BUSINESS

Enterprise SMS Portal

User Manual

Version 1.1

Contents

1.	**Introduction**	**3**
2.	**Roles and Permissions**	**4**
3.	**Login**	**5**
	3.1 Forgot Password	6
	3.2 Reset Password	7
4.	**Dashboard**	**8**
5.	**Manage Sender ID**	**9**
	5.1 Add Sender ID	10
	5.2 View/Edit Sender ID	14
	5.3 Edit Rejected Sender ID	16
6.	**Manage Groups**	**17**
	6.1 Adding a Group	18
	6.2 Editing a Group	19
	6.3 Deleting a Group	21
7.	**Consent Templates**	**22**
	7.1 View a Consent Template	23
	7.2 Enable/Disable Consent Template	24
	7.3 Creating a Consent Template	25
8.	**Understanding QR Code Template**	**27**
	8.1 Viewing a QR Code Template	28
	8.2 Enable/Disable QR Code Template	29
	8.3 Creating a QR Code Template	30
	8.4 Editing a QR Code Template	32
	8.4 Viewing QR Code Uploaded Consent	33
9.	**Understanding Revoke QR Code Template**	**34**
	9.1 Viewing Revoke QR Code Template	35
	9.2 Enable/Disable Revoke QR Code Template	36
	9.3 Creating Revoke QR Code Template	37
	9.4 Editing a Revoke QR Code Template	39
	9.5 QR/Revoke QR Code Error Codes	40
10.	**Consents**	**41**
	10.1 Consents Upload	42
	10.1.1 Understanding Consent Upload Error Codes	47
	10.1.2 Creating Consents Upload Activity	48
	10.1.3 Consents Upload by Analog Type	50
	10.1.4 Consents Upload by Digital Type	51
	10.1.5 Creating Consents Upload Activity	52
	10.1.6 Preparing CSV Files Format	53
	10.1.7 QRCode Consents Uploads by Digital Type	57
	10.2 Consents Revoke	59
	10.2.1 View Consents Revoke Activity	60
	10.2.2 Create Consents Revoke Activity	62
11.	**Search Consent**	**66**
12.	**Enterprise Consents**	**70**
13.	**Consent Downloads**	**72**
14.	**Manage Users**	**75**
	14.1 Adding a new User	76
	14.2 Adding a new Normal/Reporting User	77
	14.3 Resending Activation Link	79
	14.4 Suspending a User	80
	14.5 Deleting a User	81
	14.6 Adding an API User	82
	14.7 Viewing/Editing an API User	83
15.	**Profile**	**84**
	15.1 Update Password	86
	15.2 Update Account Details	87
16.	**API Documentation**	**89**

1. Introduction

As per the TDRA Mobile SPAM Policy, Enterprises who plan to send Promotional SMS to mobile subscriber are required to provide valid consents of their customers to the licenced telecom operators in UAE. Upon receiving Promotional SMS from the Enterprises the telecom operators will ensure the presence of a valid consent in the system and no blocking request is present against the Sender ID by the mobile subscriber before delivering the Promotional SMS to the mobile subscriber. In absence of a valid consent or in case of availability of a blocking request, no Promotional SMS will be delivered to the mobile subscriber.

To be inline with TDRA Mobile SPAM Policy requirements to control SPAM, du has launched the Enterprise SMS Portal for Enterprises ("Brands") who plan to send promotional SMS to their customers. The portal provides the Enterprises ("Brands") to open their accounts with du and directly apply for Promotional Sender IDs, manage and upload consent information of their end customers.

The Enterprise SMS Portal offers the following functionalities to customers:

- Registration of Promotional Sender IDs
- Management of Consent Templates
- Management of Sender ID Groups
- Management of User Profiles
- Management of Mobile Subscriber consent information
    - Upload of consents
    - Revocation of consents
    - Searching of consents
    - Download of consent information
- Real Time Consent Acquisition & Revocation capability via QR Code functionality
- Consent Uploads & Revocation via API functionality

In order to deliver Promotional SMS to mobile subscribers. Enterprises ("Brands") will be required to follow the below steps to successfully upload mobile subscribers consent on to the Enterprise SMS Portal.

Step 1: Register a Promotional Sender ID

Step 2: Create a Consent Template once Sender ID is approved

Step 3: Upload the consent information using the approved Sender ID and Consent Template via:

a) Manual Consent Upload Process via Analog Type or Digital Type OR
b) Real time Consent Acquisition & Upload by QR Code Functionality OR
c) Upload of Consents via API Functionality

This user manual provides the Enterprises ("Brands") the information on how to operate the above steps on the Enterprise SMS Portal. Each section of the user manual contain guidelines, business rules and instructions required to complete each step.

2. Roles and Permissions

The Enterprise SMS Portal offers the flexibility to create multiple type of User roles for the Enterprise SMS Portal account.

Admin User: is the account administrator who can has full access to the account. Admin User can perform all actions on the account including creation and management of new Users, management of Sender IDs and consents management.

Normal User: is created by the Admin User and has limited access to the account. Normal are limited to management of Sender IDs and consents only.

Reporting User: is created by the Admin User and has only view only access to the information of the account. They cannot edit any information.

Below table provides information on the view/edit rights for all type of User roles:

Role	Profile	Profile - Edit Account Details	Dashboard	Manage Users	Sender ID/ Groups	Consent/ QR Code Templates	Consent Search/ Downloads	Consents upload	Consents Revoke
Admin User	View/Edit	View/Edit	View	View / Edit / Add	View / Edit / Add	View / Edit / Add	View / Edit / Add	View / Edit / Add	View / Edit / Add
Normal User	View/Edit	-	View	-	View / Edit / Add	View / Edit / Add	View / Edit / Add	View / Edit / Add	View / Edit / Add
Reporting User	View/Edit	-	View	-	View	View	View	View	View

3. Login

Log into Enterprise SMS Portal

This module allows Enterprise Users to log into the Enterprise SMS Portal using registered credentials.

Applicable to:

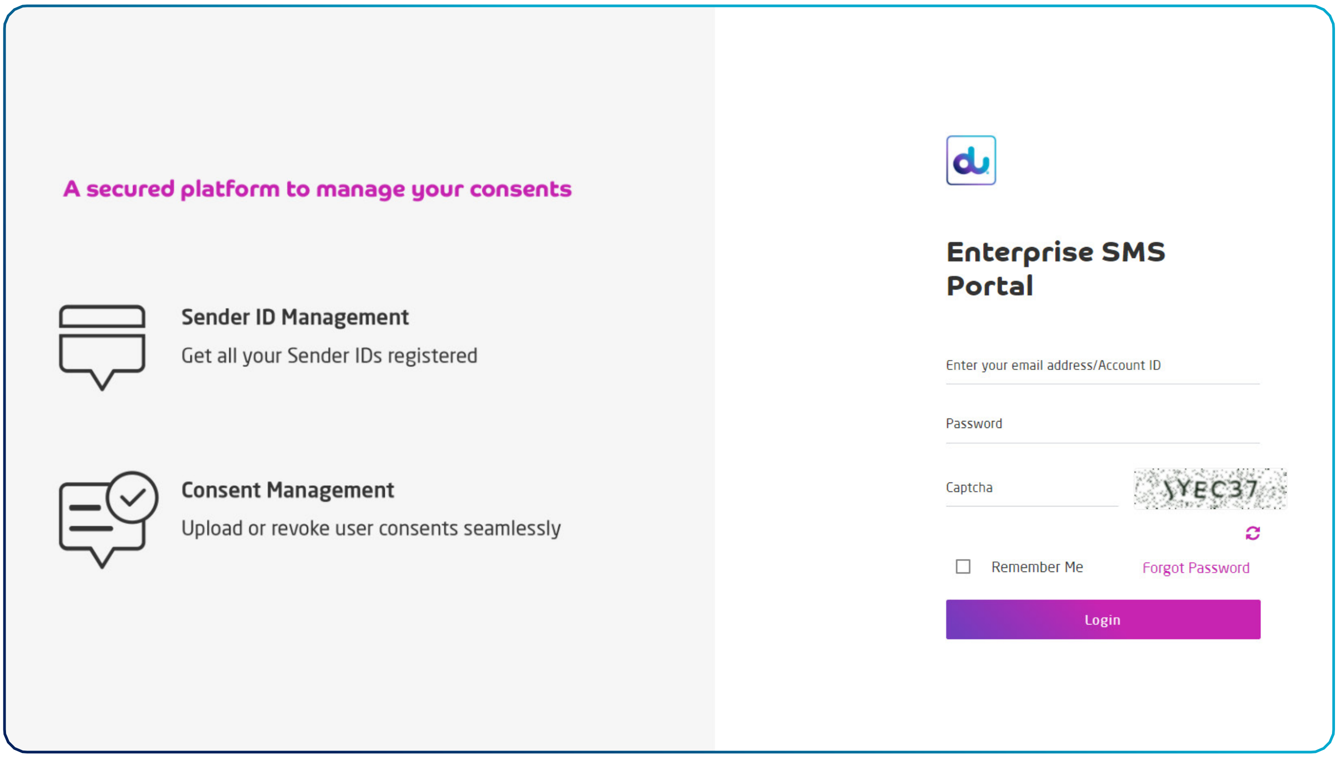
- Admin User
- Normal User
- Reporting User

Module Functionalities:

1. Enables registered Users to login to the Enterprise SMS Portal
2. Enables 'Forgot password' functionality to generate a new password
3. Enables 'Password reset' functionality in case account is locked
4. Allows Users to invoke 'Remember me' functionality

Business Rules:

1. Only Admin Users are allowed to login using registered emails as well as Entity IDs
2. Normal Users and Reporting Users will be allowed to login using their registered email IDs
3. System locks the account in case wrong password is entered consequently 3 times



3.1 Forgot Password

This module allows Users to generate a new password in case they forget the registered password.

Applicable to:

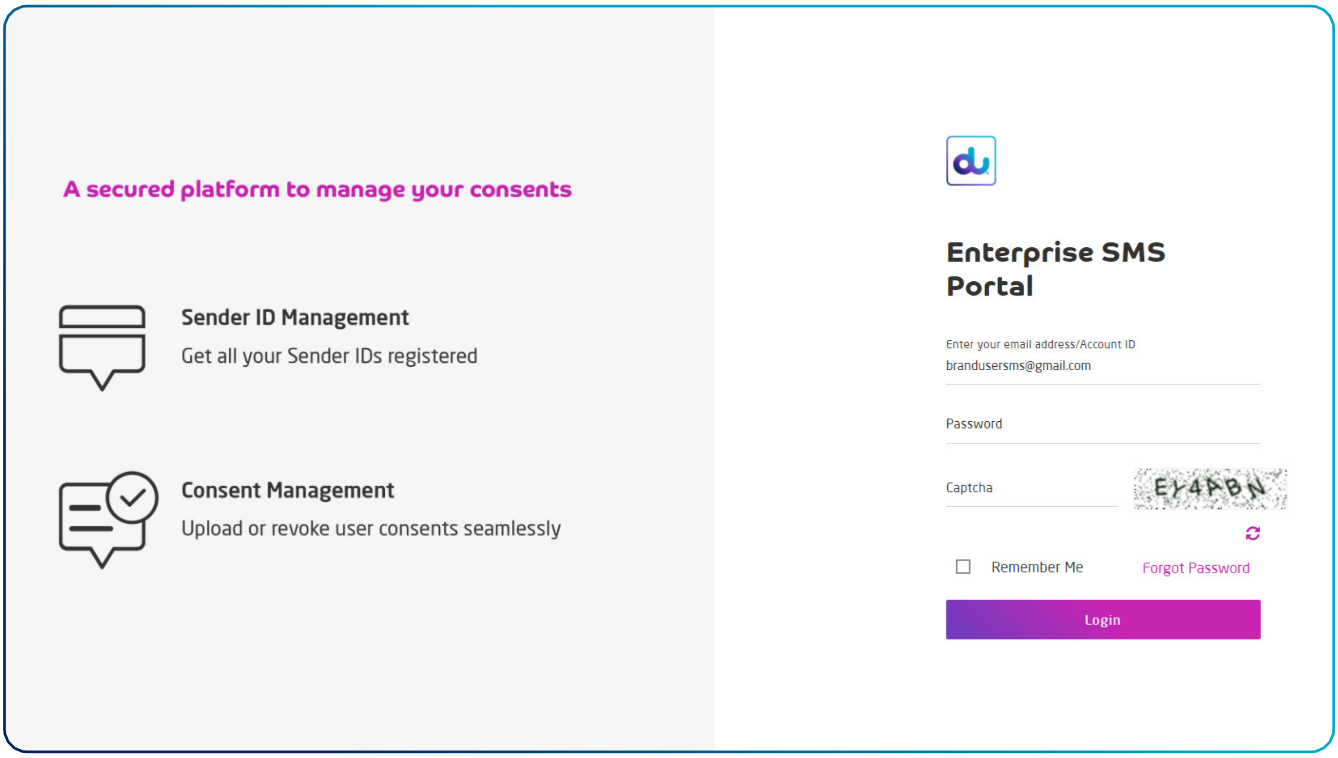
- Admin User
- Normal User
- Reporting User

Module Functionalities:

1. Enables Users to generate the re-set password link.

Business Rules:

1. Enterprise Users needs to provide a valid registered email ID to generate re-set password link.
2. Once an email address is entered, "Forget Password" link will automatically become visible.
3. System returns error code in case the provided email ID is not registered.
4. System sends the generated password link to the registered email ID.



3.2 Reset Password

This module allows Users to re-set their password in case the account is locked.

Applicable to:

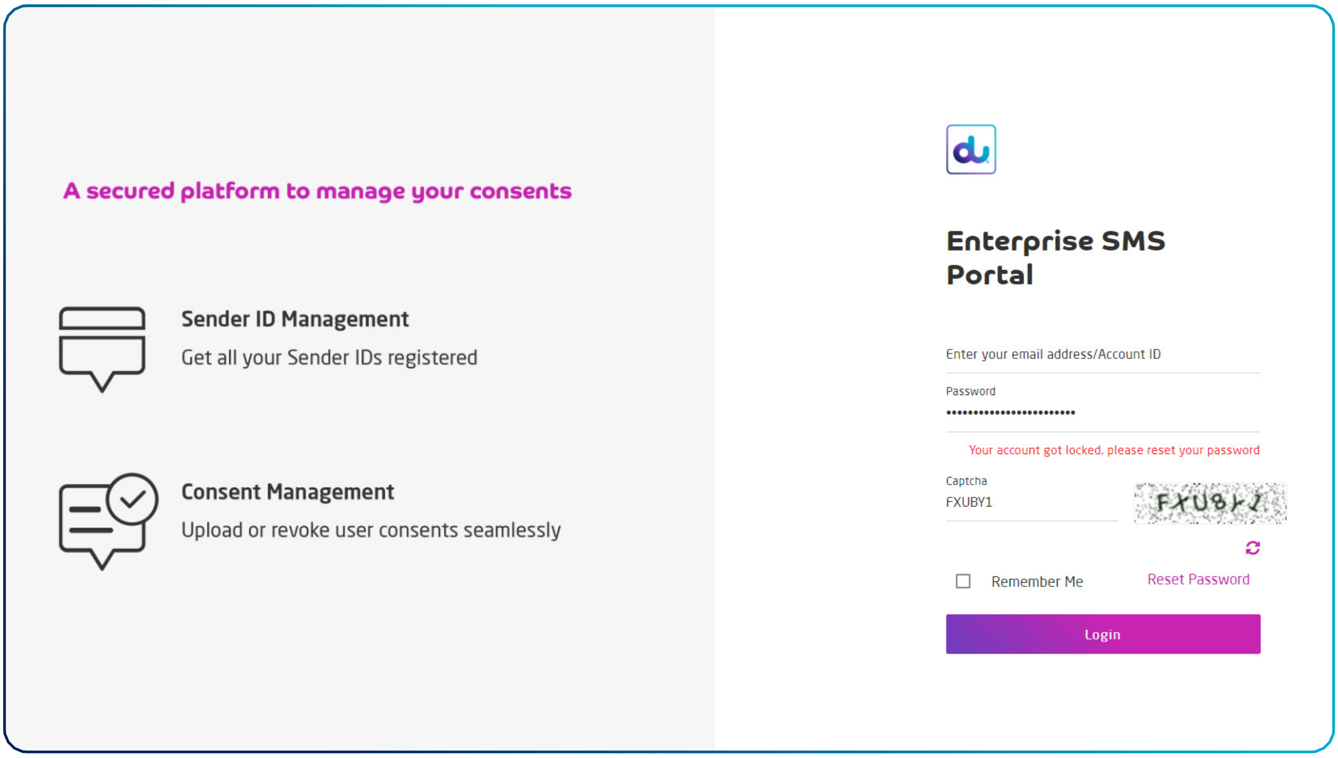
- Admin User
- Normal User
- Reporting User

Module Functionalities:

1. Enables Users to generate the re-set password link to unlock the account.

Business Rules:

1. To unlock account, admin User needs to provide entity ID along with the registered email. The entity ID can be found in the activation email sent to the admin User at the time of account activation.
2. Normal Users and Reporting User need to provide the registered email only for generating the re-set password link.
3. System will lock the account in case of three consecutive wrong passwords.
4. System sends the generate password link to the registered email ID.



4. Dashboard

The dashboard gives an overview of account activities and information related to the Sender ID(s), Consent Templates and Consents.

Applicable to:

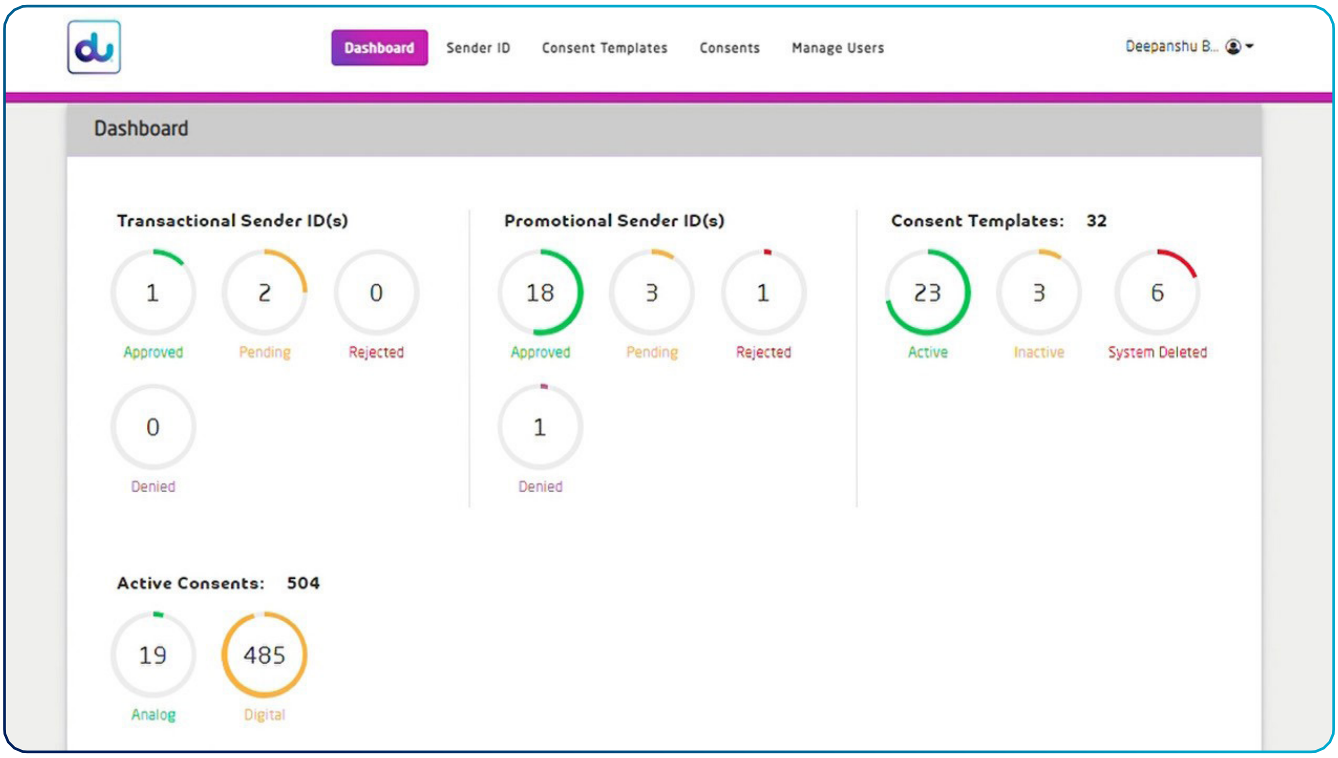
- Admin User
- Normal User
- Reporting User

Module Functionalities:

1. Enables Users to check the overview of the Enterprise account in terms of Sender IDs, Consent Templates and Consents.

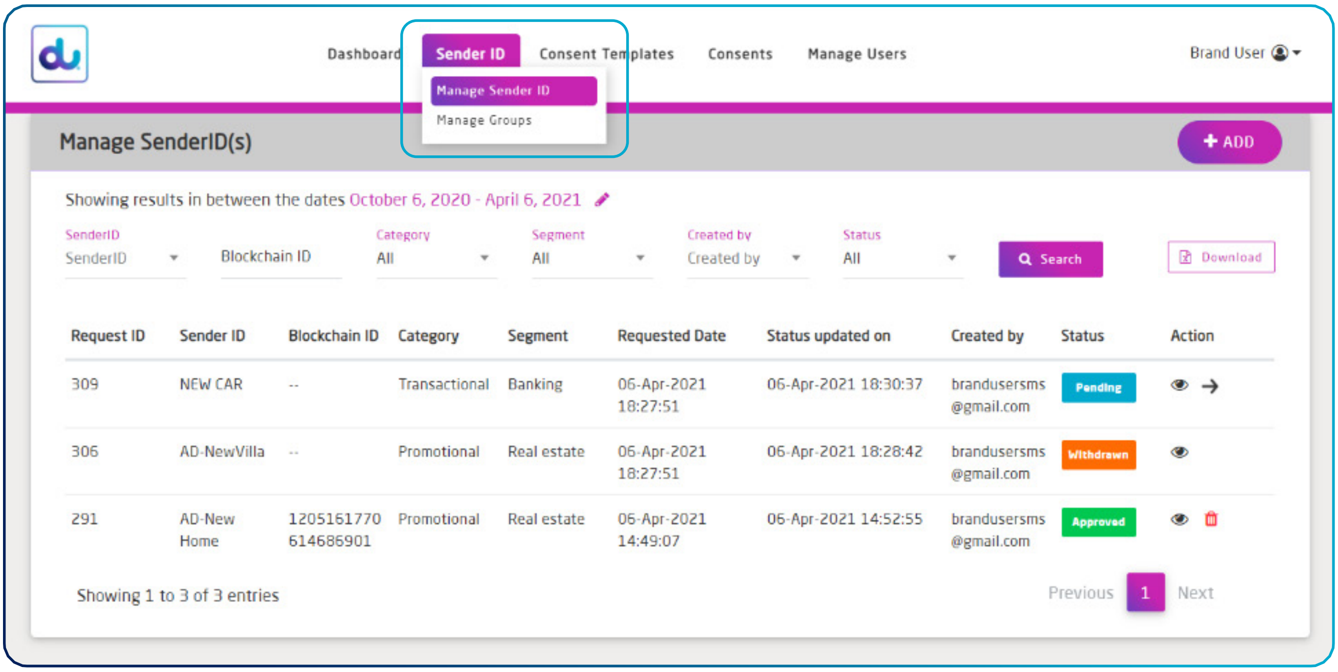
Business Rules:

1. System displays counts of registered/requested Sender IDs with respect to their status.
2. System displays counts of Consent Templates with respect to their status.
3. System displays counts of active consents bifurcated to highlight analog and digital consents.



5. Manage Sender ID

This module allows Users to view all registered Sender IDs along with their details. Through this module, the Admin and Normal Users will be able to take required actions such as apply, withdraw, delete and edit Sender ID data.



Applicable to:

- Admin User
- Normal User
- Reporting User

Module Functionalities:

1. Enables User to view all registered/requested Sender IDs as a list.
2. Enables User to search specific Sender IDs using available filters.
3. Enables User to add new Sender IDs.
4. Enables User to take actions such as withdraw, view details, delete, edit on Sender IDs.
5. Enables User to download list of Sender IDs.
6. Enables User to review all uploaded documents for Sender IDs.

Business Rules:

1. Admin and Normal User can only add or edit Sender IDs. Reporting User can only view details.
2. System displays withdraw icon on all Sender IDs that are in a pending state.
3. System displays delete icon on all Sender IDs that are in an approved state.
4. System to list all Sender IDs as per configured search/filter.
5. Edit action will only be applicable to the rejected Sender ID.

5.1 Add Sender ID

This module allows Admin and Normal Users to create new Sender IDs. User is allowed to choose their desired Sender ID as per availability and upload relevant supporting documents for its approval.

Applicable to:

- Admin User
- Normal User

Module Functionalities:

1. Enables Users to add new Sender IDs for registration (subject to availability).
2. Enables Users to add multiple Sender IDs in a single request.
3. Enables Users to add supporting documents along with the request.
4. Enables Users to choose category of Sender ID i.e. Transactional or Promotional.
5. Enables Users to select segment of Sender ID e.g. Banking, Real Estate, etc.

Business Rules:

1. Admin and Normal Users will only be able to add available Sender IDs.
2. Sender IDs that available in the system can be applied only.
3. To submit a Sender ID registration request, Users will have to submit valid documents.
4. Users will be able to view/edit all selected Sender ID prior to submission.
5. User will only be allowed to add a maximum of 10 Sender IDs at a single time.
6. Submission of Sender ID requests will only be allowed once supporting documents are uploaded.
7. Users will be allowed to submit maximum of 10 supporting documents per request.
8. Enterprise Users will be able to add explanation for Sender IDs while applying for Sender IDs.

