PERMISSION ON UPLOAD STATIC MAP

This section will guide you through the steps that can be done in order to restrict the access on any static map data uploaded to ASDC.

ASDC encourages to publicly, share and make available for download information uploaded on the platform. By default, anyone can see and download a static map. However, the document responsible can choose to limit access to the static map to some contributors and/or groups. Please keep in mind that administrators can choose who can do what for each static map and cannot be banned from viewing, downloading or editing a static map. Users can manage only the static maps they own or the static maps which they are authorized to manage.

The permissions on a certain static map can already be set when uploading files. Once you click “Upload Document” button (Figure 27) on Static Map page (Maps -> Static Maps -> Upload Document), an upload form will appear (Figure 28).

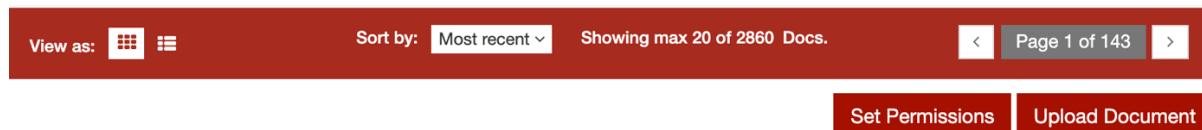


Figure 27

When the upload form appears (Maps -> Static Maps -> Upload Document) you will see the permission section on the right side (Figure 28).

The screenshot shows a form for uploading documents. At the top right is a blue button labeled "Explore Documents". Below it is a section titled "Upload Documents" with a note about allowed document types: ".doc .docx .gif .jpg .jpeg .ods .odt .odp .pdf .png .ppt .pptx .rar .sld .tif .tiff .txt .xls .xlsx .xml .zip .gz". There are four input fields: "Title" (with placeholder "name by which the cited resource is known"), "File" (with placeholder "Choose File No file chosen"), "URL" (with placeholder "The URL of the document if it is external."), and "Link to" (with placeholder "Select layer, map or empty"). To the right is a "Permissions" panel with sections for "Who can view it?", "Who can download it?", "Who can change metadata for it?", and "Who can manage it? (update, delete, change permissions, publish/unpublish it)". Under "Who can view it?", the "Anyone" checkbox is checked. Under "Who can download it?", the "Choose users..." button is visible. Under "Who can change metadata for it?", the "Choose groups..." button is visible. Under "Who can manage it?", the note "Who can manage it? (update, delete, change permissions, publish/unpublish it)" is shown.

Figure 28

As it can be seen here, the access on your static map is split up into:

- view data
- download data
- change metadata
- manage data

You can choose whether you want your static map to be viewed and downloaded by:

- anyone
- any registered user
- a certain user (or group)

If you want a static map only to be viewed by certain users or a group, you have to choose **only** users who can edit column in the part **Who can view and download this data** and do not tick the "Anyone" checkbox.

SET STATIC MAP PERMISSION

By default, anyone can see and download a static map. However, the document responsible can choose to limit access to the static map to some contributors and/or groups.

To set the permissions on specific static map, click on the static map and you will see the same menu as shown in Figure 29. Click Change Permission of this Map located at the right-hand side (Figure 30) and a pop-up menu (Figure 31) will appear to set the access of the specified static map. Once the permissions are set, click "Apply" to save the permission settings.

The shown Permission Settings Panels allows to set up who can:

- View the document;
- Download it;
- Edit its metadata;

- Manage it (update, delete, change permissions, publish/unpublish).

Usually that editing of metadata and the management of a document are in charge of the responsible of the document, i.e. the contributor who uploaded it and who has those permissions by default.