Promotional Sender ID Rules:

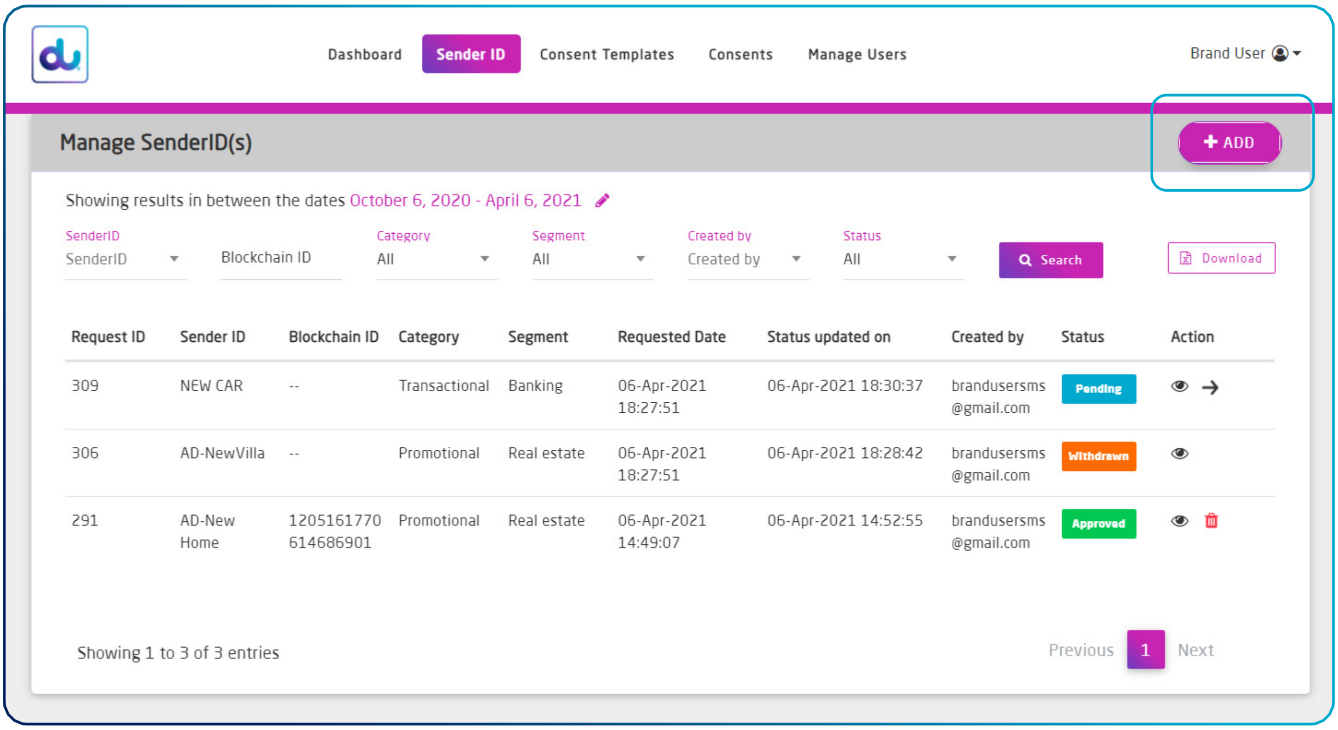
- System will always add prefix ”AD-“ to the Sender ID
- Length of Sender ID: min - 3 and max - 8 (excluding ”AD-”)
- Max special characters allowed: 2
- Promotional Sender ID cannot be all numeric
- Sender ID can contain alphabet (A-Z) (a-z), number (0-9)
- Special characters are allowed (“”” “&” “,” “.” “-“ “_” and “space”)
- Available Sender ID segments are: Banking & Finance Services, Real Estate Services, Health Services, Education Services, Retail Services and Tourism Services.

Transactional Sender ID Rules:

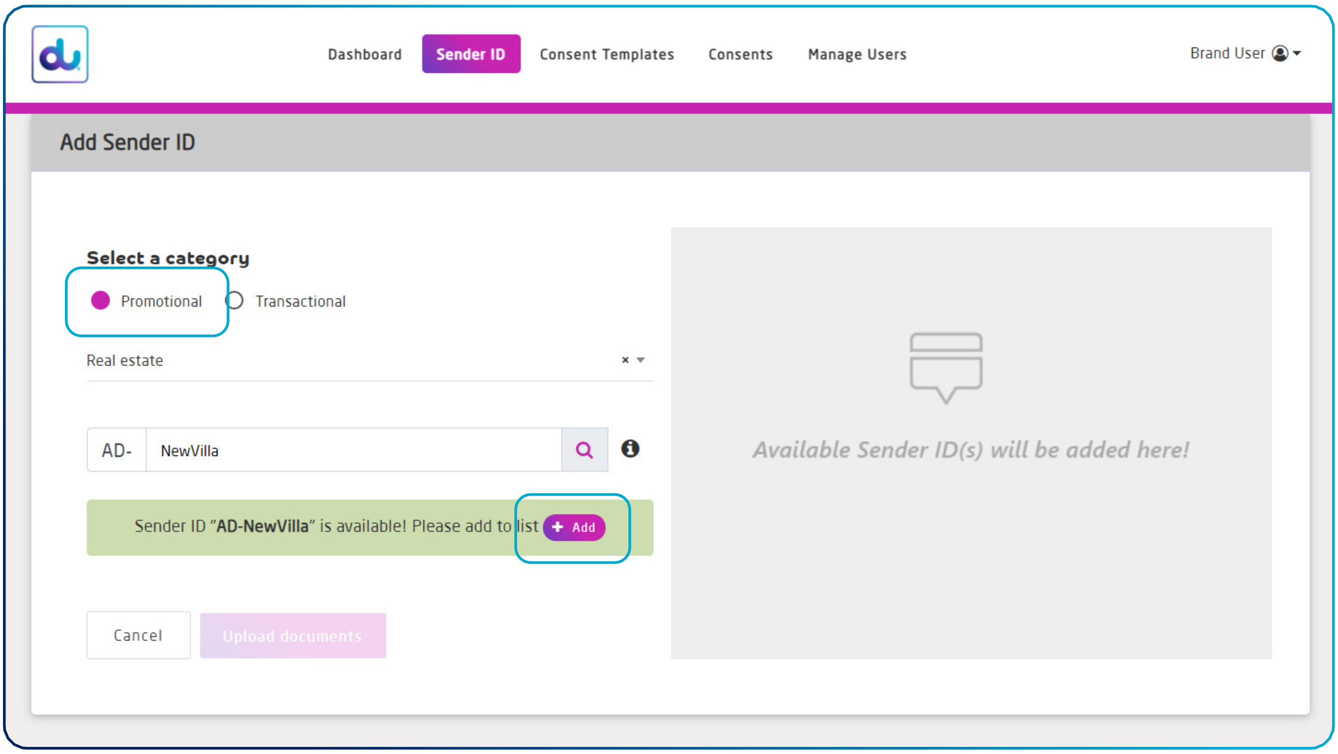
- No prefix will be attached
- Length of Sender ID: min – 3 and max – 11
- Max special characters allowed: 2
- Sender ID can contain alphabet (A-Z) (a-z), number (0-9)
- Special characters are allowed (“”” “&” “,” “.” “-“ “_” and “space”)
- Available Sender ID segments are: Banking & Finance Services, Real Estate Services, Health Services, Education Services, Retail Services, Tourism Services, Government and Energy & Utilities.

5.1 Add Sender ID

To add a new Sender ID, User to click "+ADD" button on the Manage Sender ID page as shown below:

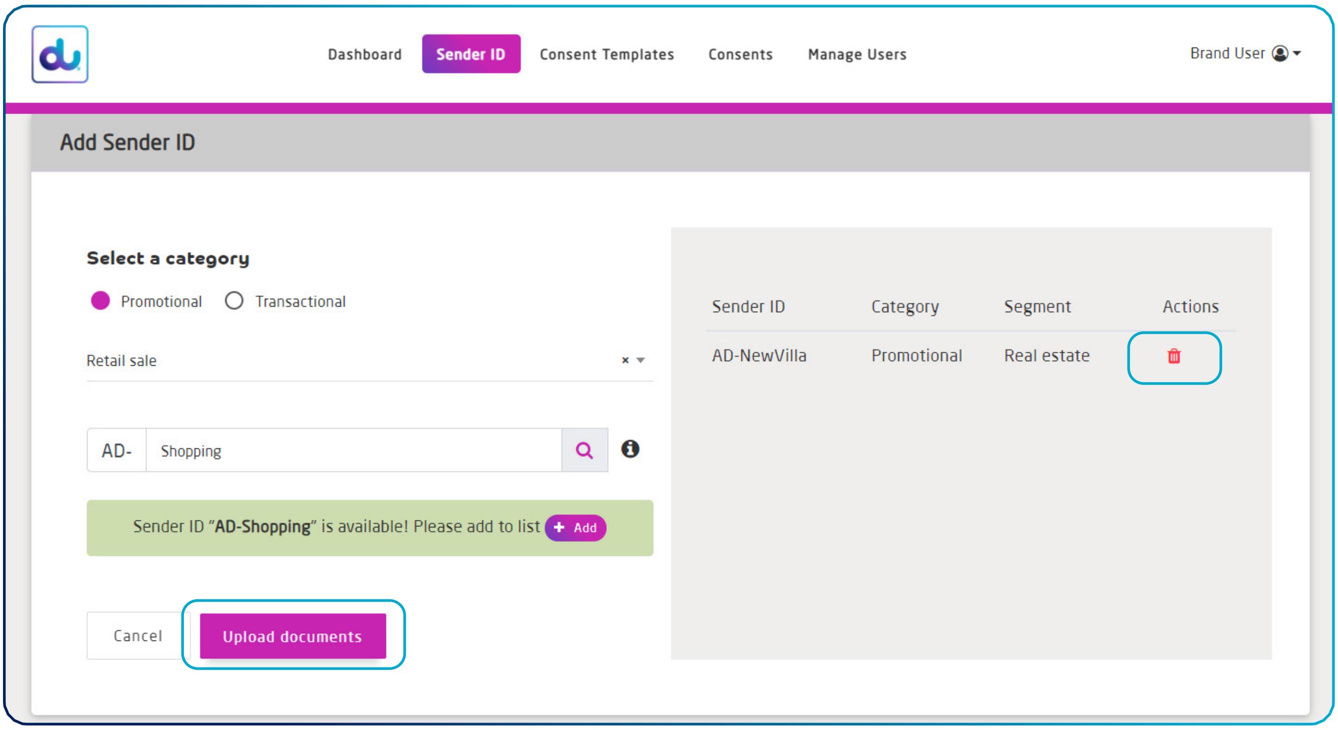


Once "+Add" button is clicked, Add Sender ID page will open as shown below. User can select the Sender ID category (Promotional or Transactional) and the segment from the drop down list, enter the Sender ID in search box and click the search button. If Sender ID is available, User will be notified and User can add the Sender ID to the list.

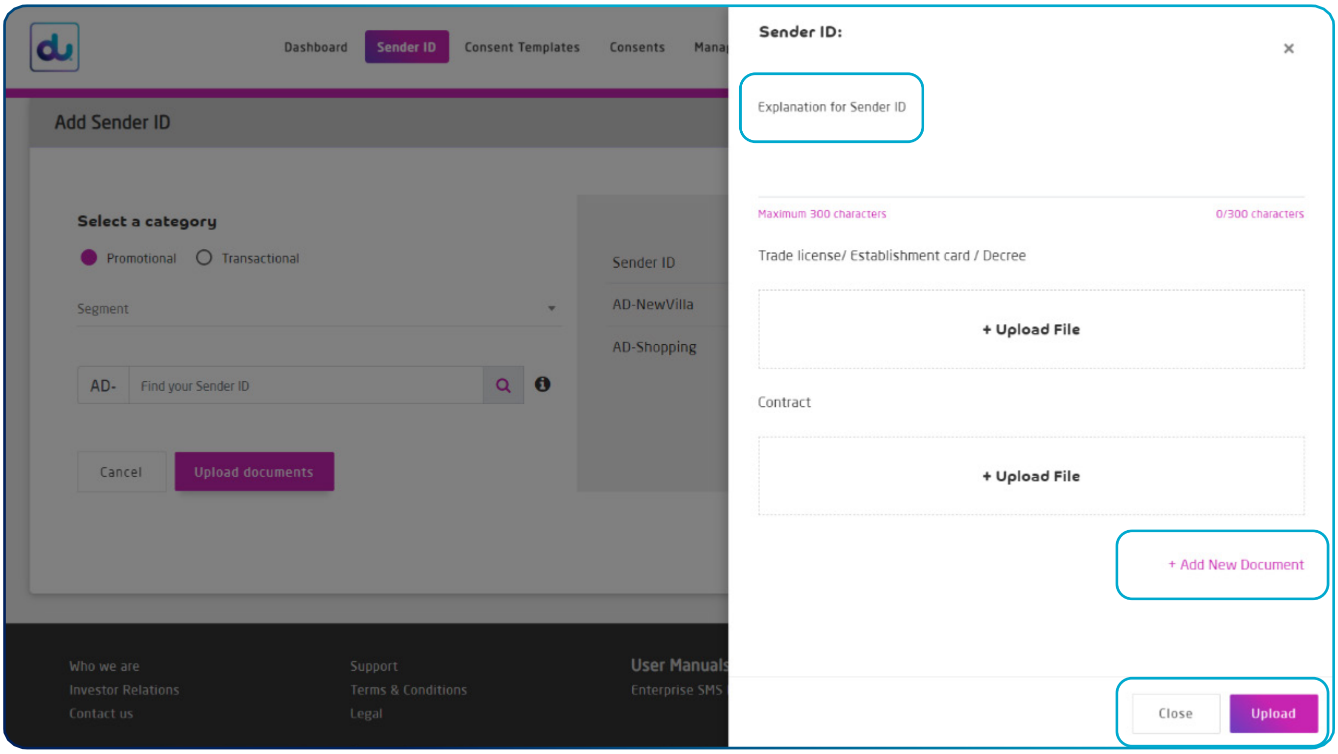


5.1 Add Sender ID

Once a Sender ID is added to the list, the User can select more Sender IDs up to max 10 at a time and add them to the list. User can also delete the selected Sender ID from the list prior to submission for approval. Once Sender IDs are added to the list, the User will click "Upload Documents" to upload required Sender ID documentation.



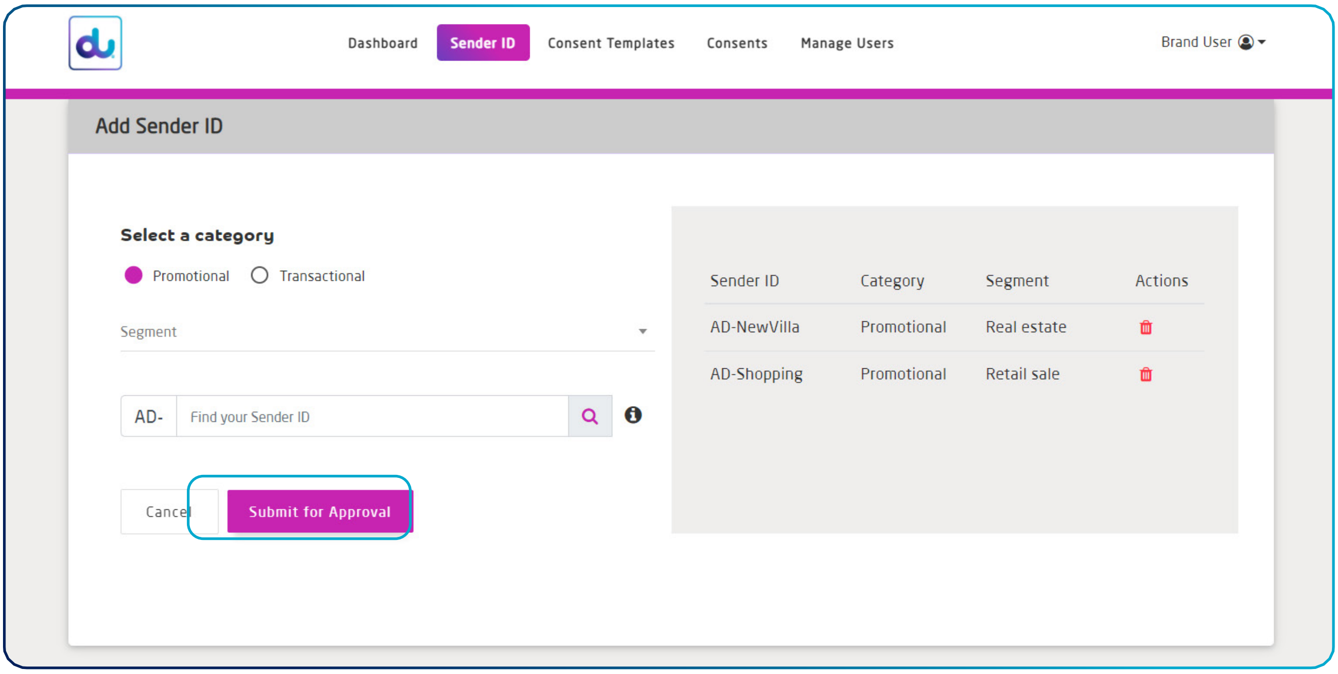
The User will upload all documents each time as mentioned on the Enterprise SMS Portal account opening form every time a new Sender ID is applied. Under 'Explanation for Sender ID' section, User will enter purpose of the Sender ID and upload required documents.



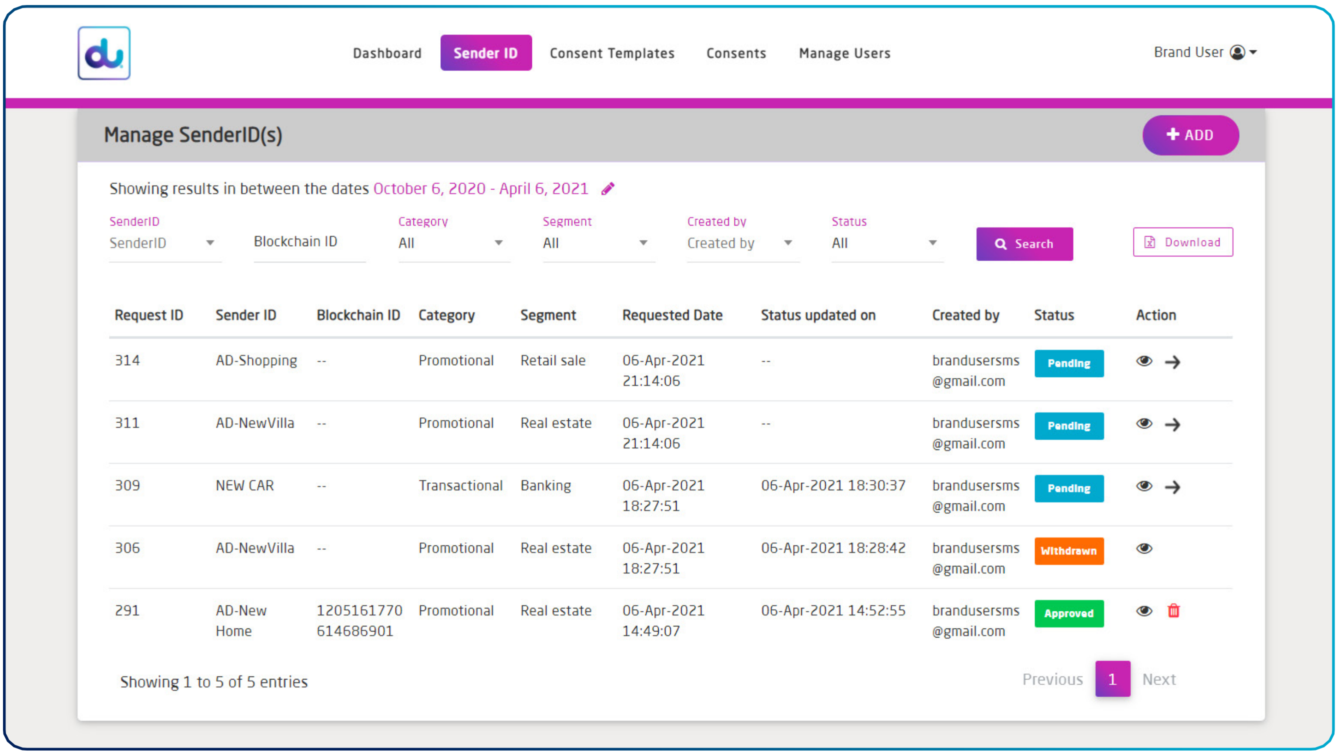
5.1 Add Sender ID

Documents in JPEG and PDF formats can be uploaded only. It is mandatory to attach a valid Trade Licence/ Establishment Card/Decree and duly filled Enterprise Account Opening Form as minimum set of document. In case other documents are required e.g. Trade Name certificates or approval from requisite authorities then such documents can be uploaded. User can add more documents by clicking "+Add New Document" button. Once all documents have been uploaded, User can click "Upload" button to finish the document upload activity.

Once documents have been successfully uploaded, User can click "Submit for Approval" button as shown below to complete Sender ID registration request.

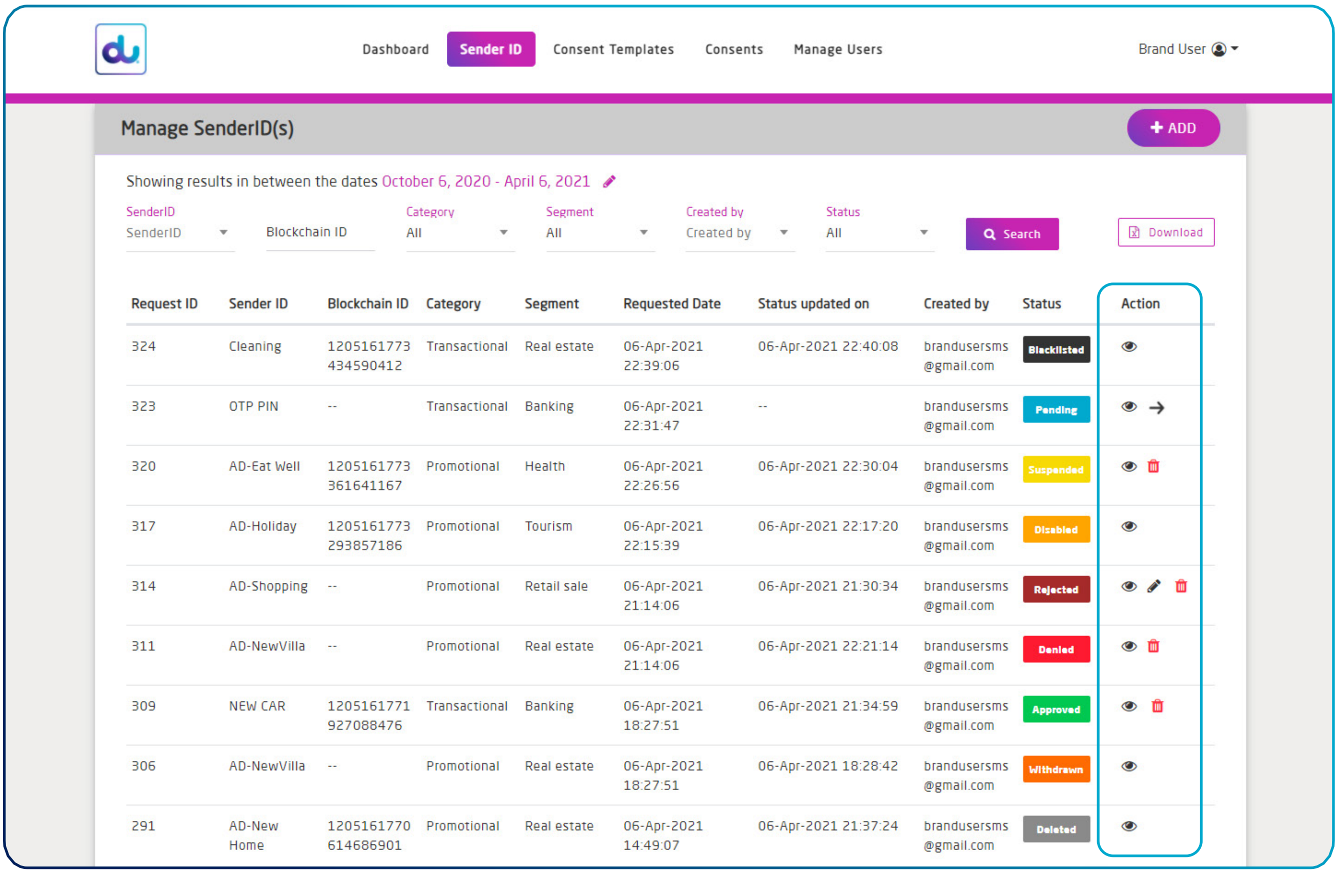


Once new Sender ID request is submitted, User can see the applied Sender ID with "Pending" Status.



5.2 View/Edit Sender ID

The Manage Sender ID module allows the User to perform various actions on the Sender IDs. Under the "Action" tab, the User can perform certain actions as per the current status of each Sender ID.



Following are the statuses and editable actions that can be performed on Sender IDs based on their status.

'Approved' Status: A Sender ID in an 'Approved; status is approved by du and can be used to upload consent information. Approved Sender IDs cannot be edited however can only be deleted by the User. Promotional SMS can only be sent to the sender ID with 'Approved' status. User can view the documentation against the sender by clicking the "EYE" icon under the 'Action' tab.

'Pending' Status: A Sender ID in a 'Pending' status is yet to be approved by du. Once a Sender ID in the 'Pending' status is approved, its status will turn to 'Approved'. Sender ID in 'Pending' status cannot be edited however can only be withdraw by the User in case Sender ID is no more required. User can view the documentation against the sender by clicking the "EYE" icon under the 'Action' tab.

'Rejected' Status: A Sender ID in a 'Rejected' status has been rejected by du due to missing documentation or any other reason. The User can edit the Sender ID by clicking the "Pen" icon and can change Sender ID segment and/or upload missing documentation or amend existing uploaded documents to re-submit for Sender ID approval. User can view the rejection reason or existing documentation against the sender by clicking the "EYE" icon under the 'Action' tab.

'Withdrawn' Status: A Sender ID is in 'Withdrawn' status when it has been revoked by the User prior to Sender ID being approved by du. In case Sender ID is already in 'Approved' or 'Rejected' status, then it cannot be withdrawn. User can view the documentation against the sender by clicking the "EYE" icon under the 'Action' tab.

5.2 View/Edit Sender ID

'Deleted' Status: A Sender ID is in 'Deleted' status when it has been deleted by the User. Sender IDs in 'Approved', 'Denied', 'Rejected' and 'Suspended' statuses can be deleted. Once a Sender ID is deleted, all consent information stored against the Sender IDs are deleted. No Promotional SMS can be sent using this Sender ID anymore. User will be required to re-apply Sender ID and again upload mobile subscriber consent information against the Sender ID for all customers. User can view the documentation against the sender by clicking the "EYE" icon under the 'Action' tab. Deleted Sender ID are automatically removed from any Groups they are tagged with.

'Denied' Status: A Sender ID is put in "Denied" status by du when it cannot be approved due to any reason. Sender IDs in 'Denied' status can be deleted by the User. User can view reason for denial or the documentation against the sender by clicking the "EYE" icon under the 'Action' tab.

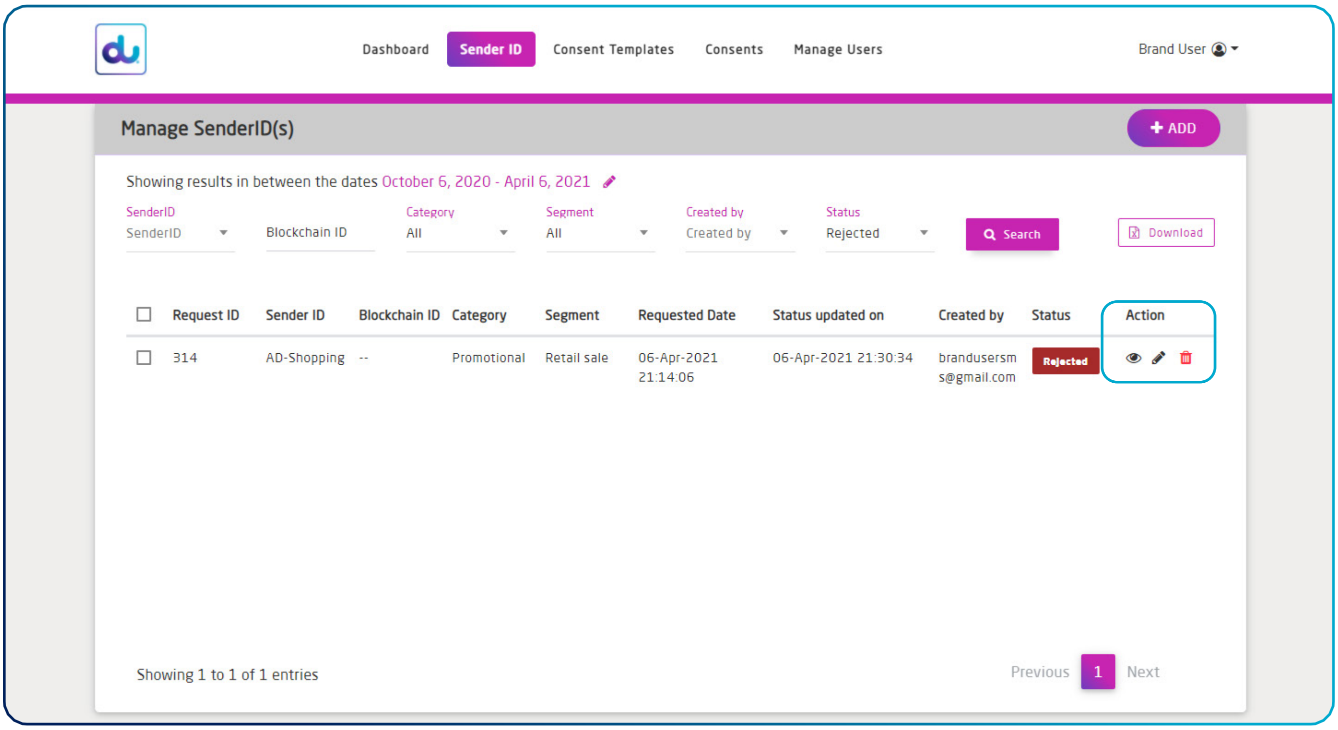
'Suspended' Status: A Sender ID is put in 'Suspended' status by du in case of any non-compliance of the terms and condition of use of Enterprise SMS Portal, Mobile SPAM Policy or Bulk SMS Service provided by du. In 'Suspended' status, the User will not be able to send Promotional SMS to its customers however can upload/revoke mobile subscriber consent information against the Sender ID. All consents against the Sender IDs will be disabled automatically. Once the Sender ID is made active again, all consent will be automatically enabled. User can view the suspension reason and/or documentation against the sender by clicking the "EYE" icon under the 'Action' tab.

'Disabled' Status: A Sender ID is put in 'Disabled' status by du in case of any non-compliance of the terms and condition of use of Enterprise SMS Portal, Mobile SPAM Policy or Bulk SMS Service provided by du. In Disabled status, the User will neither be able to send Promotional SMS to its customers nor can upload/revoke mobile subscriber consent information against the Sender ID. All consents against the Sender IDs will be disabled automatically. Once the Sender ID is made active again, all consent will be automatically enabled. Disabled Sender IDs cannot be deleted by the User. User can view the documentation against the sender by clicking the "EYE" icon under the 'Action' tab. Disabled Sender ID are automatically removed from any Groups they are tagged with.

'Blacklisted' Status: A Sender ID is put in "Blacklisted" status by du in case of a major non-compliance of the terms and condition of use of Enterprise SMS Portal, Mobile SPAM Policy or Bulk SMS Service provided by du. All consents against the Sender IDs will be deleted automatically and User will not be able to send Promotional SMS to its customers. A Blacklisted Sender ID will not be available for re-registration. User can view the blacklisting reason and/or documentation against the sender by clicking the "EYE" icon under the 'Action' tab.

5.3 Edit Rejected Sender ID

In case a requested Sender ID is not denied by du however only temporarily rejected, this functionality allows Users to resubmit missing documentation or correct Sender ID information as requested by du. In case the User submits the correct information or uploads required documentation, the Sender ID will be approved.



To view the rejection reason, User can click on the "Eye" icon under the 'Action' tab. The User can act on the details to resubmit proper documentation and re-submit approval.

By clicking on the "Pen" icon under the 'Action' tab, the User can edit previously uploaded details of Sender ID.

The User can also edit the Sender ID segment, modify already uploaded documents or add new supporting documents. Users will not be able to modify selected Sender IDs or change its category.

6. Manage Groups

This module allows Users to tag multiple promotional Sender IDs together in a Group in order to perform an action on multiple Sender IDs in a single activity to save time. Multiple Groups can be created and multiple Sender ID can be tagged to multiple Group to perform common action. Group are useful to use when same activity is required to be performed on multiple Sender IDs e.g. consent information against a single mobile subscriber for multiple Sender IDs can be uploaded in a single activity if all Sender ID are made part of a common Group.

Applicable to:

- Admin User
- Normal User
- Reporting User

Module Functionalities:

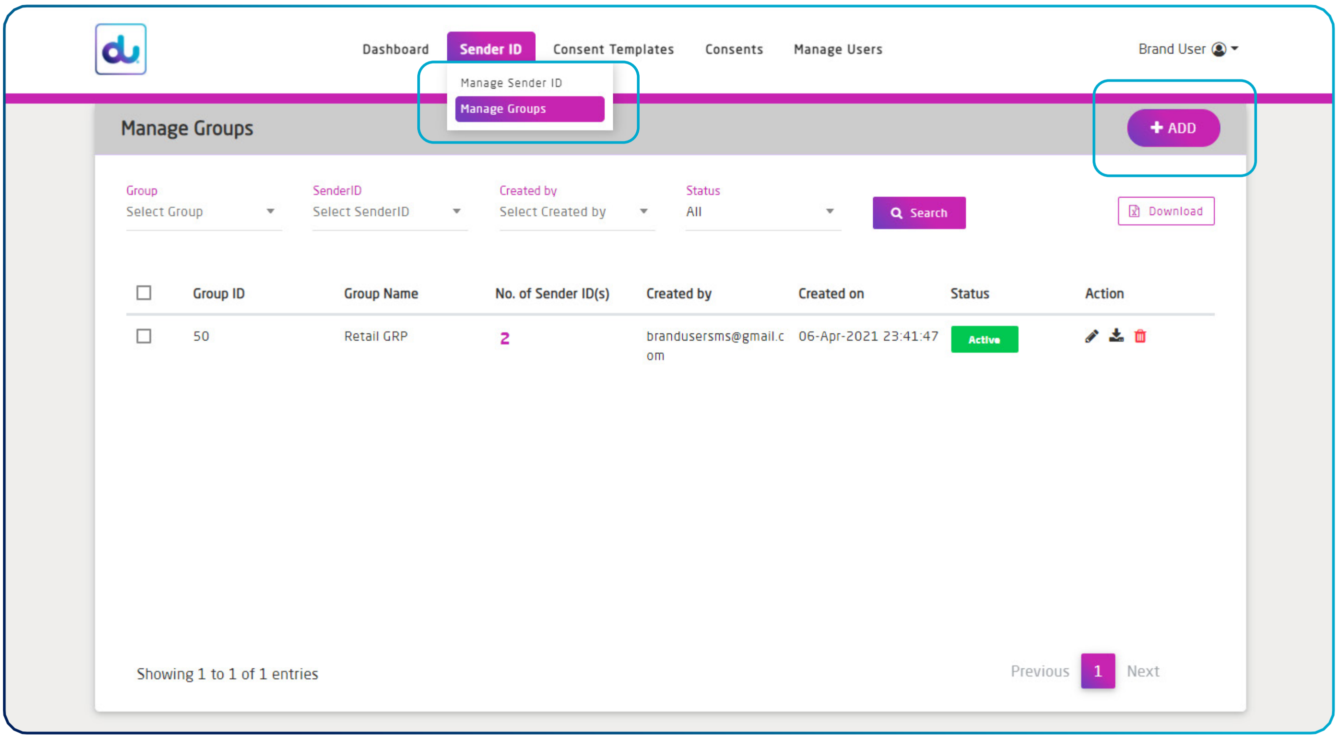
1. Enables Users to create new Groups on the account.
2. Enables Users to edit existing Groups i.e. add/remove Sender ID to/from a Group.
3. Enables Users to delete the existing Group.
4. Enables Users to download a list of Group.
5. Enables Users to search Groups using available filters.

Business Rules:

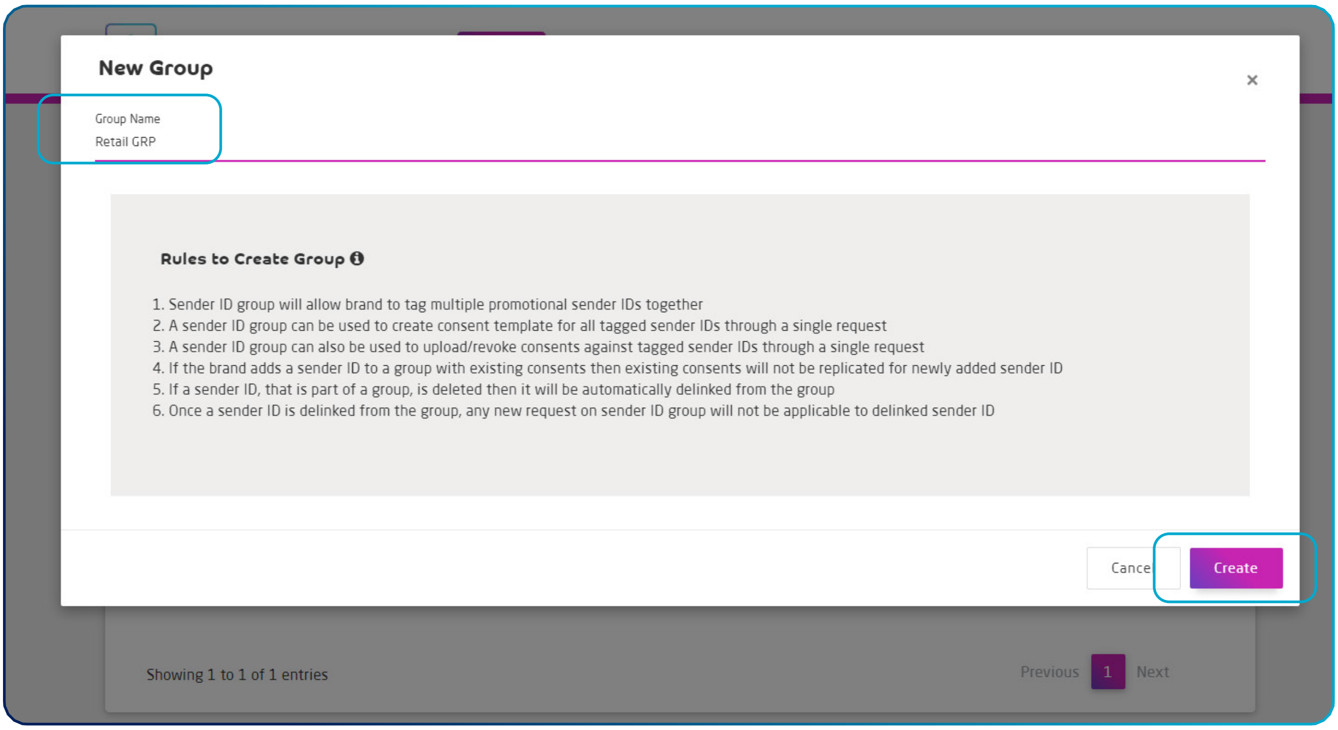
1. Only promotional Sender IDs can be tagged to a Group.
2. Groups are limited to perform common activities such as upload or revoking a consent for a number of Sender IDs that are part of the Group.
3. Adding or deleting a Sender ID from a Group has no impact on Sender ID or mobile subscribers consent information associated with a Sender ID. Similarly deleting a Group has no impact on the list of Sender IDs which were part of the Group at the time of deletion.
4. If a Group is used to tag multiple Sender ID, then the action performed on the Group will reflect on all the Sender IDs which are part of the Group at any point of time e.g. if a Group has 3 Sender IDs and a consent upload activity was performed, then consent information will be replicated against all Sender ID in that Group.
5. If a Group which has been previously used for any activity is modified to add or remove certain Sender IDs, then the next activity will only be performed on the Sender ID which are currently part of the Group. Sender IDs which are removed from the Group remain unaffected.
6. If a Sender ID which was part of an active Group is deleted or disabled, then the Sender ID is automatically removed from the active Group. Any activity done on the Group will not have any impact on the deleted Sender ID or its associated consent information.
7. Users can create a Consent Template for a Group. All Sender IDs that are part of the Group will automatically use the same Consent Template when consents are uploaded.

6.1 Adding a Group

To add a Group, click on the "Manage Groups" option of the 'Sender ID' tab on the Dashboard as shown below to open the 'Manage Groups' page. Click on the "+ADD" action button to create a new Group.

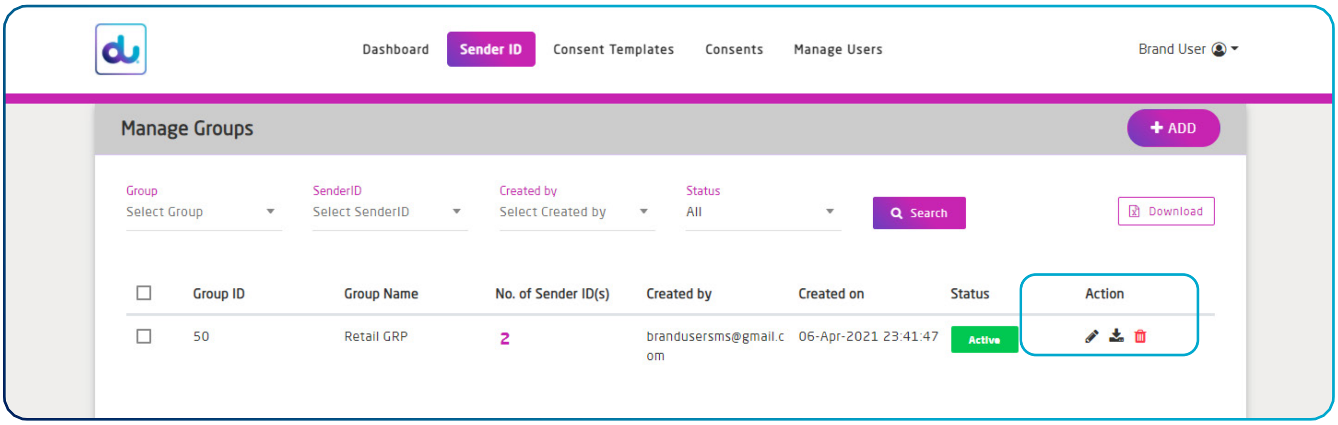


Once the "+ADD" button is clicked, a Group creation page is opened. Enter the name of the Group in the text box and click "Create" button to create the new Group.

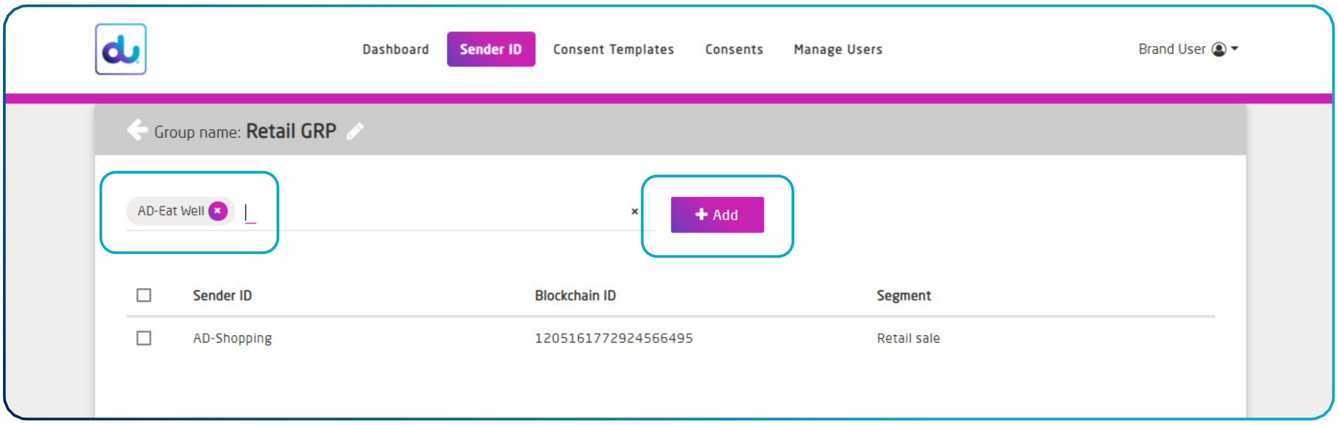


6.2 Editing a Group

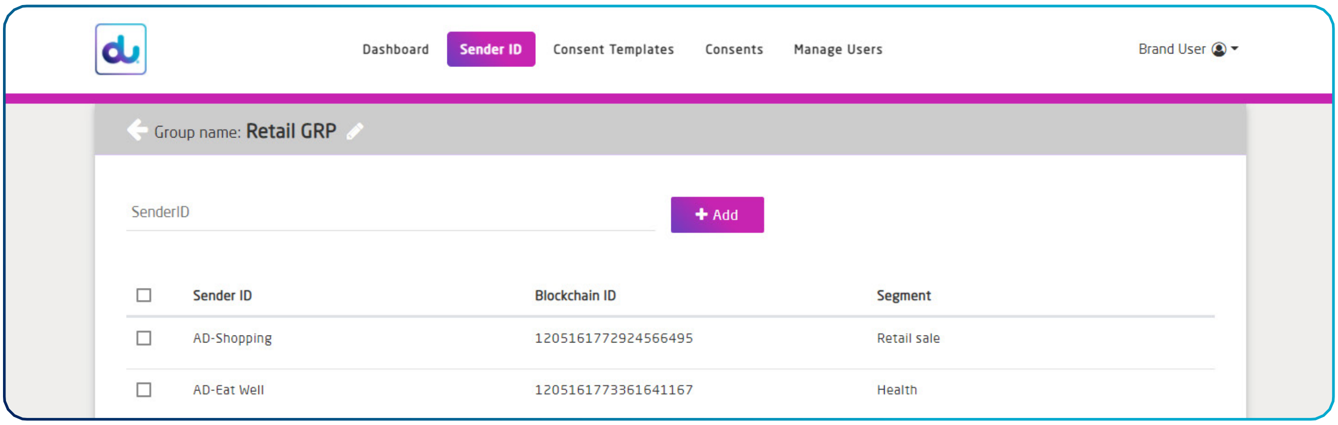
Once a Group is created, click on the "Pen" icon to edit the Group to tag Sender IDs.



Once "Pen" icon is clicked, the Group edit screen will open. Type the name of the promotional Sender ID to be tagged in the text box and click "+Add" button to add the Sender ID to the Group.

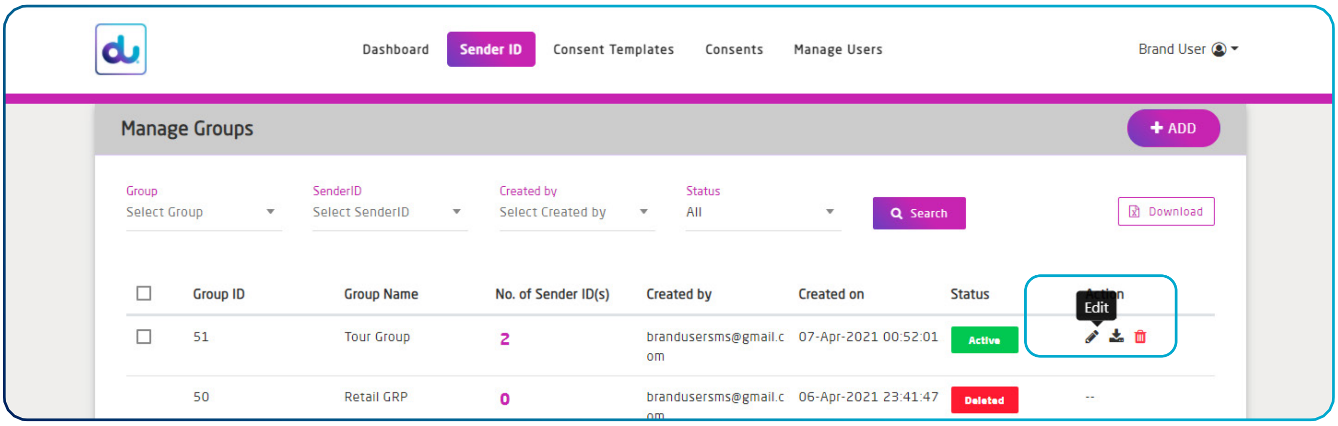


Upon clicking "+Add", the Sender ID will be added to the Group as shown below:

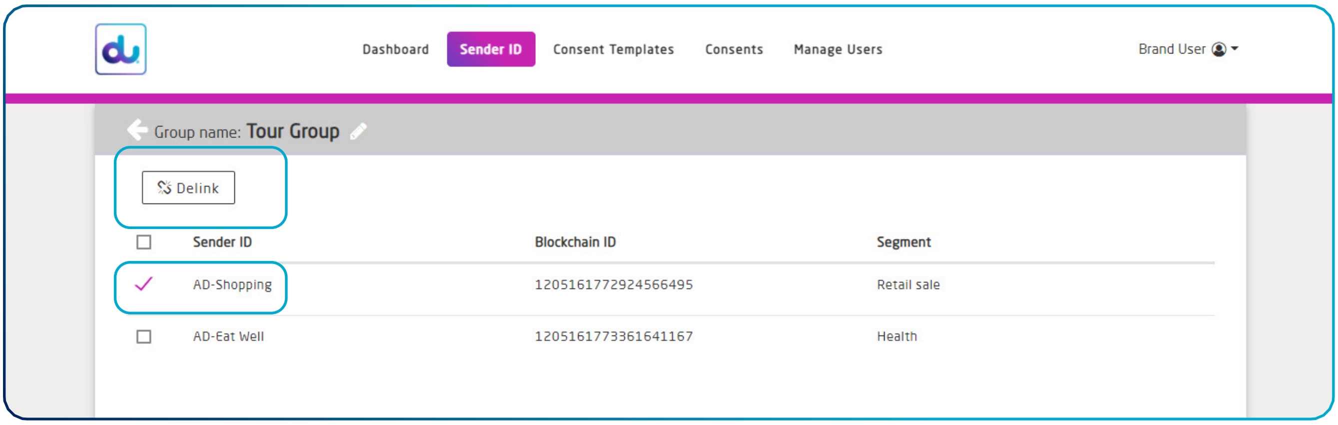


6.2. Editing a Group

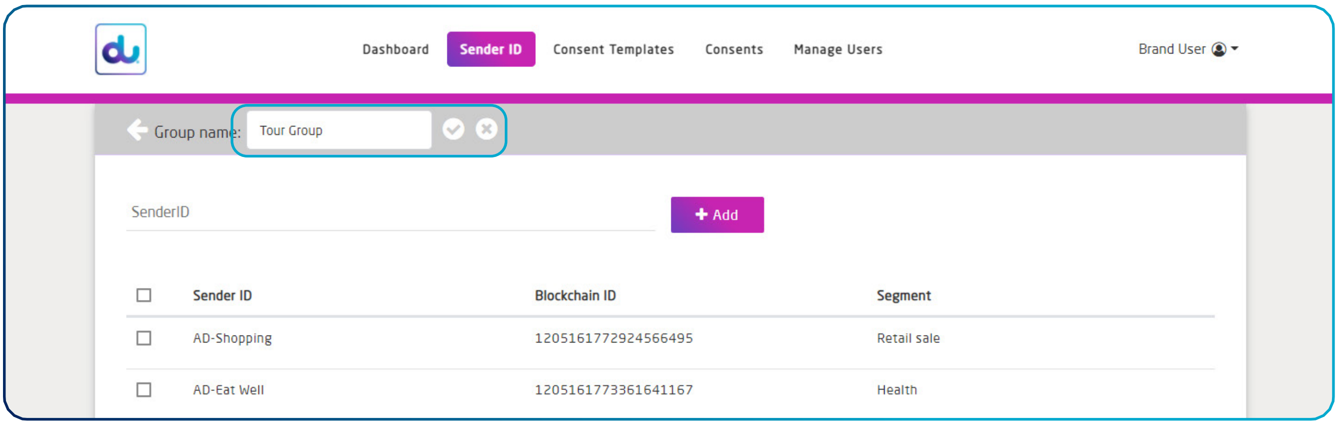
To delink a Sender ID from a Group click the "Pen" icon under the 'Action Tab' to edit the Group as show below:



To delink a Sender ID, tick mark the "Check Box" next to the Sender ID and click "Delink".