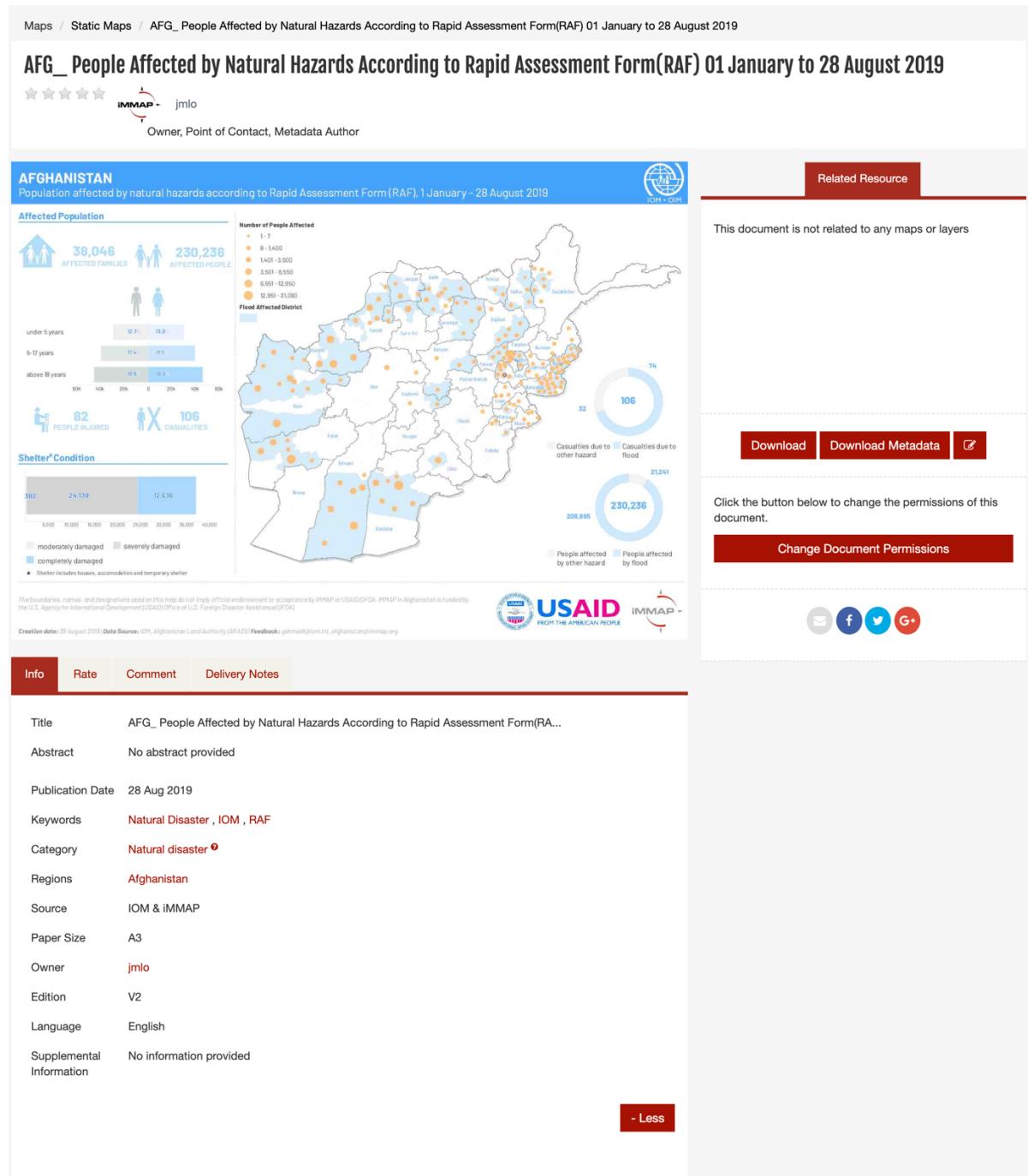


Figure 29

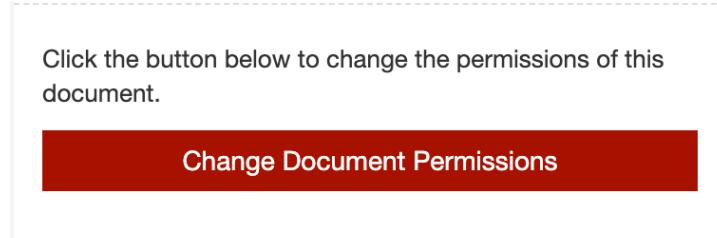


Figure 30

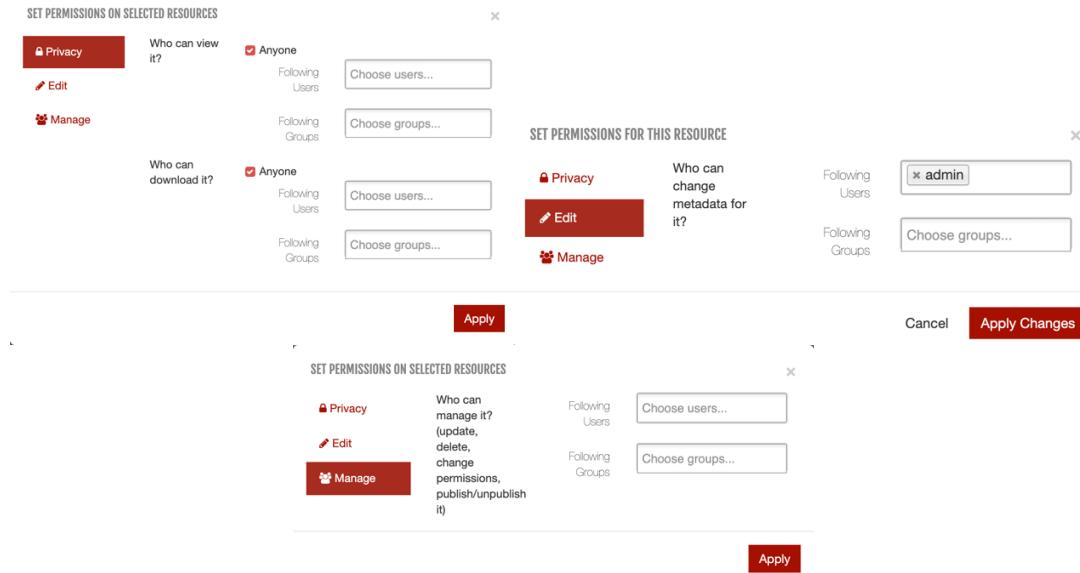


Figure 31

SET MULTIPLE STATIC MAP PERMISSION

You could also set up the access by selecting multiple static maps at once by clicking the checklist button that appear on the upper left side in each of the layer thumbnail in static maps list. Click Set Permission button on the upper right side (Figure 32) and a pop-up (Figure 31) menu will appear to set the access of these static maps.