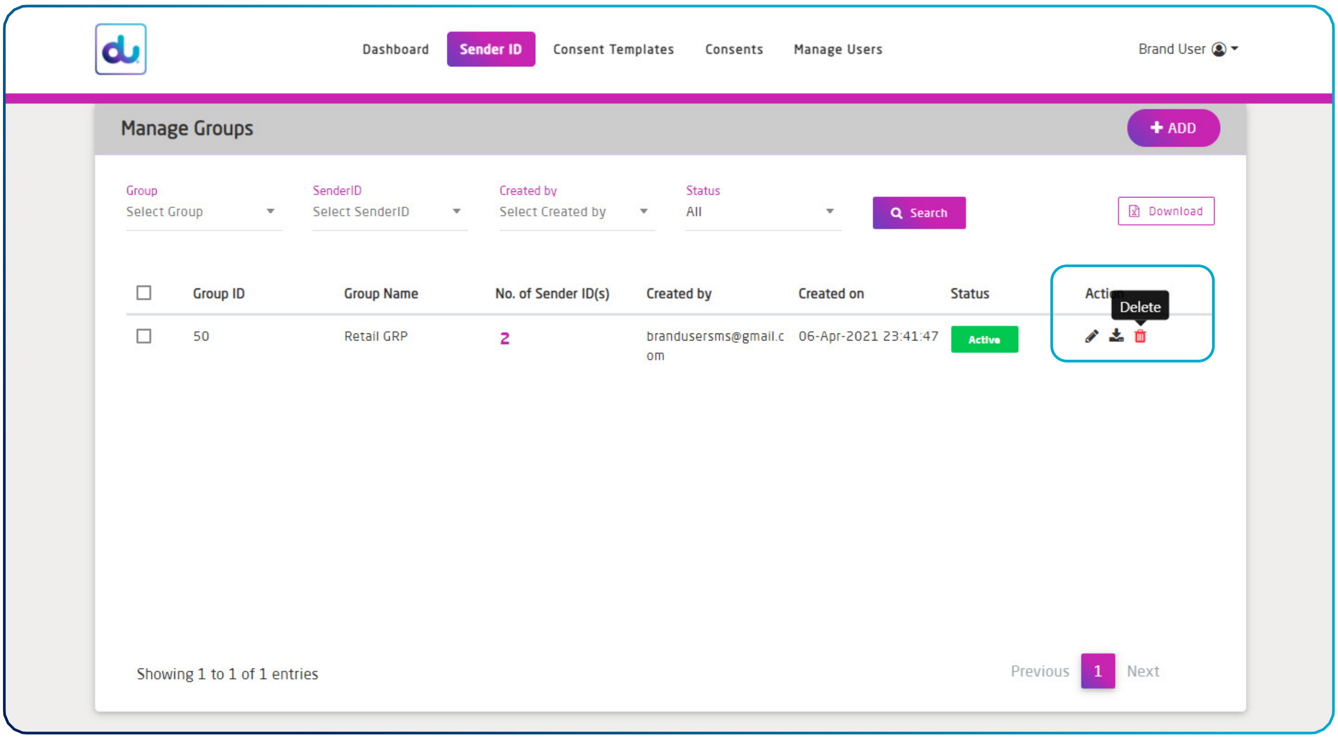


User can also edit the name of the Group by click the "Pen" icon next to the 'Group Name'.

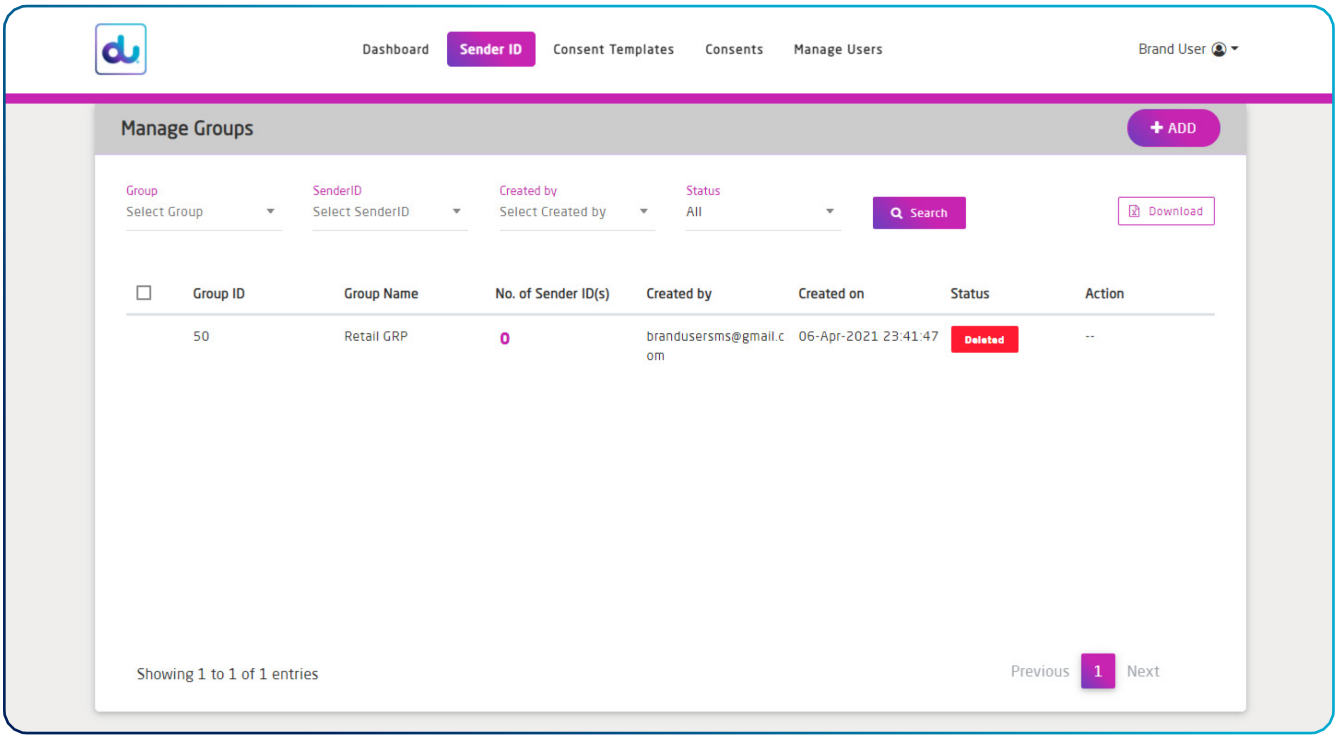


6.3 Deleting a Group

A Group can be deleted by clicking the "Bin" icon under the 'Action' tab as shown below. Deleting a Group will only delink the Sender IDs tagged to the Group.



Once a Group is deleted, the status of the Group will change to 'Delete' and all Sender ID will be delinked automatically as shown below:



7. Consent Templates

This module allows Users to create and view all registered Consent Templates, QR Code and Revoke QR Code Templates on the portal along with its requisite details. A Consent Template is created to contain the "Keywords" that a mobile subscriber accepts or acknowledges in order to receive promotional SMS from any brand. Once a Consent Template is created, it can be tagged to a Sender ID or a Group. In order for the User to upload any mobile subscriber consent information, Consent Template name needs to be provided against the registered Sender ID or Group. The Consent Template content i.e. "Keywords" will be uploaded with the mobile subscriber consent information to the system. The QR Code Template provides the functionality to digitally acquire and upload a new consent directly by end customers via scanning a QR Code. The Revoke QR Code Template provides the functionality to revoke an existing consent directly by end customers via scanning a QR Code.

Applicable to:

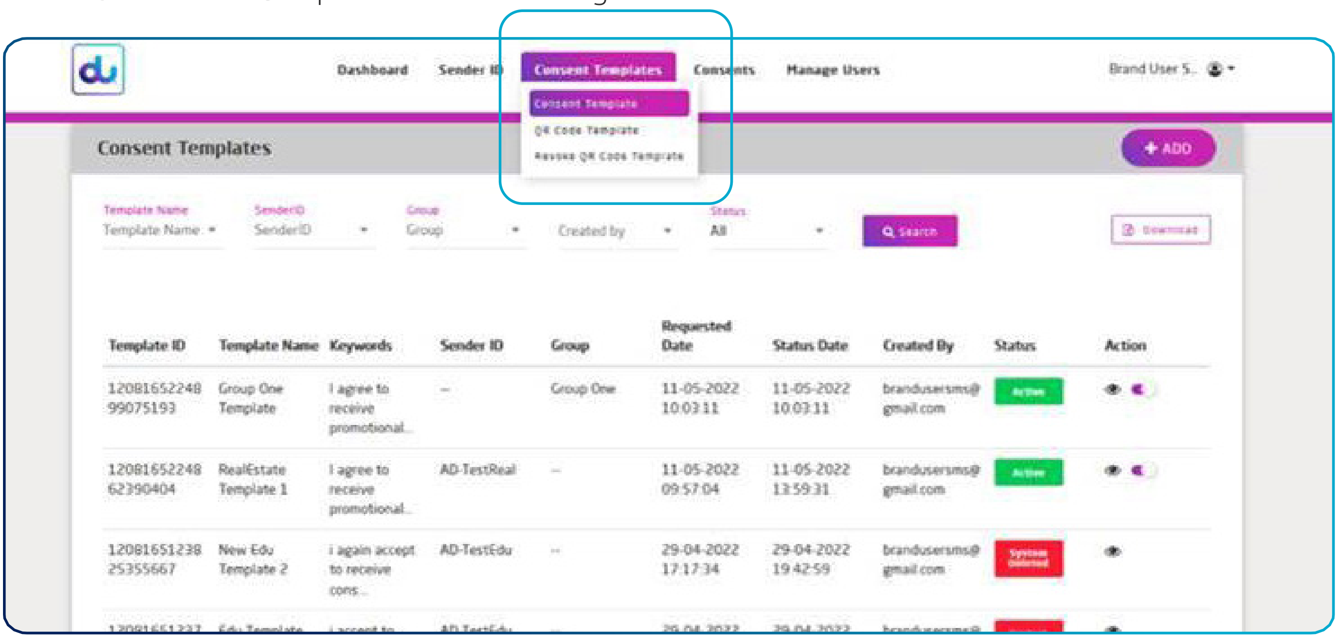
- Admin User
- Normal User
- Reporting User

Module Functionalities:

1. Enables User to create new Consent Templates, QR Code Templates and Revoke QR Code Templates
2. Enables User to view all types of registered Templates.
3. Enables User to search from list of available Templates.
4. Enables admin and normal User to disable/enable a Templates.
5. Enables User to view details of Templates.

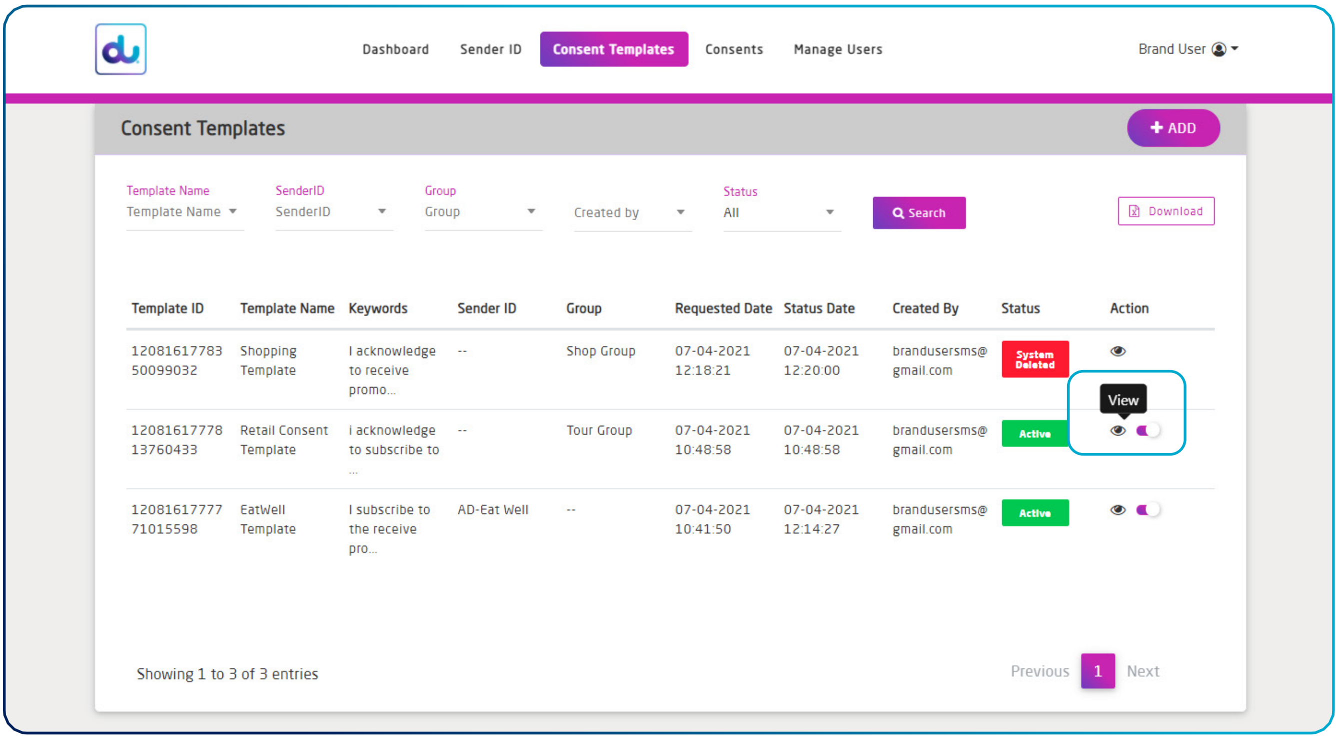
Business Rules:

1. Disabled Consent Template will not be allowed to be used while uploading consent.
2. Only Admin and Normal User will be allowed to create/edit any type of Templates.
3. A Consent Template once created cannot be edited by any User however QR Code and Revoke QR Code Templates can be edited.
4. Consent Templates cannot be deleted by any User. They are automatically deleted once the tagged Sender ID or Group is deleted from the system.

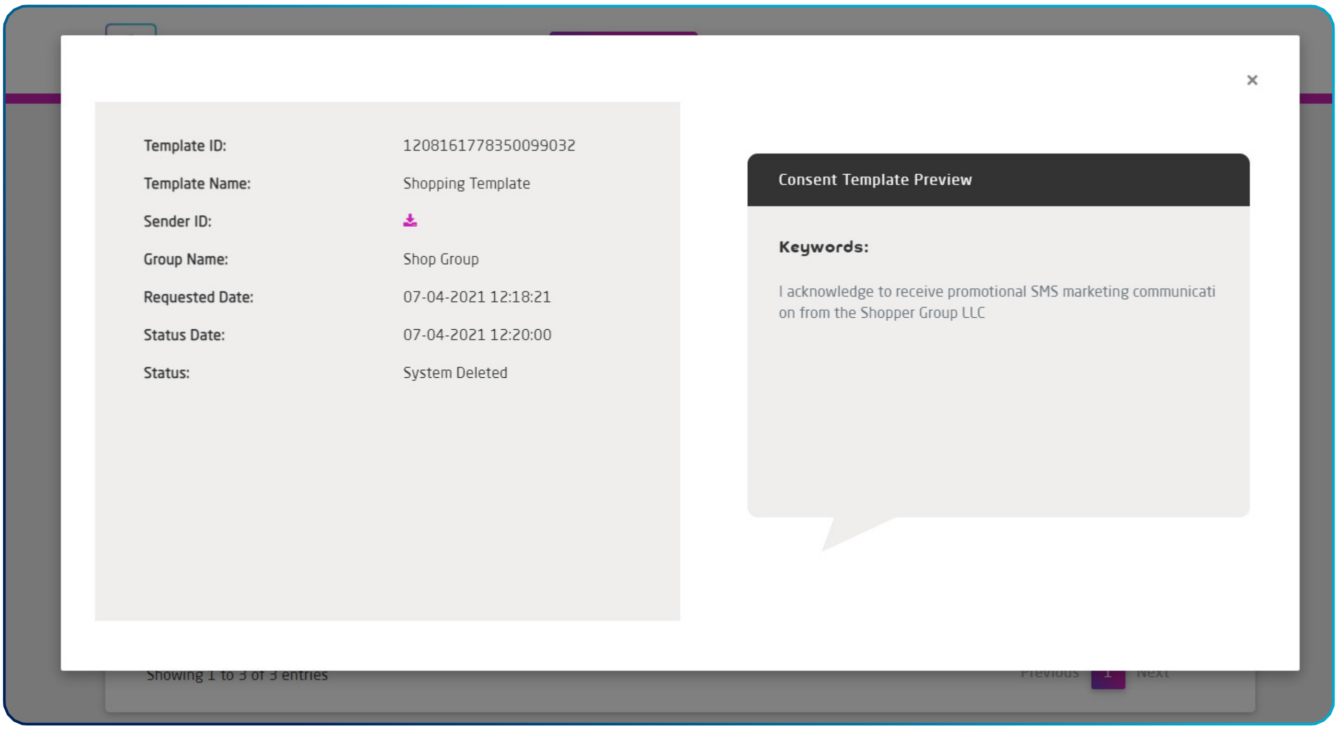


7.1 View a Consent Template

The content in a Consent Template can be viewed by clicking the "EYE" icon under the 'Action' tab on the Consent Templates page as shown below:

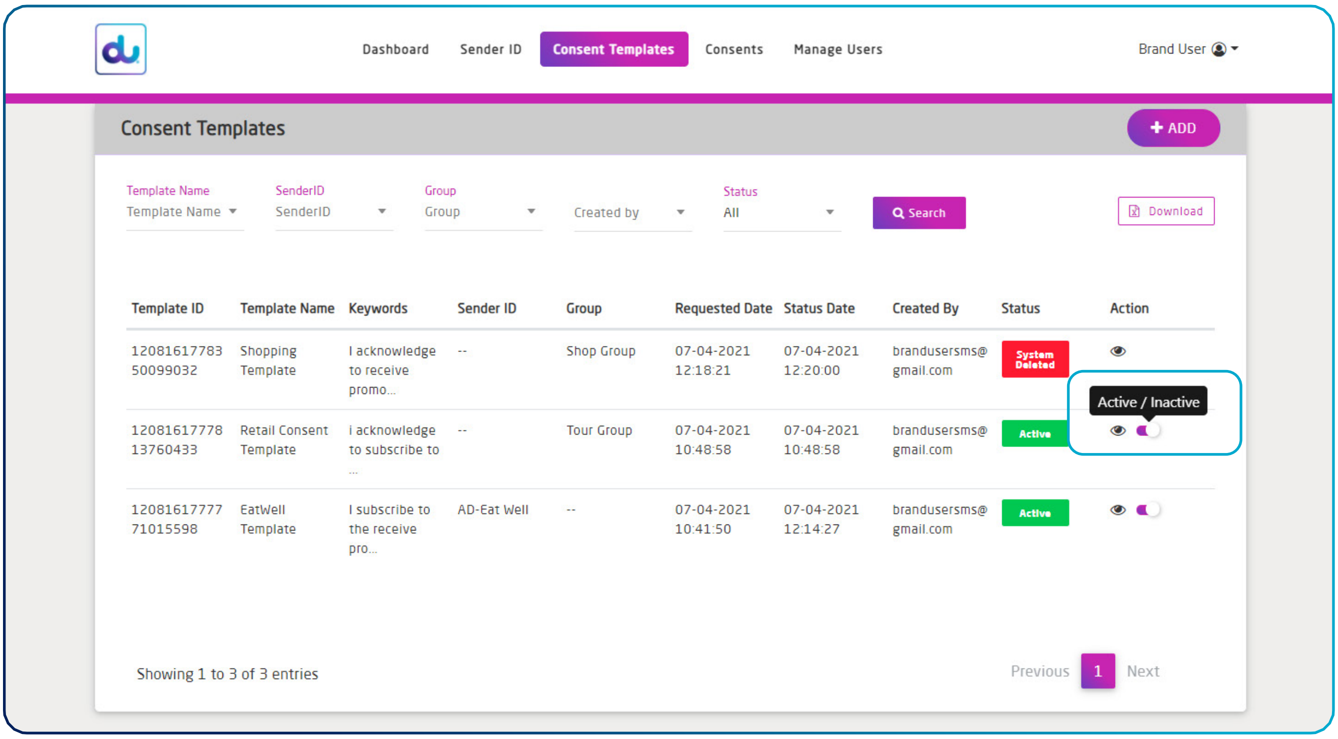


Once the "Eye" icon is clicked, the User will be able to review all consent information as shown below including the "Keywords" used in template, the status of the template, Group tagging information along with system ID and time stamp of each action taken on the template.

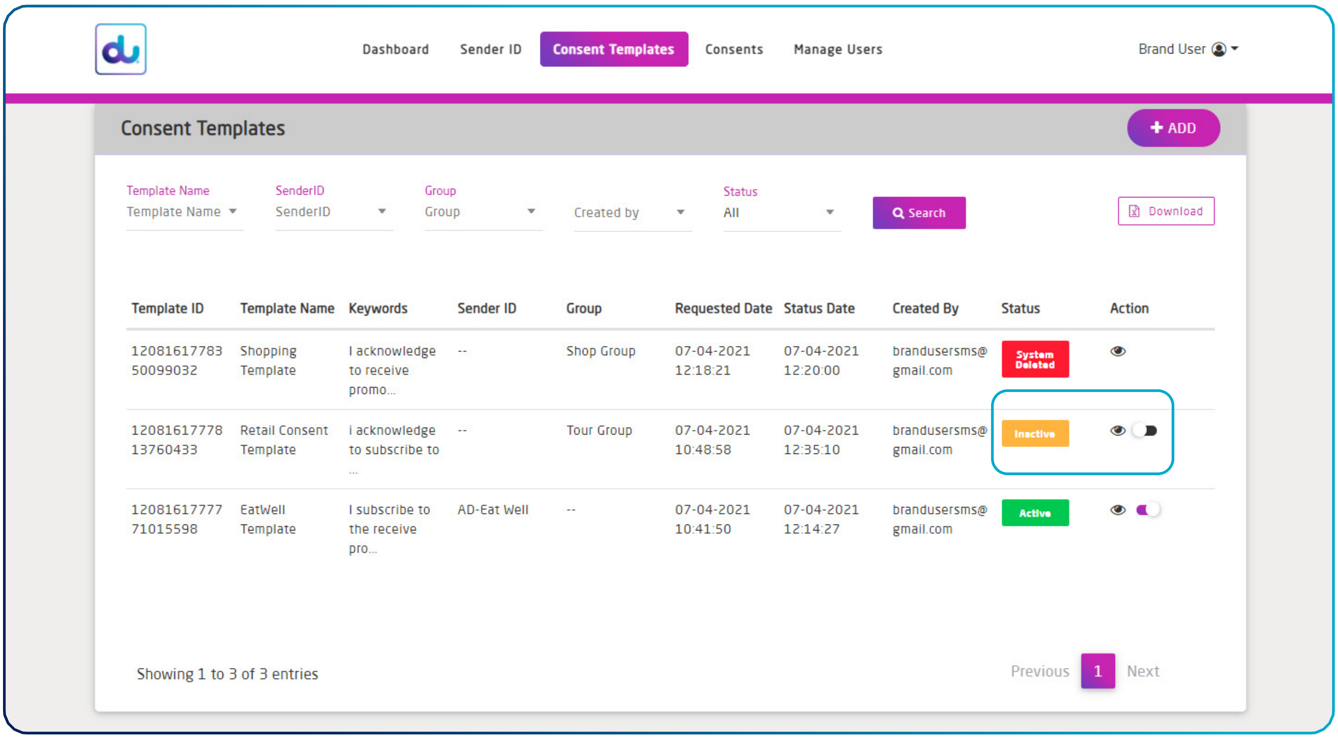


7.2 Enable/Disable Consent Template

A consent template can be temporarily enabled or disabled by the Admin or Normal User. The User can click the "Active/Inactive" toggle switch under the 'Action' tab on the Consent Templates page.



Once a consent template is disabled, its status will change from 'Active' to 'Inactive' and it cannot be used to upload consent information.



7.3 Creating a Consent Template

This functionality allows Admin and Normal Users to create Consent Templates by selecting a registered Sender ID or a Group and providing relevant "Keywords".

Applicable to:

- Admin User
- Normal User

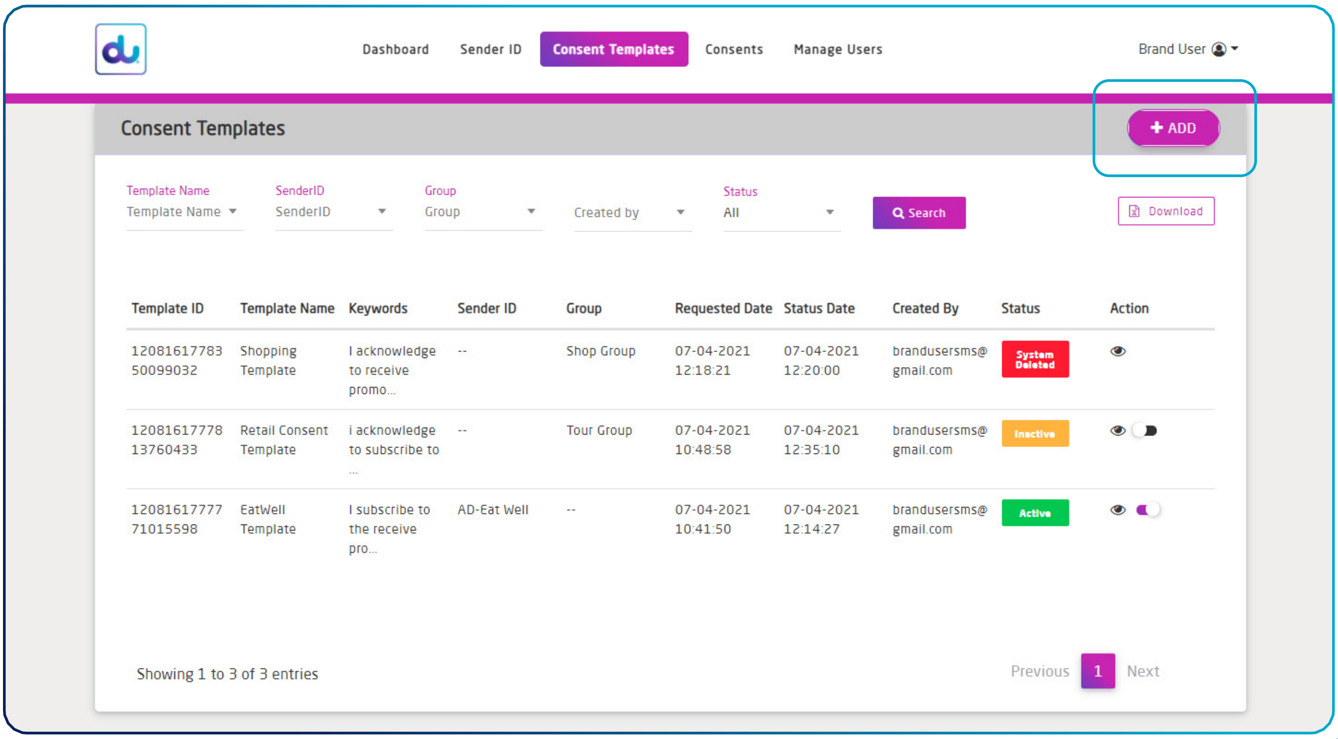
Module Functionalities:

1. Enables User to create new Consent Templates.
2. Enables User to select desired Sender ID or Group to tag a Consent Templates.
3. Enables User to enter desired "Keywords" in a Consent Template.
4. Enables User to preview the entered "Keywords".

Business Rules:

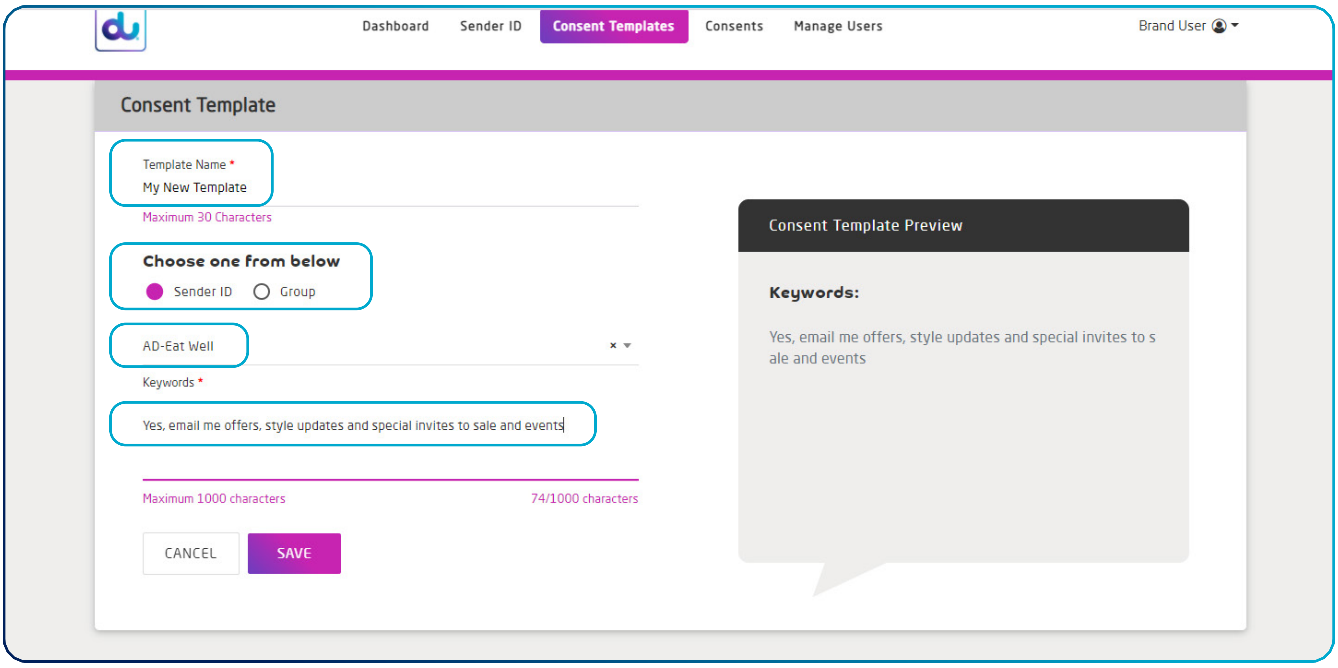
1. Consent Template can only be created for promotional Sender IDs.
2. User will be able to select active promotional Sender IDs or a Group for template tagging.
3. User will be able to add "Keywords" with minimum 20 and up to 1000 characters.

To create a new Consent Template, the User will click "+ADD" button on the Consent Templates Page as shown below:



7.3 Creating a Consent Template

Once the "+ADD" button is clicked, the following Consent Template creation screen will appear. The User will be required to enter template name, choose either a Sender ID or a Group radio button. In case Sender ID is selected, the User will enter an active Sender ID. In case Group is selected, User will be required to enter Group name. User will be required to enter "Keywords". The entered "Keywords" can be reviewed in the Consent Template Preview window. User can click 'SAVE' button to create the template.



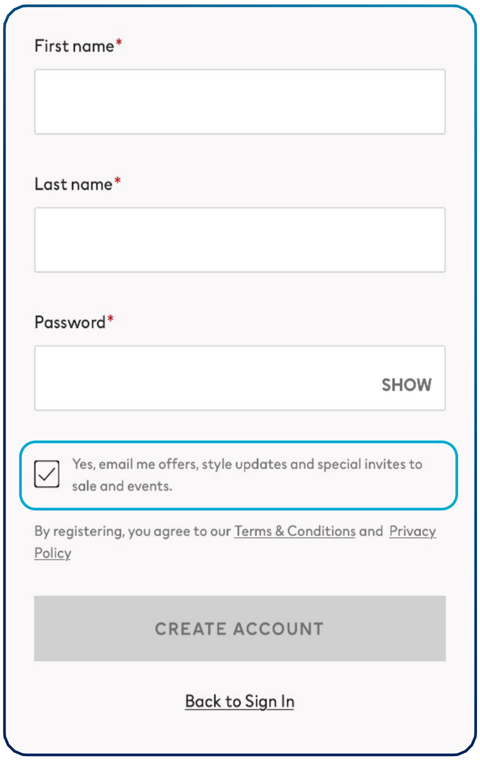
Important information about "Keywords":

"Keywords" denote the set of explicit words that a mobile subscriber has acknowledged and agreed to at the time of becoming a customer and allowing any brand to send promotional SMS to the mobile subscriber.

The consent template must contain the entire set of "Keywords" that the customers has agreed to at the time of signing up an application form, mobile application or website membership.

As an example on the right side, a mobile application contains the "Keywords" as highlighted in the blue box to collect consent from a mobile subscriber. Hence the consent template must contain the following as "Keywords" as shown in the above template creation window.

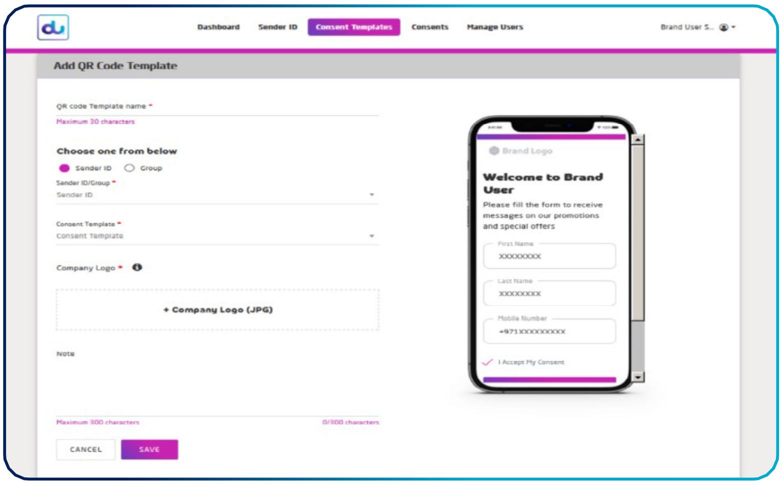
"Yes, email me offers, style updates and special invites to sale and events."



8. Understanding QR Code Template

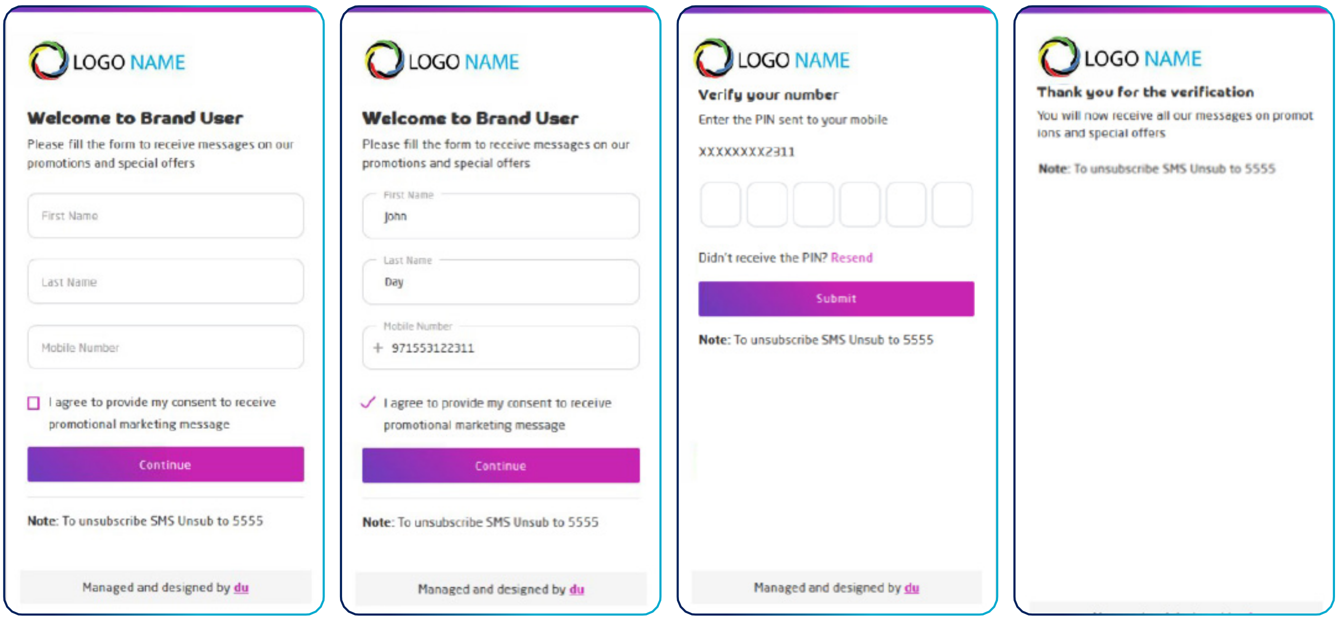
The QR Code Template offers Enterprises ("Brands") a digital capability to automatically acquire and upload an end customer digital consent upon scanning of a QR Code. This functionality can be used by any Enterprises ("Brands") using Enterprise SMS Portal and enables such Enterprises ("Brands") to get rid of existing manual consent upload processes via Analog Type or Digital Type (refer to Section 10. Consents for more information on how to use Analog Type (Section 10.1.4) or Digital Type (Section 10.1.5). Consents acquired and uploaded by QR Code scanning are denoted as Consent Type: "QR Code" on the portal.

A QR Code Template can be easily created by Enterprises ("Brands") in a single step. A unique QR Code for each template is generated which can be displayed by Enterprises ("Brands") on their website, retail outlets, etc. End customers will only be required to scan the QR Code from their smartphones. Upon scanning to the QR Code by end customers, a webpage will be opened where end customers can enter their first/last name along with their mobile number. End customers will receive an OTP to validate their consent. Upon submission of the OTP, end customer consent will be directly uploaded in the Enterprise SMS Portal which can be later extracted or downloaded from the Portal.



QR Code Template can be easily created in a single step

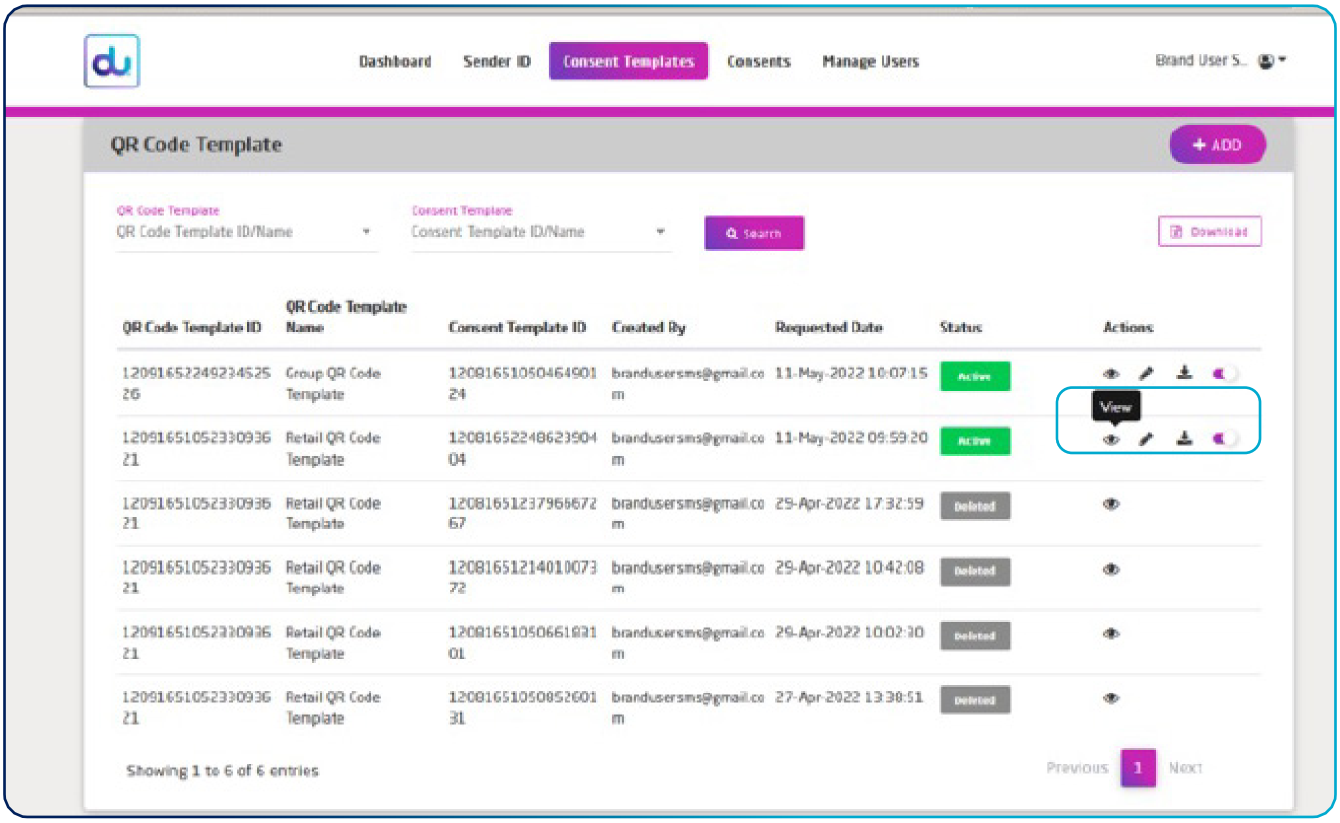
A QR Code will be generated



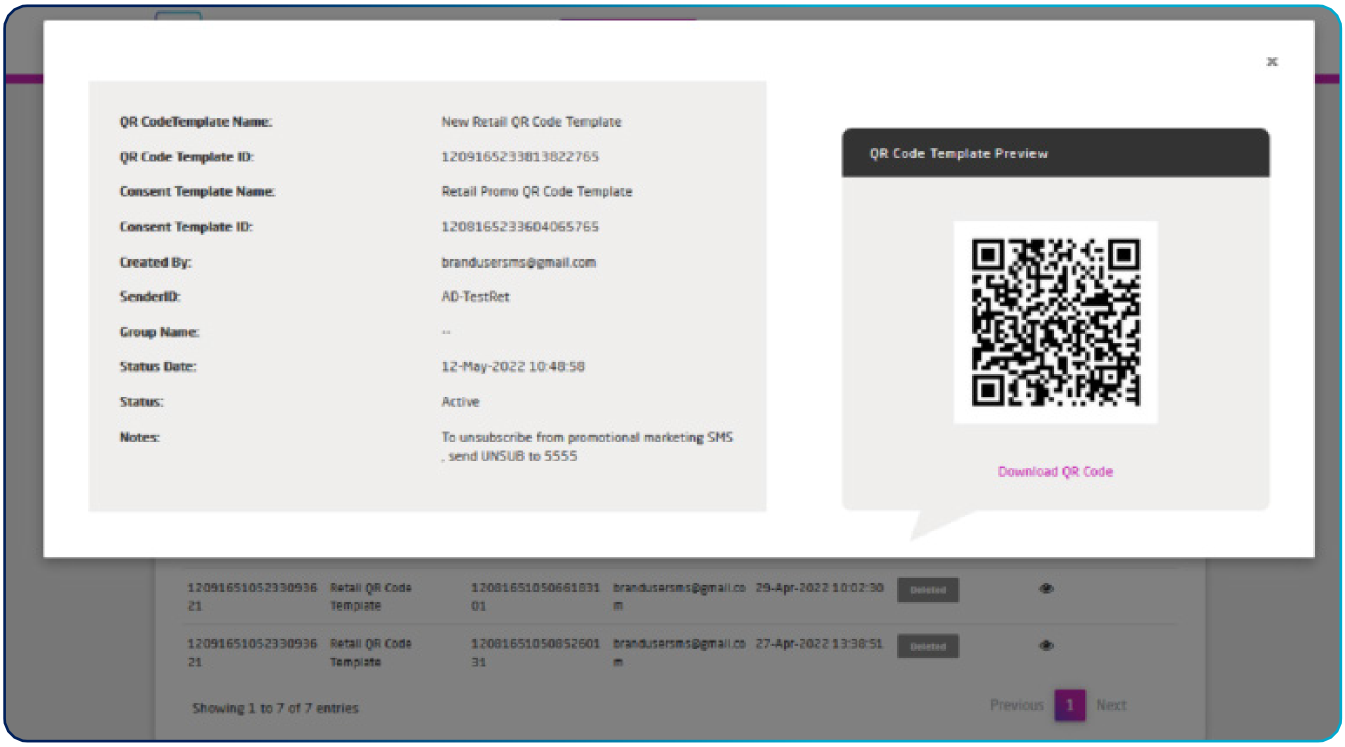
End customers can scan the QR Code to open a webpage. Enter their name and mobile number. End customer will receive an OTP on their mobile number and upon submission their consent will be stored

8.1 Viewing a QR Code Template

The content in a QR Code Template can be viewed by clicking the "EYE" icon under the 'Action' tab on the QR Code Template page as shown below:

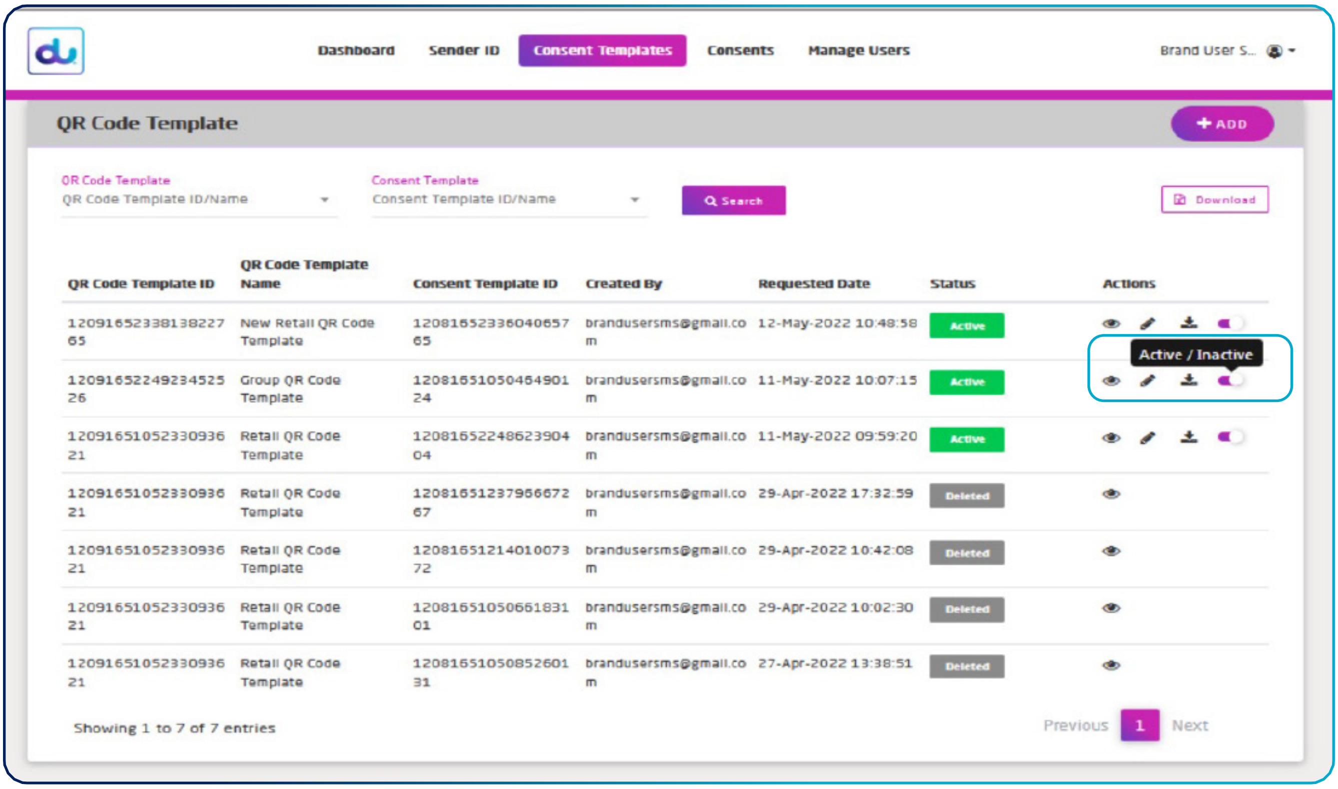


Once the "Eye" icon is clicked, the User will be able to review all QR Code Template information as shown below including information on Consent Template used, the status of the template, Sender ID/Group tagging information along with system ID, Notes and the ability to view and download the template QR Code.

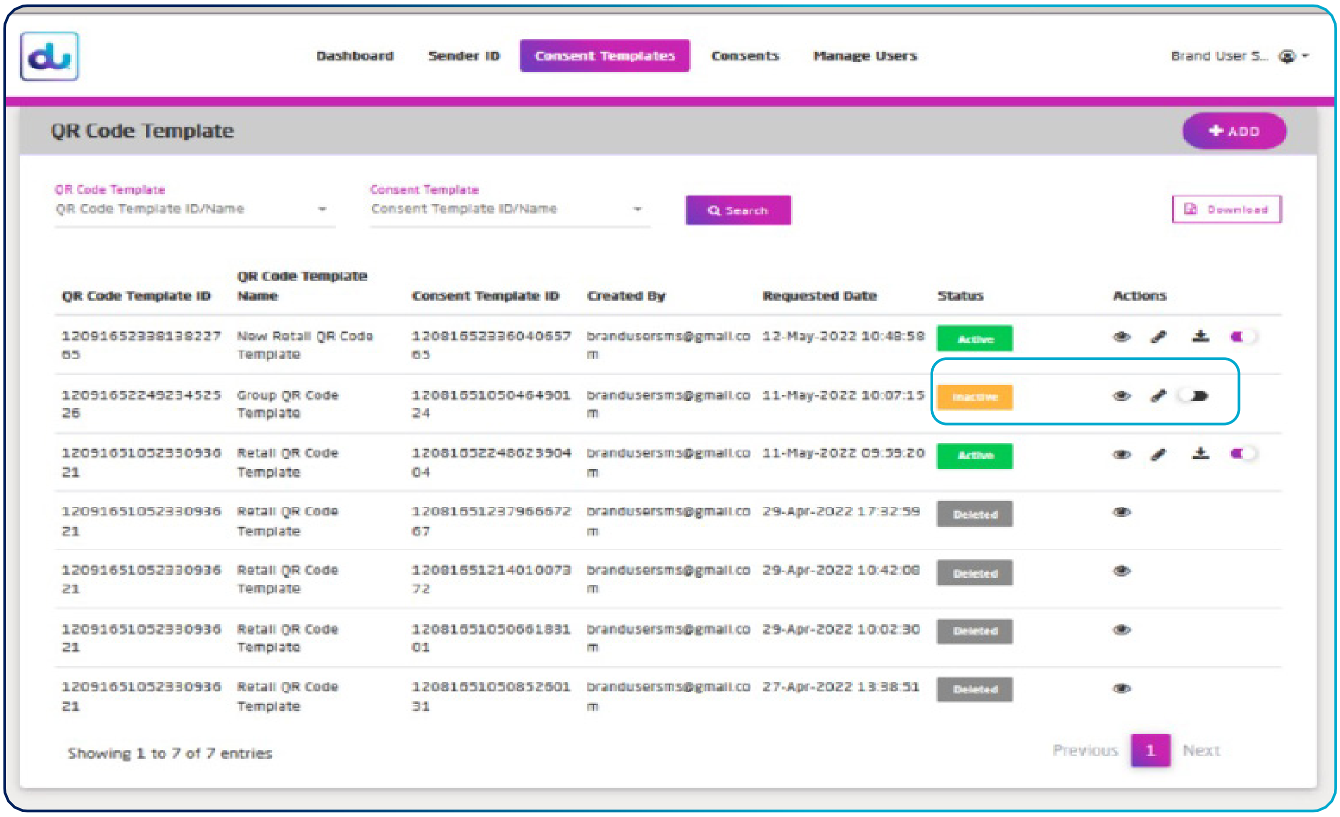


8.2 Enable/Disable QR Code Template

A QR Code Template can be temporarily enabled or disabled by the Admin or Normal User. The User can click the "Active/Inactive" toggle switch under the 'Action' tab on the QR Code Template page.



Once a QR Code Template is disabled, its status will change from 'Active' to 'Inactive' and QR Code scanning will not work. In case an end customer tries to scan a disabled QR Code, an error will be displayed.



8.3 Creating a QR Code Template

This functionality allows Admin and Normal Users to create a QR Code Template to acquire and upload digital consents directly by the end customers via scanning a QR Code.