View as: Sort by: Most recent ▾ Showing max 20 of 2860 Docs. Page 1 of 143 < >

[Set Permissions](#) [Upload Document](#)

28 August 2019

AFG_People Affected by Natural Hazards According to Rapid Assessment Form(RAF) 01 January to 28 August 2019

[View](#)

28 August 2019

AFG_IOM Humanitarian Assistance Program (HAP) Stock update – 28 August 2019

[View](#)

22 August 2019

Eshkmesh Takhar Earthquake 5.0 Magnitude

[View](#)

21 August 2019

AFG_People Affected by Natural Hazards According to Rapid Assessment Form(RAF) 01 January to 21 August 2019

[View](#)

Figure 32

CREATE AND SET GROUP PERMISSION

Major learning objectives

At the end of this section the trainee should be able to:

1. Create a group
2. Set up the permission for certain group

Through the section called Auth (See Figure 33), it has the link to access all the groups that exist at the moment by clicking "Groups" (Auth -> Groups).



Figure 33

Create a new group by clicking "Add Group" button on the upper left side (Figure 34).



Figure 34

Fill up the form and choose type of the access you granted for this group (Figure 35) and confirm it with "save" button at the bottom left (Figure 36).

A screenshot of the 'Add group' configuration page. It shows a 'Name:' field with a placeholder 'Group name'. Below it is a 'Permissions:' section. On the left, a list of 'Available permissions' is shown, including various account-related actions like 'Can add account', 'Can change account', etc. On the right, a list of 'Chosen permissions' is shown, which is currently empty. At the bottom of the permissions section are 'Choose all' and 'Remove all' buttons.

Figure 35



Figure 36

CHECKING SNAPSHOT

Major learning objectives

At the end of this section the trainee should be able to:

1. Checking if the snapshot is working as intended
2. Fixing each of the snapshot according to the kind of issue

At the homepage of ASDC, there is a section called Snapshot Section (Figure 37) which shows three different latest condition of Flood Prediction, Avalanche Prediction, and Snow Cover occurred in Afghanistan. Each of these snapshots has its own periodical update time.

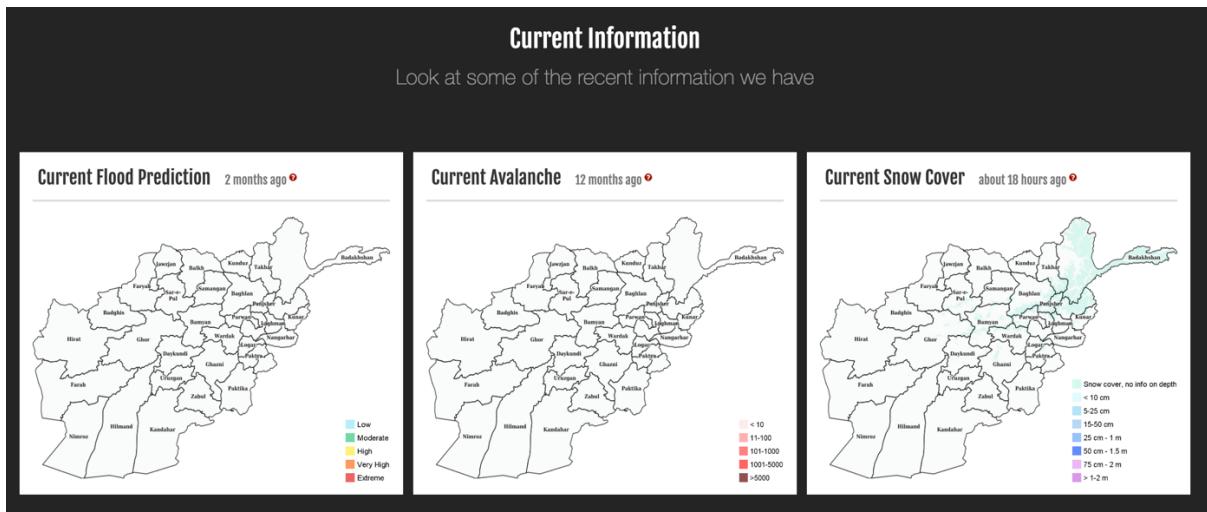


Figure 37

River flood prediction are valid for 4 days and updated every 6 hours, whereas the flash floods are valid for 6 hours and updated hourly. The map and statistics are **updated every 6 hours**.

Once a day the **avalanche risk** based on snow cover and depth is assessed. The map and statistics are updated on a daily basis (**less than 24 hours**).

Every day the **snow cover** is downloaded. The map and statistics of the snow depth are updated **4 times a day**.

If the update time showed at the homepage doesn't follow the above rules, it is a sign that celery task scheduler is not working. Restarting Celery Service in the server could fix this issue.