Applicable to:

- Admin User
- Normal User

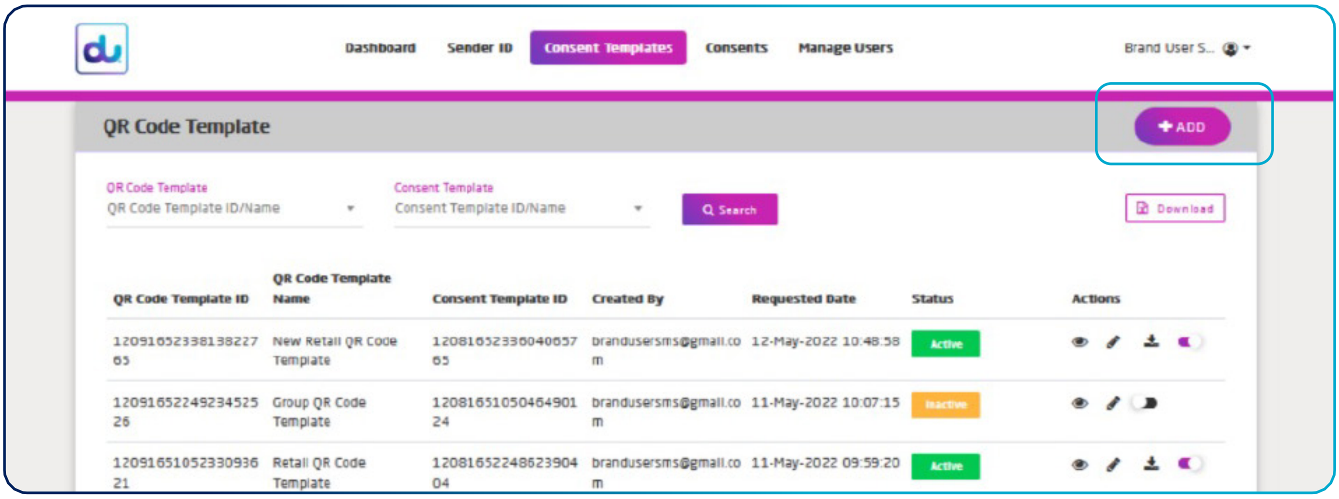
Module Functionalities:

1. Enables User to create new QR Code Templates.
2. Enables User to select desired Sender ID or Group to tag a QR Code Templates.
3. Enables User to select desired Consent Template linked to a Sender ID or Group.
4. Enables User to upload Company Logo to be displayed on QR Code Template.
5. Enables User to add special notes to the QR Code Template if required for additional information
6. Enables User to edit a QR Code Template to replace existing Sender ID/Group, Logo or Consent Template

Business Rules:

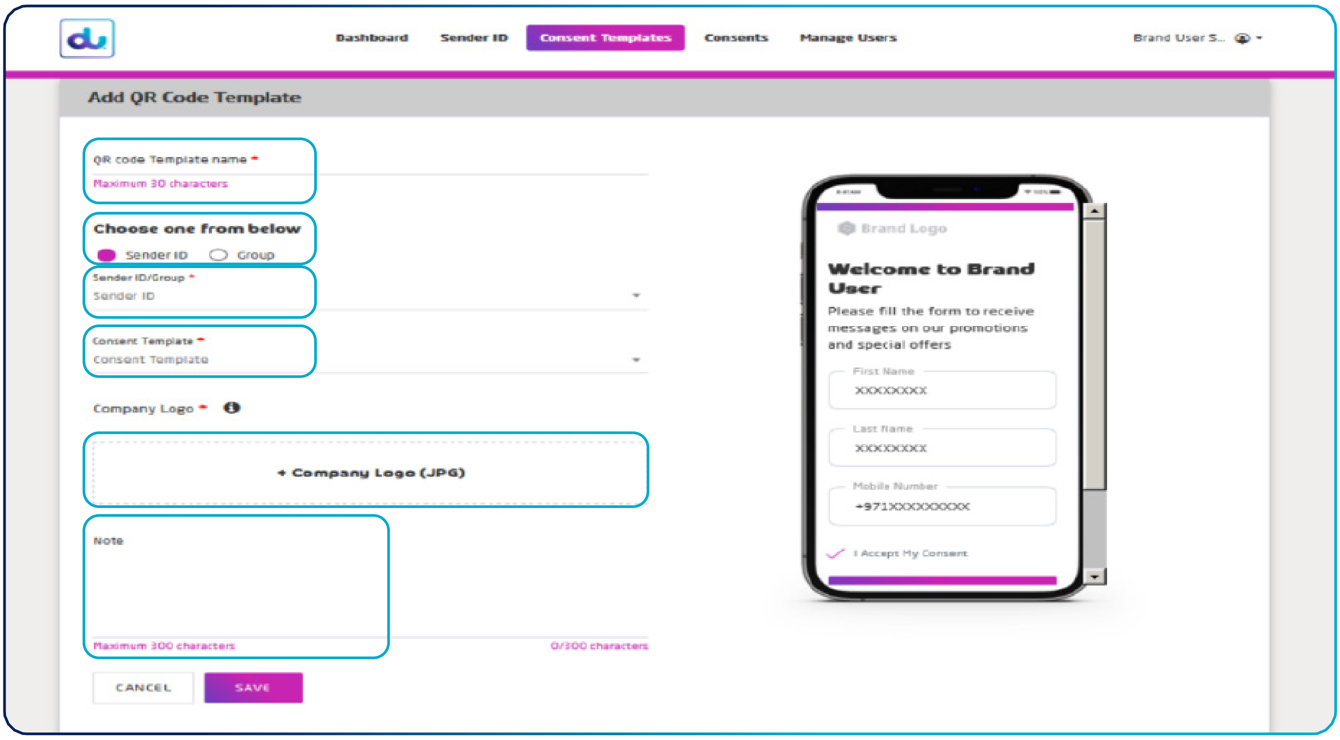
1. Consents acquired and uploaded via QR Code scanning are always denoted as Consent Type: "QR Code"
2. QR Code Template can only be created for promotional Sender IDs.
3. User will be able to select promotional Sender IDs in "Active" or "Suspended" status for template tagging
4. Only one QR Code can be created for one any Consent Template
5. A QR Code Template cannot be deleted and can only be disabled.
6. User will be able to add "Note" with up to 300 characters
7. User will be able to upload company logo in JPG format with maximum 10MB file size
8. Once a QR Code template is active, scanning or re-scanning of the QR Code will override any existing consents with new consents. Old consents will be revoked and replaced by new QR Code consents
9. An end customer can scan a QR code and upload consent only 3 times within a 15 minutes window. After 3 times, customer will be required to wait for another 15 minutes to resubmit his consent.

To create a new QR Code Template, the User will click "+ADD" button on the QR Code Template Page as shown below:

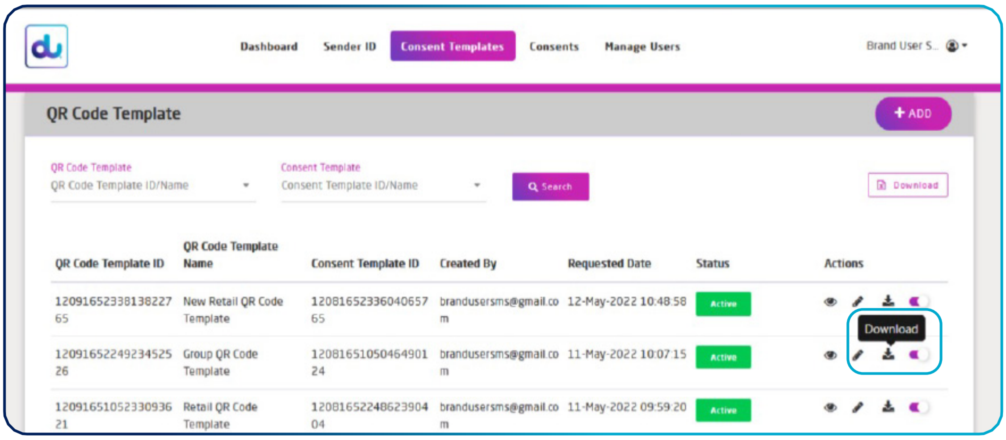


8.3 Creating a QR Code Template

Once the "+ADD" button is clicked, the following QR Code Template creation screen will appear. The User will be required to enter template name, choose either a Sender ID or a Group radio button. In case Sender ID is selected, the User will enter a Sender ID. In case Group is selected, User will be required to enter Group name. User will be required to select an active Consent Template tagged to the Sender ID/Group. User will be required to upload company logo to be displayed on the template. In case the User wants to add any special notes to be displayed to the end customer, User can input these in the "Notes" section. User can click 'SAVE' button to create the new template.



Once the QR Code template is saved, User can view the created template from the QR Code Template home screen and download the QR Code by clicking the "Download" icon under the 'Action' tab. Once download is clicked, QR Code will be downloaded in PDF format file.



8.4 Editing a QR Code Template

This functionality allows Admin and Normal Users to edit an existing QR Code Template.

Applicable to:

- Admin User
- Normal User

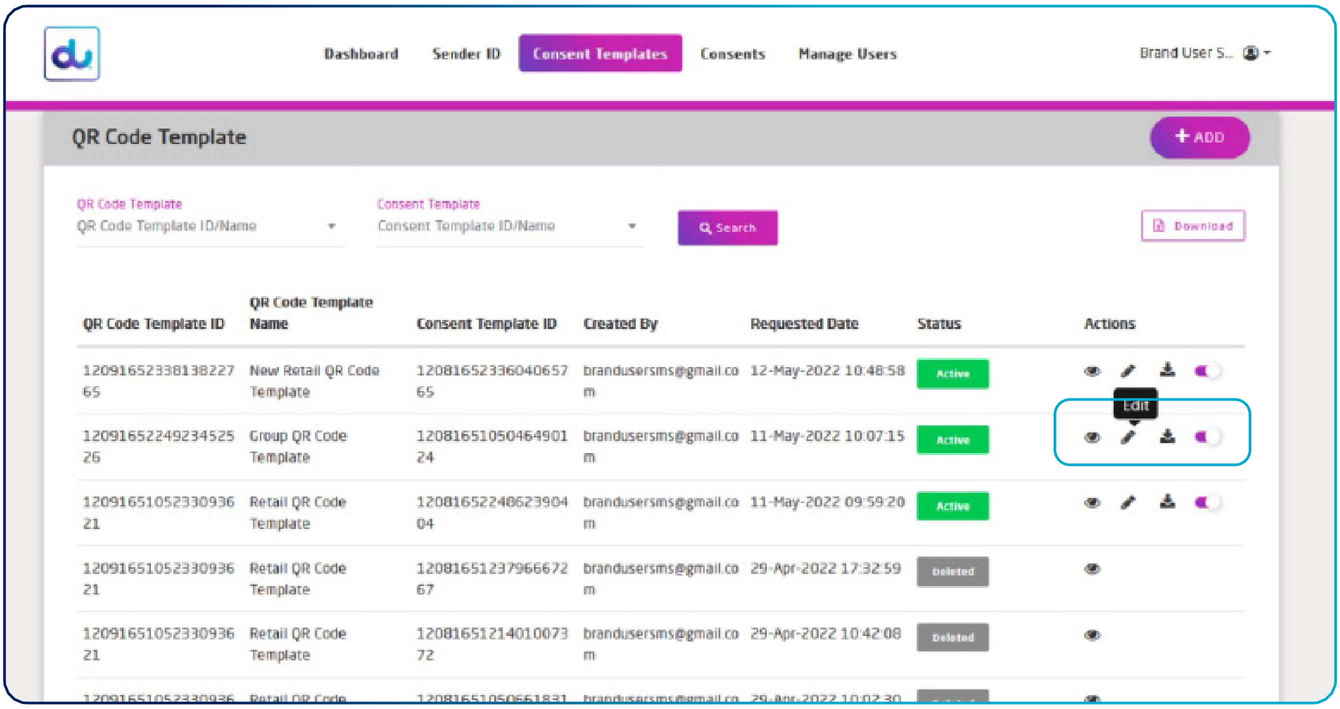
Module Functionalities:

1. Enables User to edit existing QR Code Templates.
2. Enables User to select a new Sender ID or Group to be tagged to an existing QR Code Template.
3. Enables User to select a new Consent Template linked to a Sender ID or Group.
4. Enables User to upload a new Company Logo to be displayed on QR Code Template.
5. Enables User to update special notes to the QR Code Template.

Business Rules:

1. Editing a QR Code template will not generate a new QR Code pattern
2. If a Consent Template has already been used in a QR Code template once, it cannot be re-used again even if it is still active. A new Consent Template will be required to be created in order to be used.
3. In case a Consent Template has been disabled by the User, QR Code Template will become inactive. In order to use the same QR Code Template, either disabled Consent Template needs to be enabled or new Consent Template needs to be tagged
4. In case a Consent Template has been deleted by the System, QR Code Template will become inactive. In order to use the QR Code Template, a new Consent Template needs to be tagged.

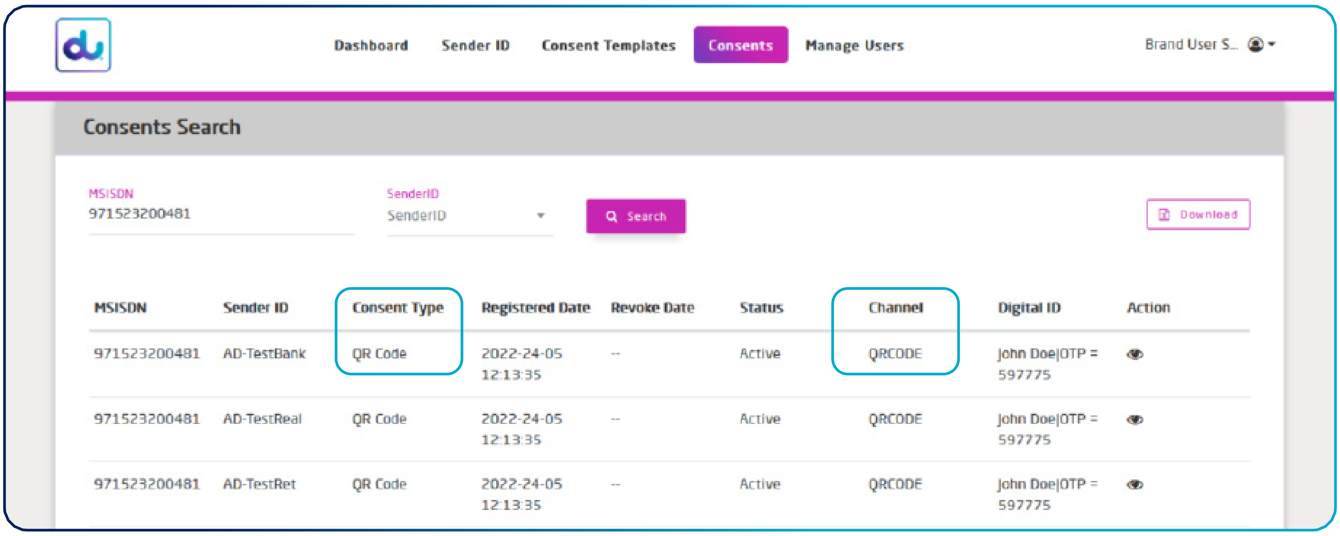
To edit a new QR Code Template, the User will click "Pen" icon on the QR Code Template Page as below.



8.4 Viewing QR Code Uploaded Consent

Once an end customer successfully scans a QR code to upload his consent, the consent evidence can be reviewed by the User in the "Search Consent" menu item. Kindly refer to Section 11 "Search Consent" of the user guide on how to view information on consents and their evidence against a mobile subscriber and sender ID.

In case a consent has been uploaded using a QR Code, upon search of consent using "Search Consent" menu item, User can review the following information for the particular MSISDN as shown below.



As consents uploaded via QR Code is a form of Digital Consents, the information will be similar to Digital Consent with following conditions to differentiate it from consent uploaded by "Digital Type" which is a manual consent upload process.

Consent Type will always be displayed as **"QR Code"** and Channel will always be **"QRCODE"**

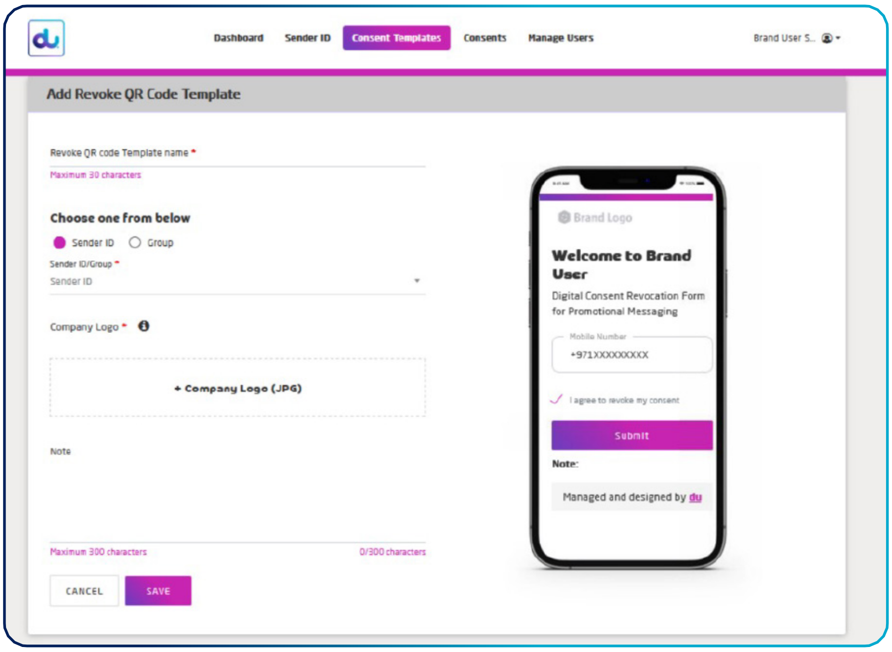
User can view all consent details including:

MSISDN: (Mobile number of the customer).
SENDER ID: (Sender ID the customer has subscribed).
CONSENT TYPE: QR Code.
REGISTERED DATE: (Date & Time when consent was uploaded on the system).
REVOKE DATE: (Date & Time in case the consent was revoked from the system).
Status: (If consent is 'Active' or 'Revoked').
CHANNEL: QRCODE
DIGITAL ID: The end customer First and Last Name with OTP entered during QR Code scanning process.
More information available by clicking "EYE" icon under 'Action' tab:
CONSENT ID: (System ID of the stored consent).
TEMPLATE ID: (System ID of the Consent Template).
TEMPLATE NAME: (Consent Template Name).
KEYWORDS: (Keywords stored in the Consent Template).
CONSENT DATE & TIME: (Timestamp of the customer scanning the QR Code to provide the consent).
DIGITAL CHANNEL VALUE: (QR Code Template ID used for scanning of the QR Code)

9. Understanding Revoke QR Code Template

The Revoke QR Code Template offers Enterprises ("Brands") a digital capability to automatically revoke an end customer consent upon scanning of a QR Code. This functionality can be used by any Enterprises ("Brands") using Enterprise SMS Portal and enables such Enterprises ("Brands") to get rid of existing manual consent revoke process (refer to Section 10 Consents for more information on how to revoke consents (Section 10.2)).

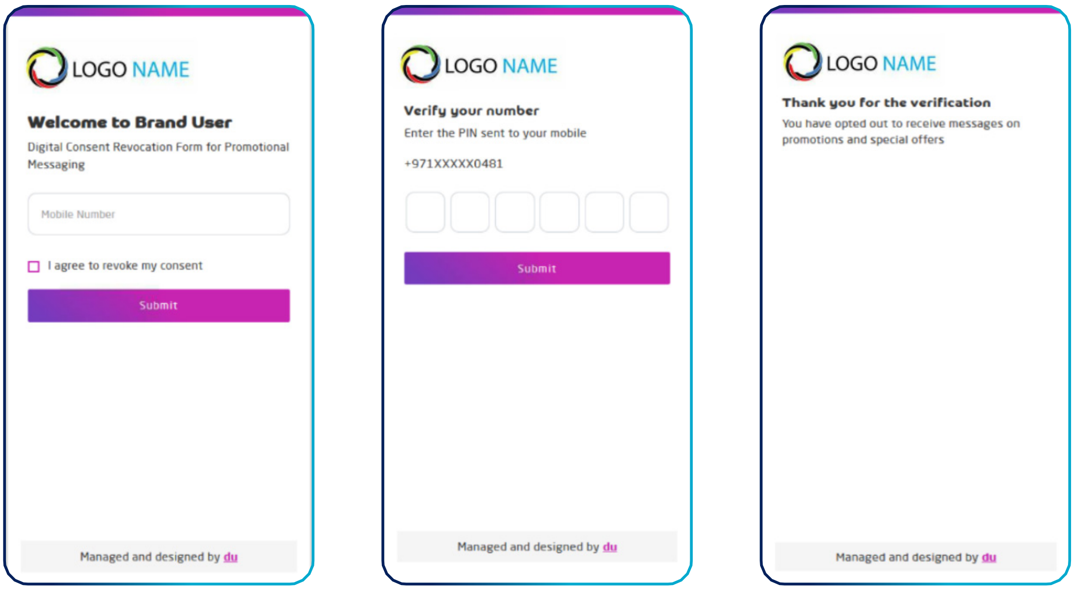
A Revoke QR Code Template can be easily created by Enterprises ("Brands") in a single step. A unique QR Code for each template is generated which can be displayed by Enterprises ("Brands") on their website, retail outlets, etc. End customers will only be required to scan the QR Code from their smartphones. The QR Code scanning will open a webpage where end customers can enter their mobile number. End customers will receive an OTP to validate their revoke consent request. Upon submission of the OTP, end customer consent will be directly revoked in the Enterprise SMS Portal.



https://10.183.191.4/qrcode_templates/qrrevokerequest/Yxk8me pYwPyv2nr1P52aMyJNj/

A QR Code will be generated

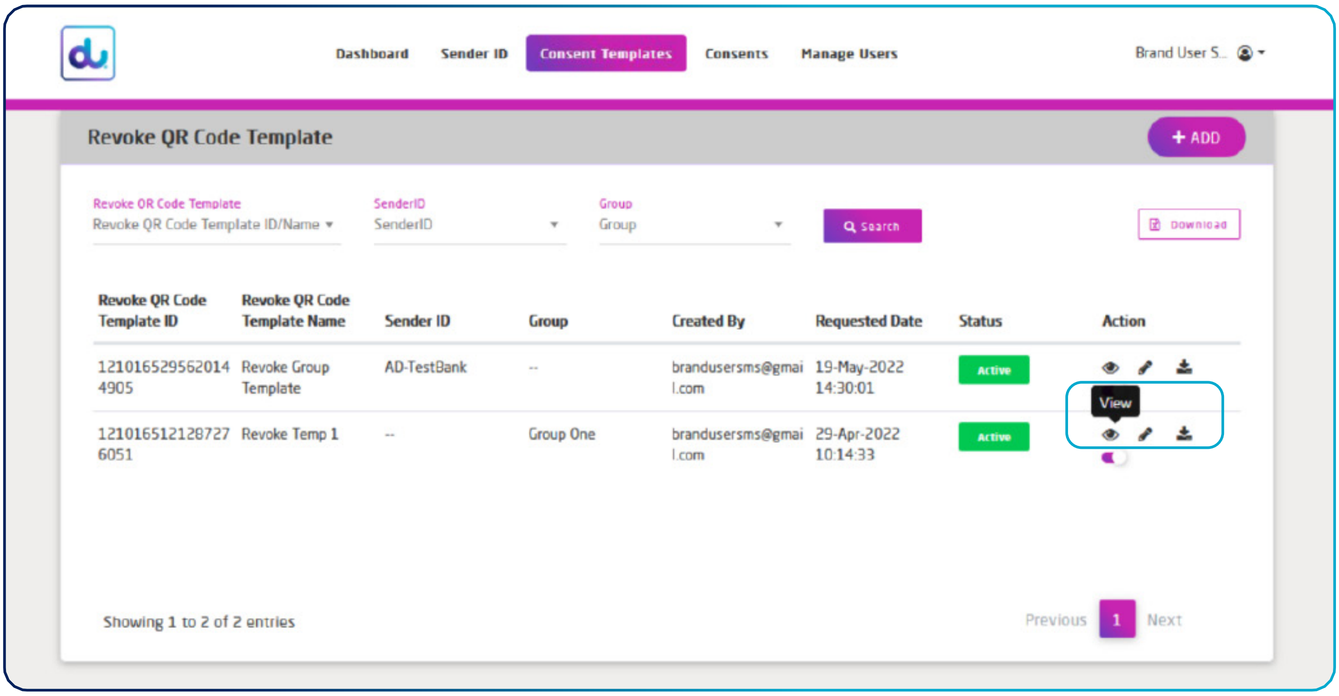
Revoke QR Code Template can be easily created in a single step



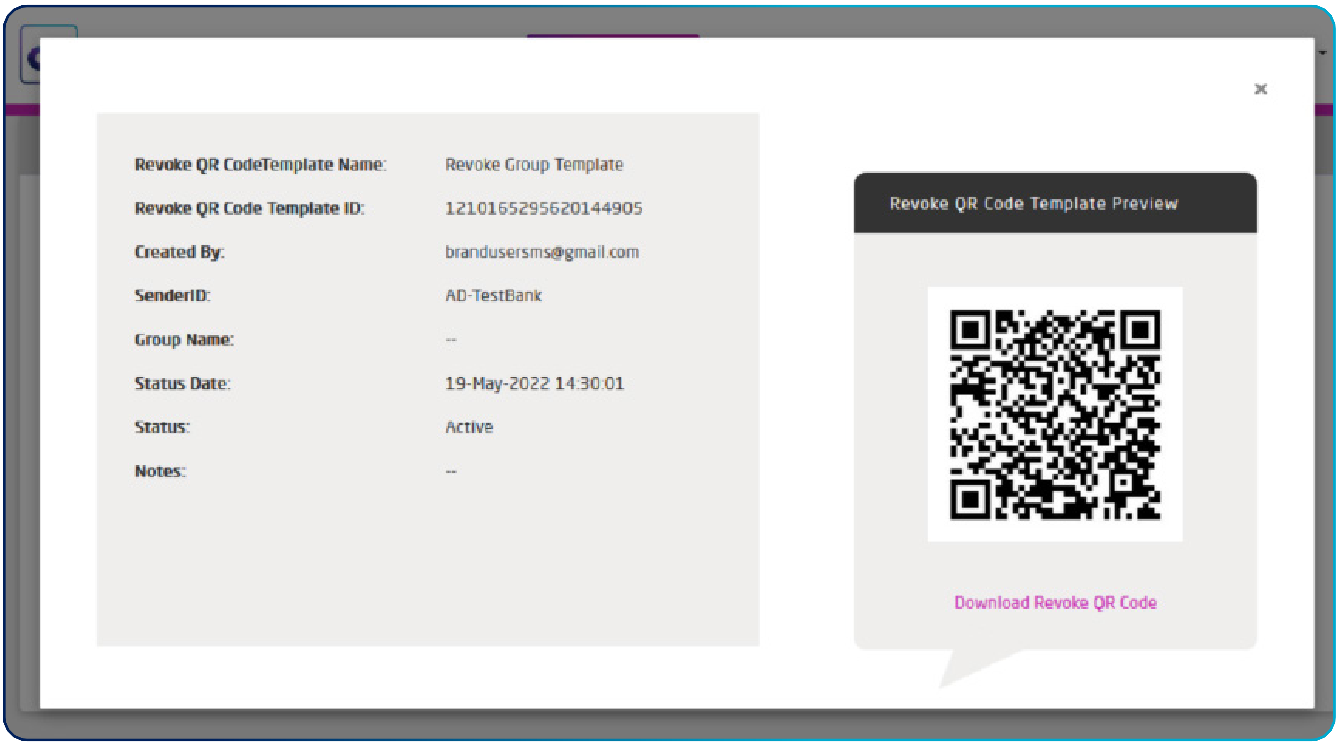
End customers can scan the Revoke QR Code to open a webpage. Enter their mobile number. End customer will receive an OTP on their mobile number and upon submission their consent will be revoked

9.1 Viewing Revoke QR Code Template

The content in a Revoke QR Code Template can be viewed by clicking the "EYE" icon under the 'Action' tab on the Revoke QR Code Template page as shown below:

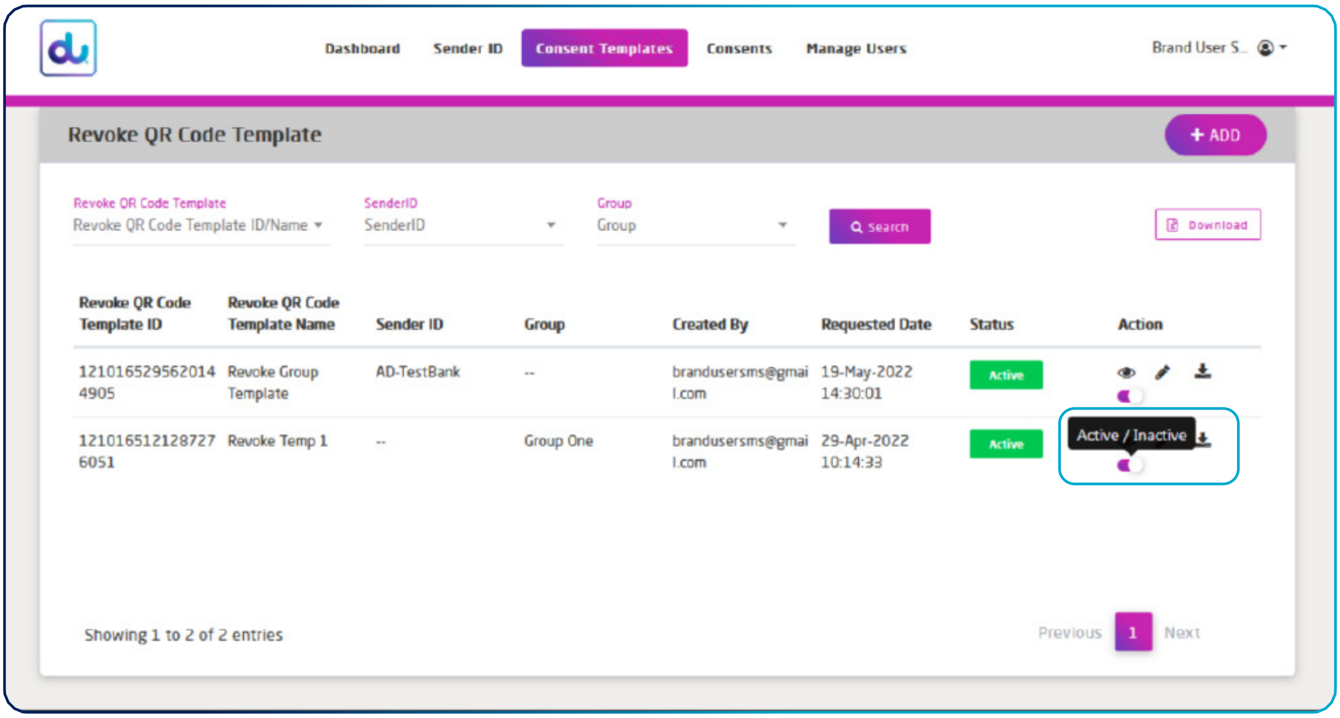


Once the "Eye" icon is clicked, the User will be able to review all Revoke QR Code Template information as shown below including info on the status of the template, Sender ID/Group tagging information along with system ID, Notes and the ability to view and download the template QR Code.

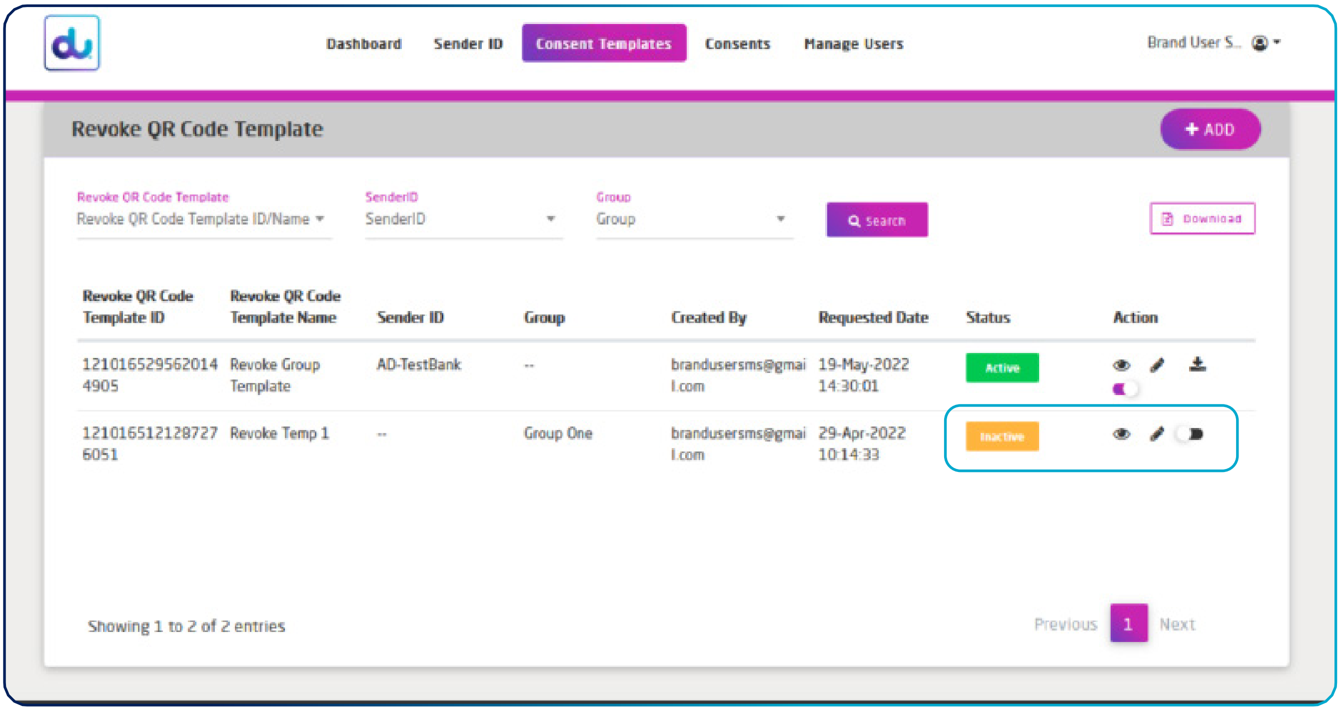


9.2 Enable/Disable Revoke QR Code Template

Revoke QR Code Template can be temporarily enabled or disabled by the Admin or Normal User. The User can click the "Active/Inactive" toggle switch under the 'Action' tab on the QR Code Template page.



Once a Revoke QR Code Template is disabled, its status will change from 'Active' to 'Inactive' and QR Code scanning will not work. In case as end customer tries to scan a disabled QR Code, an error will be displayed,



9.3 Creating Revoke QR Code Template

This functionality allows Admin and Normal Users to create a Revoke QR Code Template to revoke consents directly by the end customers via scanning a QR Code.

Applicable to:

- Admin User
- Normal User

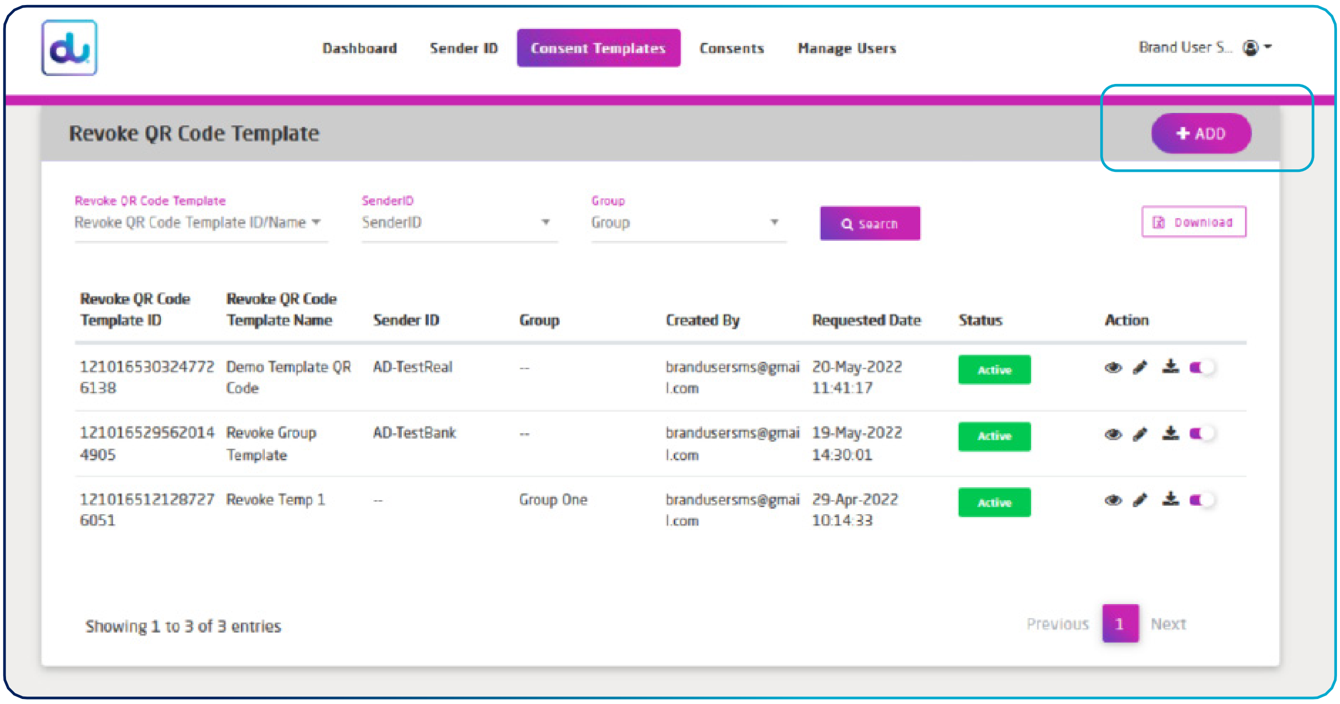
Module Functionalities:

1. Enables User to create new Revoke QR Code Templates.
2. Enables User to select desired Sender ID or Group to tag a Revoke QR Code Template.
3. Enables User to upload Company Logo to be displayed on Revoke QR Code Template.
4. Enables User to add special notes to the Revoke QR Code Template if required for additional information
5. Enables User to edit a QR Code Template to replace existing Sender ID/Group or Logo

Business Rules:

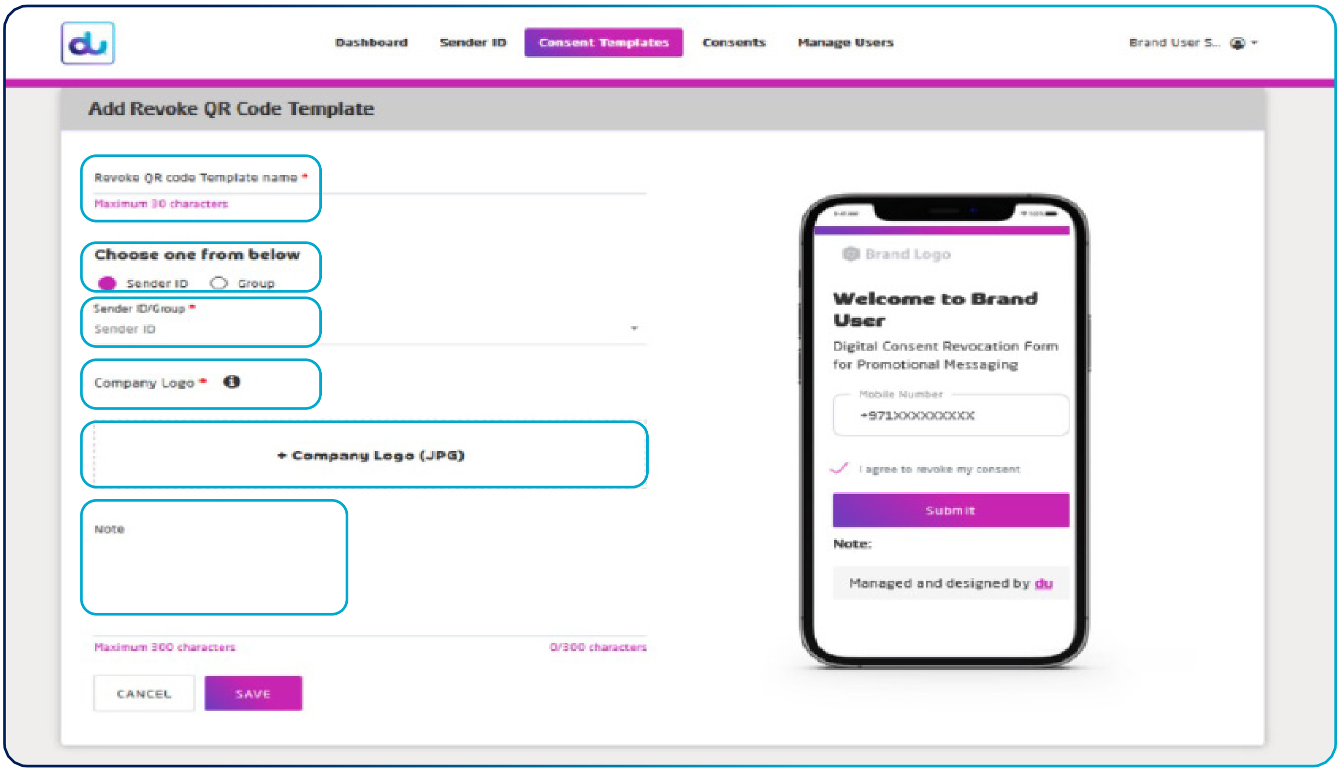
1. Revoke QR Code Template can only be created for promotional Sender IDs.
2. User will be able to select promotional Sender IDs with 'Active' or 'Suspended' status for template tagging.
3. Any particular Sender ID or a Group can only have one Revoke QR Code template tagging.
4. A Revoke QR Code Template cannot be deleted and can only be disabled.
5. User will be able to add "Note" with up to 300 characters
6. User will be able to upload company logo in JPG format with maximum 10MB file size

To create a new Revoke QR Code Template, the User will click "+ADD" button on the Revoke QR Code Template Page as shown below:

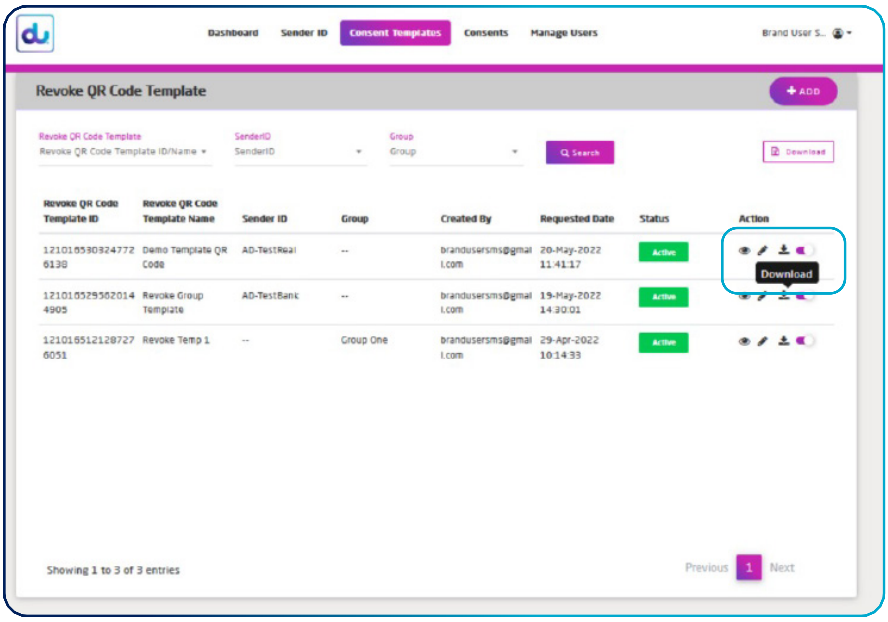


9.3 Creating Revoke QR Code Template

Once the "+ADD" button is clicked, the following QR Code Template creation screen will appear. The User will be required to enter template name, choose either a Sender ID or a Group radio button. In case Sender ID is selected, the User will enter an 'Active' or 'Suspended' status Sender ID. In case Group is selected, User will be required to enter Group name. User will be required to upload company logo to be displayed on the template. In case the User wants to add any special notes to be displayed to the end customer, User can input these in the Notes section. User can click 'SAVE' button to create the template.



Once the Revoke QR Code template is saved, User can view the created template from the Revoke QR Code Template home screen and download the QR Code by clicking the "Download" icon under the 'Action' tab. Once download is clicked, QR Code will be downloaded in PDF format file.



https://10.183.191.4/qrcode_templates/qrrevokerequest/9QqM7e5yngNpDg0RGEBe2vp5l/

9.4 Editing a Revoke QR Code Template

This functionality allows Admin and Normal Users to edit an existing Revoke QR Code Template.

Applicable to:

- Admin User
- Normal User

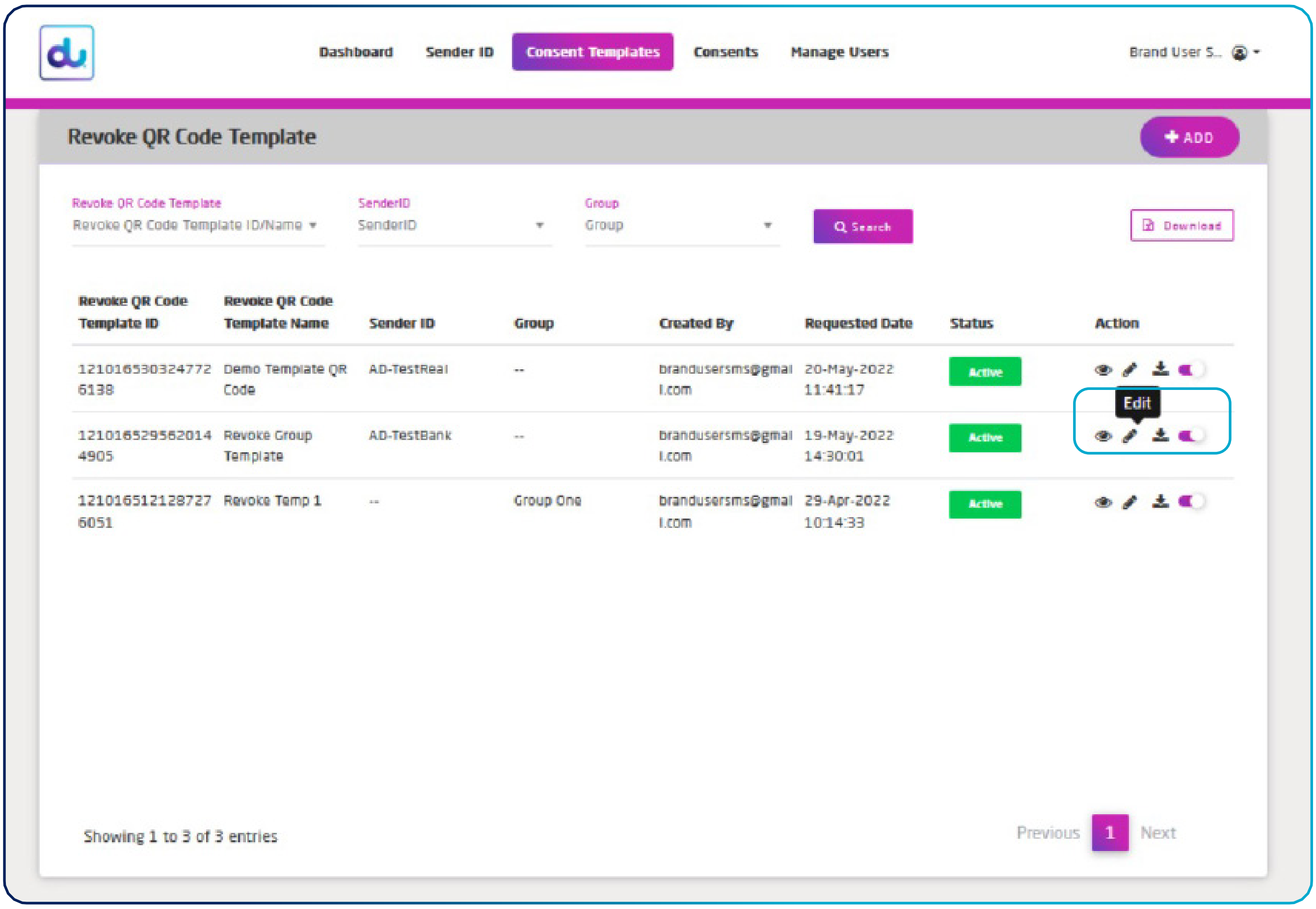
Module Functionalities:

1. Enables User to edit existing Revoke QR Code Templates.
2. Enables User to select a new Sender ID or Group to be tagged to an existing Revoke QR Code Template.
3. Enables User to upload a new Company Logo to be displayed on Revoke QR Code Template.
4. Enables User to update special notes to the Revoke QR Code Template.

Business Rules:

1. Editing a QR Code template will not generate a new QR Code pattern
2. Any particular Sender ID or a Group can only have one Revoke QR Code template tagging. In case a new QR code template needs to be created for the same Sender ID or Group, the Sender ID or the Group needs to be removed from the previous linked template.

To edit a new QR Code Template, the User will click "Pen" icon on the QR Code Template Page as below.



9.5. QR/Revoke QR Code Error Codes

Various error messages will be displayed in case QR Code or Revoke QR Code scanning is disabled. Following is the description of all error codes that will be displayed to the end user upon scanning of QR Code.

Scanning an "Inactive" QR/Revoke QR Code Template:

In case any template has been made inactive by the User, the following error message will be appear to the end customer upon scanning:

"Error code: 001. QR code scanning has been disabled."

Scanning the QR code for "Suspended" or "Suspend Restricted" Enterprise "Brands" accounts:

In case du has put an Enterprise "Brands" account under any suspension status on the Enterprise SMS Portal, the following error message will be appear to the end customer upon scanning:

"Error code: 002. QR code scanning has been disabled."

Scanning a QR/Revoke QR Code Template with a "Disabled" Sender ID status:

In case an end customer scans any QR/Revoke QR Code that is linked to a Sender ID with "Disabled" status, the following error message will be appear to the end customer upon scanning:

"Error code: 003. QR code scanning has been disabled."

Scanning a QR Code Template with a "Disabled" Consent Template:

In case any Consent Template tagged to a QR Code Template has been disabled, the following error message will be appear to the end customer upon scanning:

"Error code: 004. QR code scanning has been disabled."

Scanning a QR/Revoke QR Code Template with a "Deleted" or "Blacklisted" Sender ID status:

In case an end customer scans any QR/Revoke QR Code for a Sender ID with "Deleted" or "Blacklisted" status, the following error message will be appear to the end customer upon scanning:

"Error code: 005. QR code scanning has been disabled."

Disabled QR/Revoke QR Code Functionality:

In case of QR/Revoke QR Code functionality has been disabled for Enterprises ("Brands") by du, all types of QR/Revoke QR Code scanning will be disabled. The User will receive the following pop up message upon clicking QR Code or Revoke QR Code tab under the Consent Templates menu item.

"QR code functionality has been disabled. Kindly contact our customer care team at Care.Business@du.ae"

In case an end customer scans an existing QR Code/Revoke QR Code image, the following error message will appear to the end customer:

"Error code: 006. QR code scanning has been disabled."

10. Consents

This module allows Users to perform consent information related activities that include Consents Upload, Consents Revoke, access to Search Consents of any end customer, Enterprise Consents search for summary details or Consent Downloads functionality.

Applicable to:

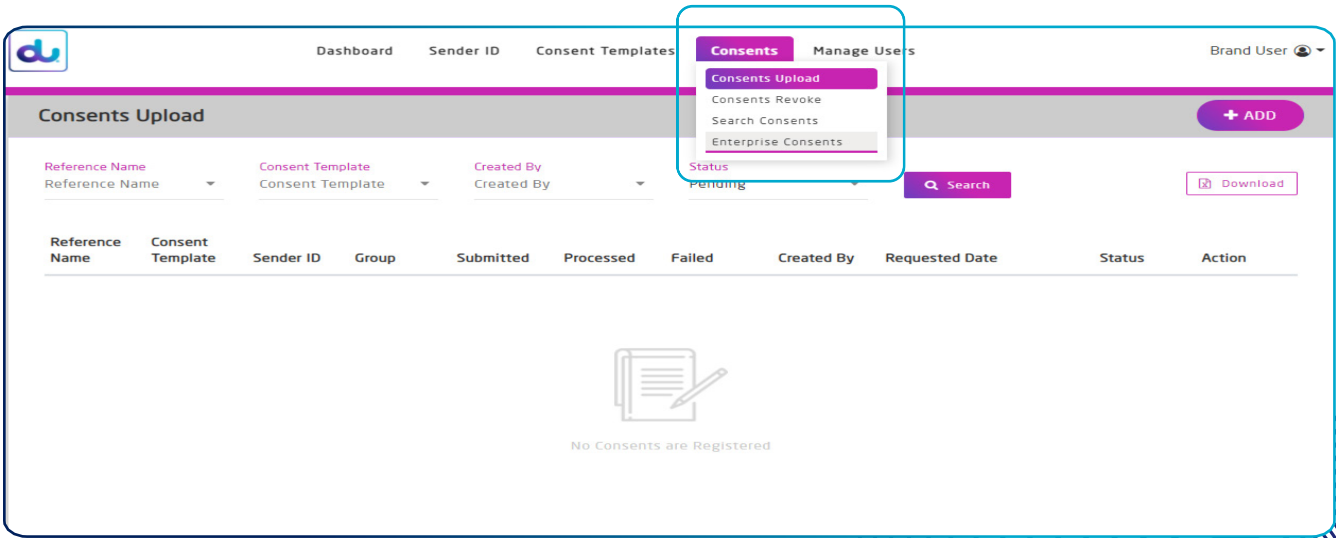
- Admin User
- Normal User
- Reporting User

Module Functionalities:

1. Enables User to upload new consents.
2. Enables User to revoke existing consents.
3. Enables User to search for consent based on MSISDN or Sender ID search filters.
4. Enable User to download consent information against a particular Sender ID.
5. Under ‘Enterprise Consents’ enables User to download the summary report of active consents count against a particular Sender ID
6. Under ‘Consent Downloads’ enables User to download consent information of all end customers for active consents

Business Rules:

1. There are 3 types of consents on the system:
   - Consent Type ‘Analog’ : Consents that hold evidence as a scanned image/document and are manually uploaded on the system via Consent Upload by Analog Type
   - Consent Type ‘Digital’ : which are acquired via any digital channel and are manually uploaded on the system via Consent Upload by Digital Type
   - Consent Type ‘QR Code’ : Consents which are acquired via QR Code scanning and directly uploaded on the system (refer to Section 8. Understanding QR Code Template of the User Guide)
2. Only Admin and Normal Users can upload or revoke consents.
3. Consents can be uploaded or revoked against Sender IDs that are in ‘Active’ or ‘Suspended’ status only.
4. Reporting User can only search consents.
5. Consent Downloads will only be done for active consents stored in the system. Revoked consents data will not be downloaded.



10.1 Consents Upload

This module allows Users to view information on all Consents Upload activities done by the User.

Applicable to:

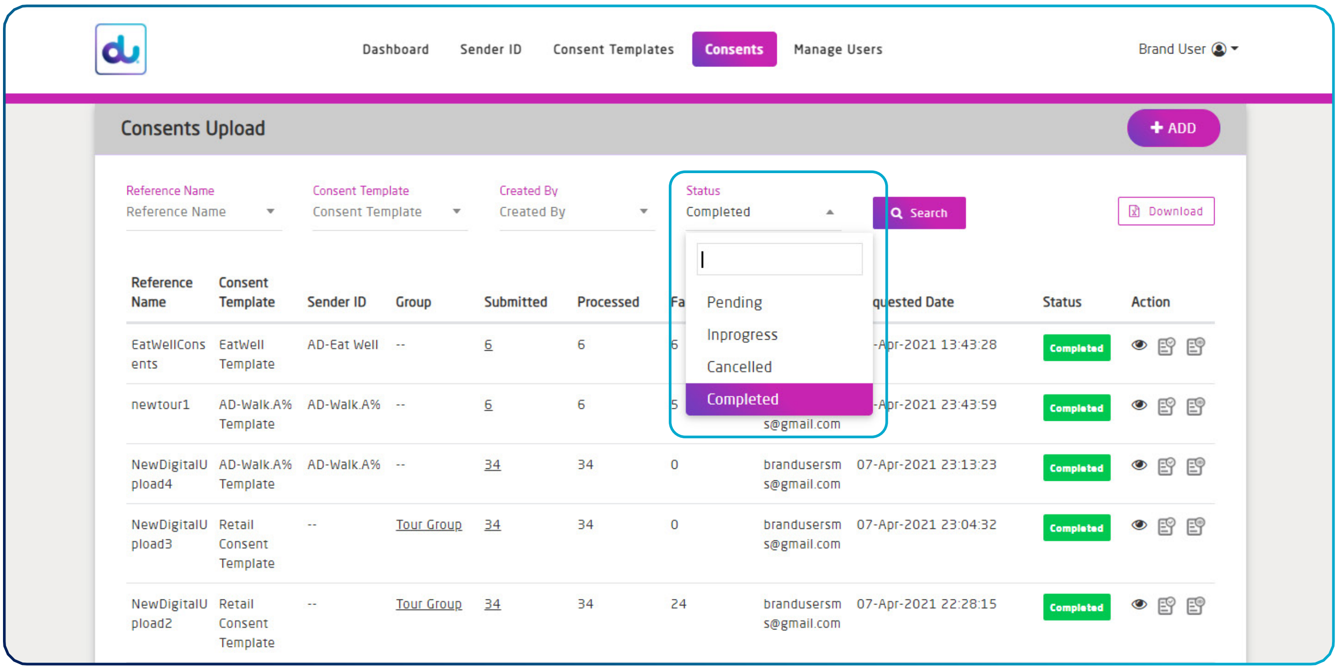
- Admin User
- Normal User
- Reporting User

Module Functionalities:

1. Enables User to view log of all Consents Upload activities based on their status.
2. Enables User to download the list of Consents Upload activity logs.
3. Enables User to view and download the summary of Consents Upload activity.
4. Enables User to download the detailed report against Consents Upload for failed cases.
5. Enables User to download the uploaded CSV file with MSISDNs for the Consents Upload activity.
6. Enables Admin and Normal User to create new Consents Upload activities.

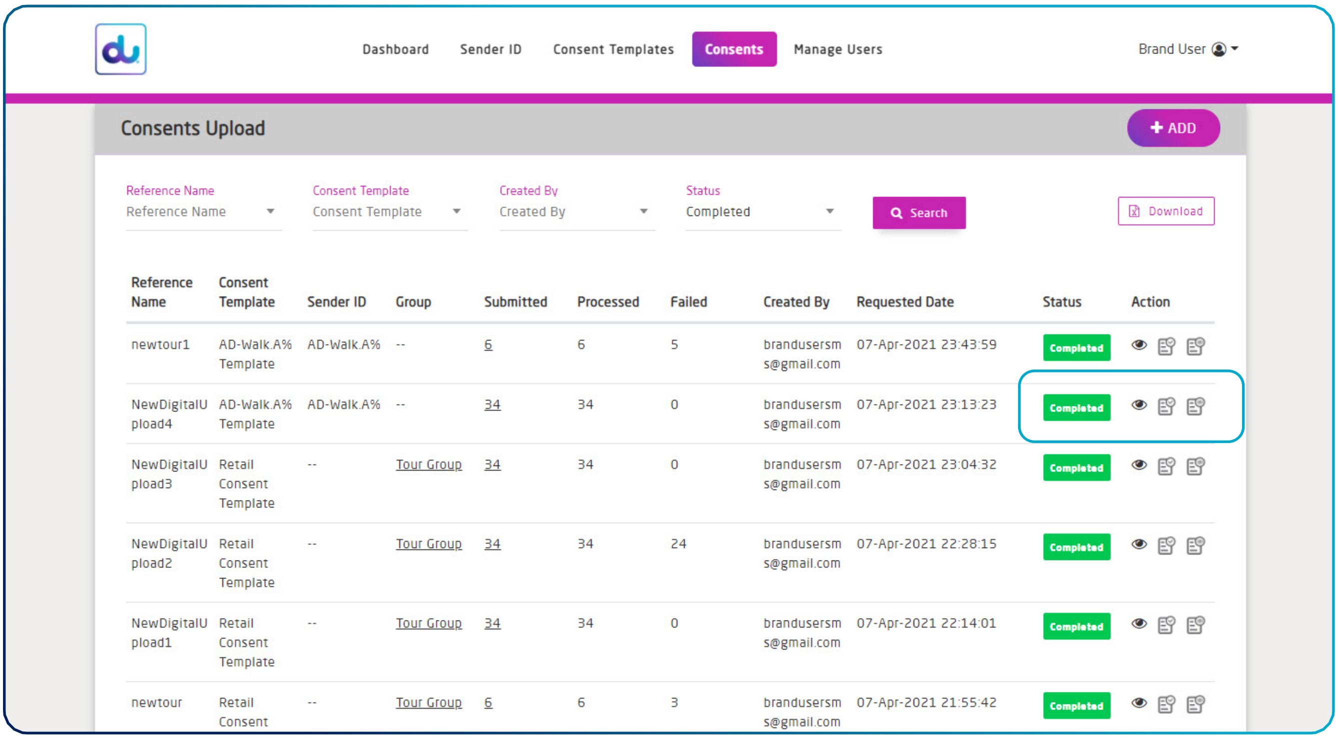
Business Rules:

1. All Users can view details for consent logs.
2. Admin and Normal Users are only allowed to add new Consents Upload.
3. User will be able to view each request as a separate row.
4. Activity logs of any one status will be shown at any one point of time.
5. Activity status: 'Pending' means that Consents Upload activity has been submitted to the system.
6. Activity status: 'In progress' means that consents are being updated on system.
7. Activity status: 'Completed' means that consents are successfully updated on the on system.
8. Activity status: 'Cancelled' means that the Consents Upload activity failed due to system issue.
9. Admin User will receive email notification once the status is completed.
10. User is able to filter request by reference name, Consent Template, created by and status filter.
11. User is able to view details of consent activity logs by clicking on the "EYE" icon under 'Action' tab.
12. User can download the list of MSISDN's upon clicking on the submitted column hyperlink.
13. User can download the list of Sender IDs tagged to a Group by clicking on the Group column hyperlink.

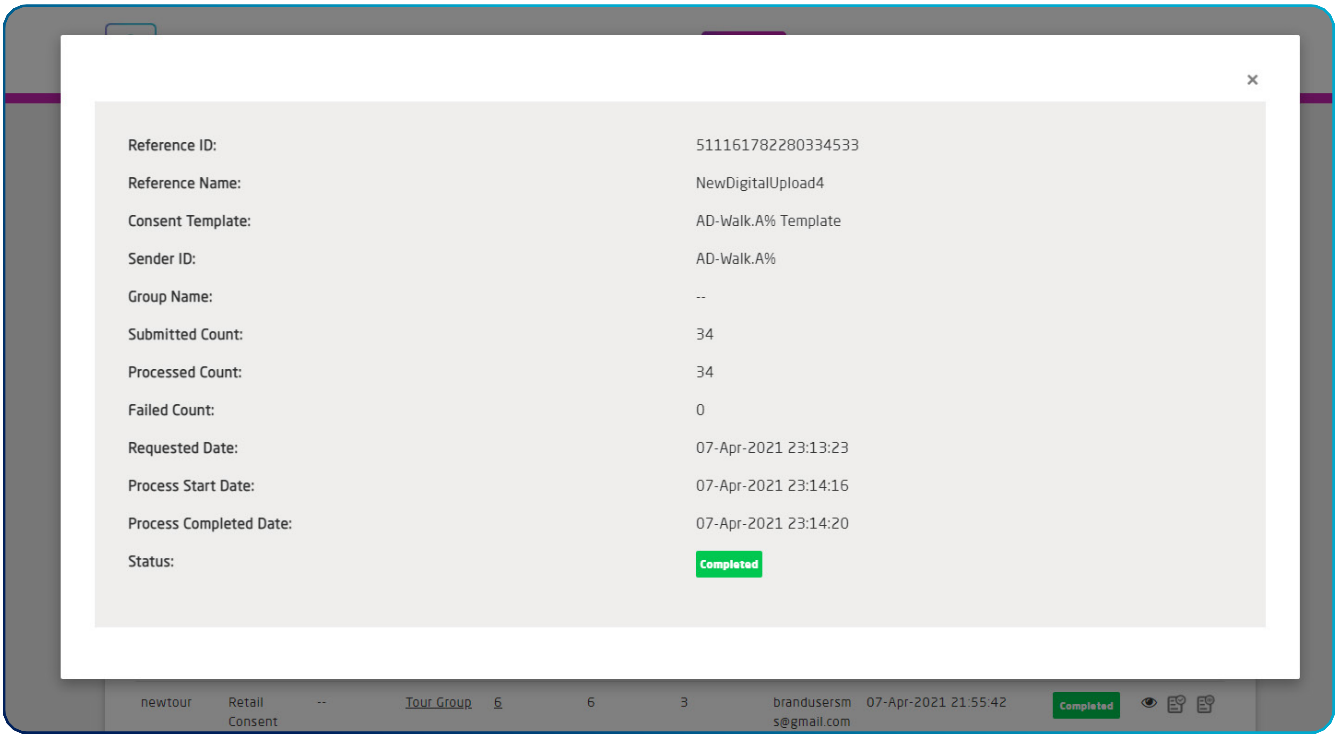


10.1.1 View Consents Upload Activity

To view the Consents Upload activity summary, click on the "EYE" icon under the 'Action' tab.

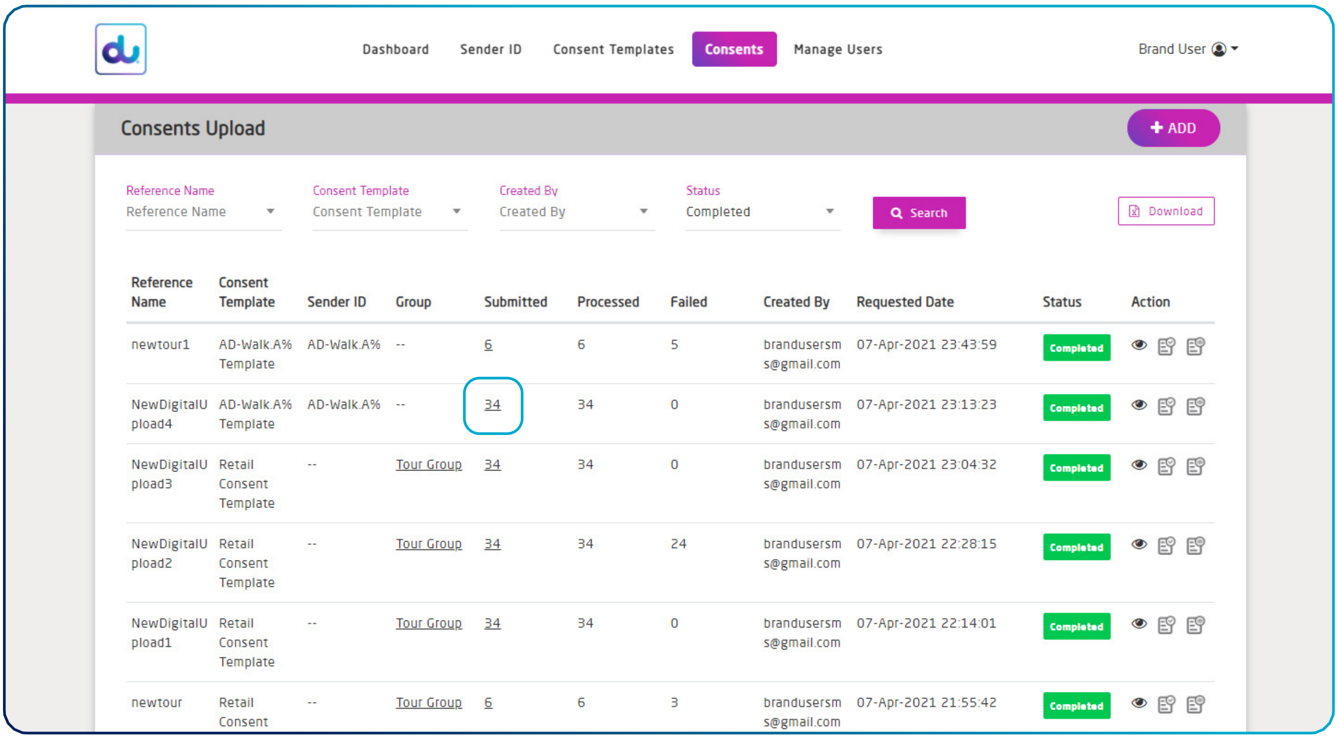


Once the "Eye" icon is clicked, the following summary page is displayed. The User can review the Consents Upload activity details including the count of total MSISDNs submitted, the total count of MSISDNs processed and the failed count. Also information on the status of the activity and activity start and end time is shown.



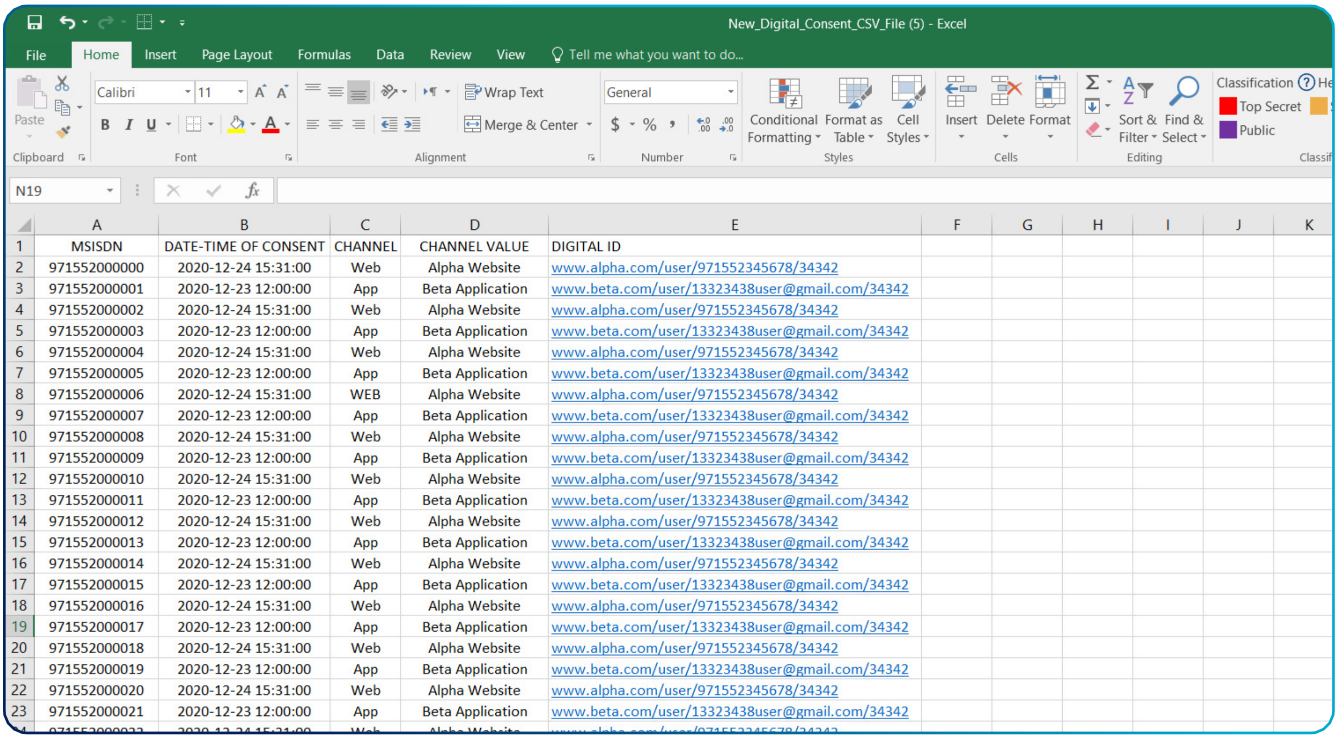
10.1.1 View Consents Upload Activity

To download the Consents Upload activity CSV file for each row, the User can click on the on the hyperlink under the 'Submitted' column tab. The CSV will be available as download file to the User.



Reference Name	Consent Template	Sender ID	Group	Submitted	Processed	Failed	Created By	Requested Date	Status	Action
newtour1	AD-Walk.A% Template	AD-Walk.A%	--	6	6	5	brandusersms@gmail.com	07-Apr-2021 23:43:59	Completed	
NewDigitalUpload4	AD-Walk.A% Template	AD-Walk.A%	--	34	34	0	brandusersms@gmail.com	07-Apr-2021 23:13:23	Completed	
NewDigitalUpload3	Retail Consent Template	--	Tour Group	34	34	0	brandusersms@gmail.com	07-Apr-2021 23:04:32	Completed	
NewDigitalUpload2	Retail Consent Template	--	Tour Group	34	34	24	brandusersms@gmail.com	07-Apr-2021 22:28:15	Completed	
NewDigitalUpload1	Retail Consent Template	--	Tour Group	34	34	0	brandusersms@gmail.com	07-Apr-2021 22:14:01	Completed	
newtour	Retail Consent	--	Tour Group	6	6	3	brandusersms@gmail.com	07-Apr-2021 21:55:42	Completed	

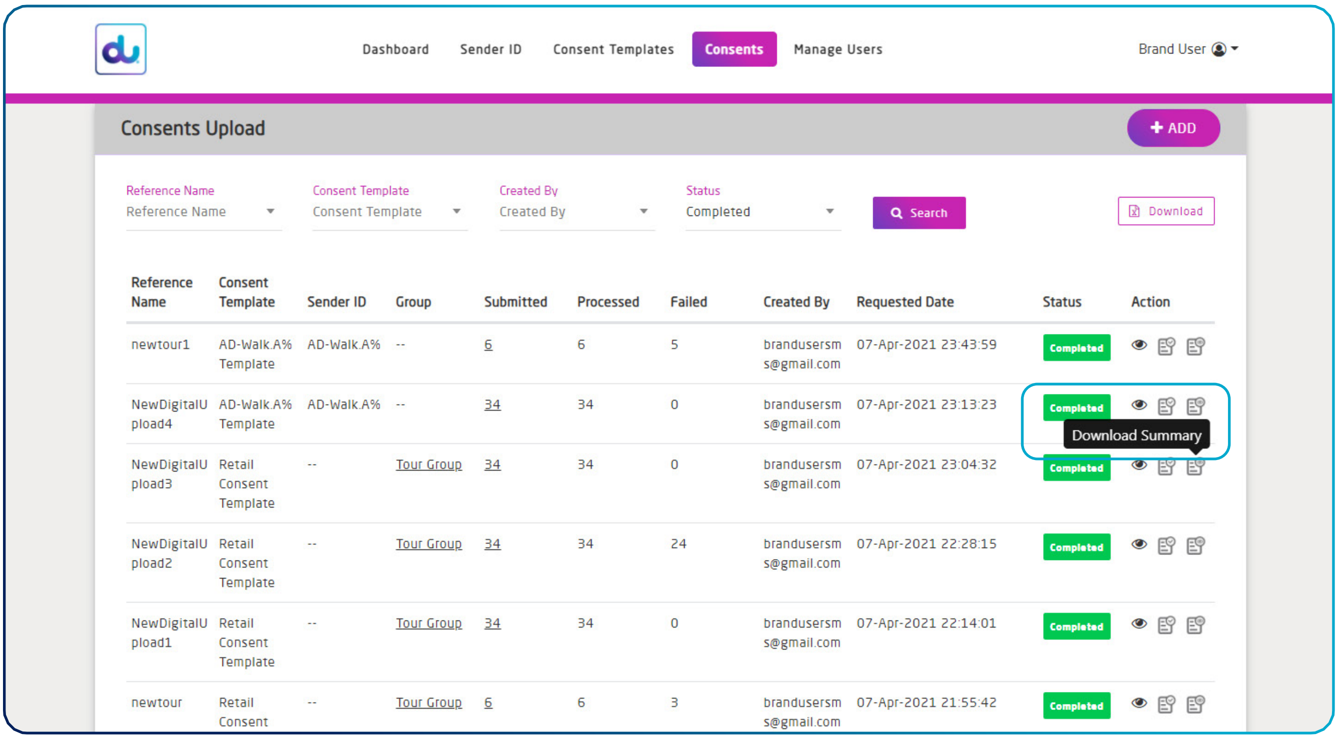
Sample downloaded file:



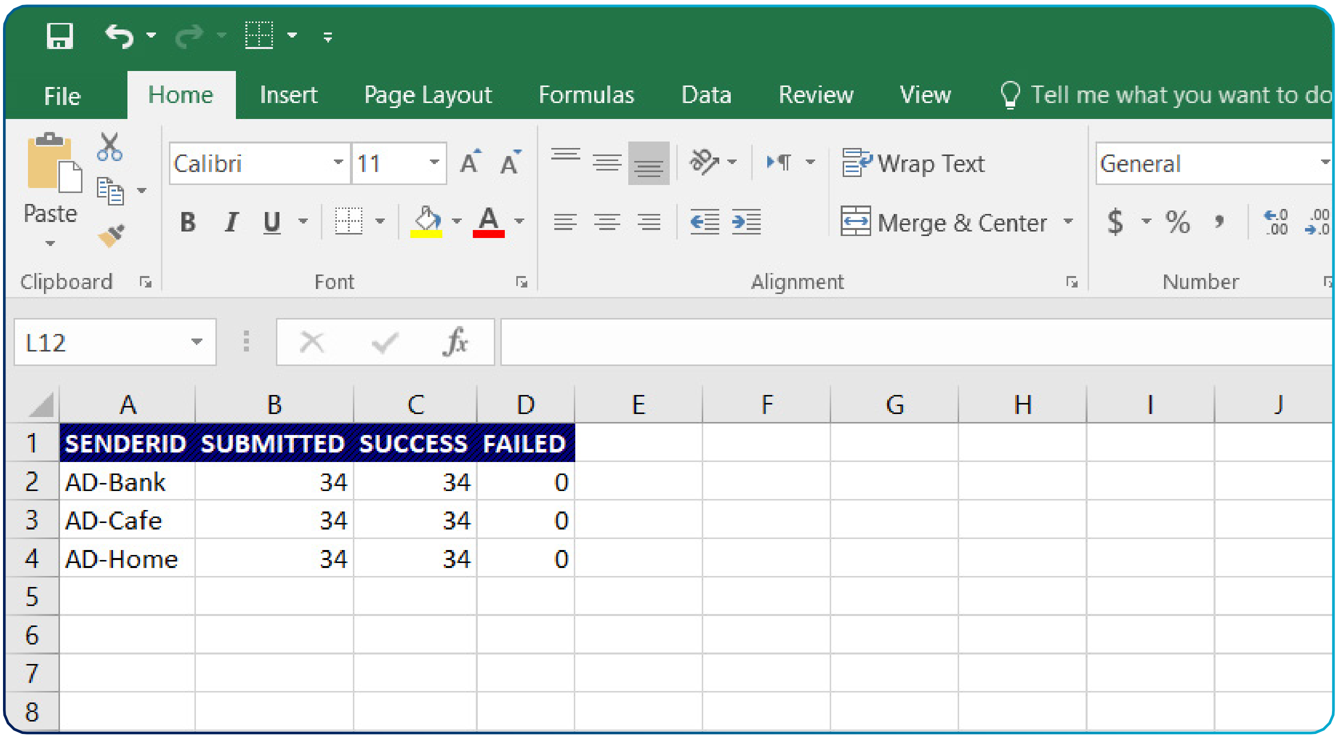
	A	B	C	D	E
1	MSISDN	DATE-TIME OF CONSENT	CHANNEL	CHANNEL VALUE	DIGITAL ID
2	971552000000	2020-12-24 15:31:00	Web	Alpha Website	www.alpha.com/user/971552345678/34342
3	971552000001	2020-12-23 12:00:00	App	Beta Application	www.beta.com/user/13323438user@gmail.com/34342
4	971552000002	2020-12-24 15:31:00	Web	Alpha Website	www.alpha.com/user/971552345678/34342
5	971552000003	2020-12-23 12:00:00	App	Beta Application	www.beta.com/user/13323438user@gmail.com/34342
6	971552000004	2020-12-24 15:31:00	Web	Alpha Website	www.alpha.com/user/971552345678/34342
7	971552000005	2020-12-23 12:00:00	App	Beta Application	www.beta.com/user/13323438user@gmail.com/34342
8	971552000006	2020-12-24 15:31:00	WEB	Alpha Website	www.alpha.com/user/971552345678/34342
9	971552000007	2020-12-23 12:00:00	App	Beta Application	www.beta.com/user/13323438user@gmail.com/34342
10	971552000008	2020-12-24 15:31:00	Web	Alpha Website	www.alpha.com/user/971552345678/34342
11	971552000009	2020-12-23 12:00:00	App	Beta Application	www.beta.com/user/13323438user@gmail.com/34342
12	971552000010	2020-12-24 15:31:00	Web	Alpha Website	www.alpha.com/user/971552345678/34342
13	971552000011	2020-12-23 12:00:00	App	Beta Application	www.beta.com/user/13323438user@gmail.com/34342
14	971552000012	2020-12-24 15:31:00	Web	Alpha Website	www.alpha.com/user/971552345678/34342
15	971552000013	2020-12-23 12:00:00	App	Beta Application	www.beta.com/user/13323438user@gmail.com/34342
16	971552000014	2020-12-24 15:31:00	Web	Alpha Website	www.alpha.com/user/971552345678/34342
17	971552000015	2020-12-23 12:00:00	App	Beta Application	www.beta.com/user/13323438user@gmail.com/34342
18	971552000016	2020-12-24 15:31:00	Web	Alpha Website	www.alpha.com/user/971552345678/34342
19	971552000017	2020-12-23 12:00:00	App	Beta Application	www.beta.com/user/13323438user@gmail.com/34342
20	971552000018	2020-12-24 15:31:00	Web	Alpha Website	www.alpha.com/user/971552345678/34342
21	971552000019	2020-12-23 12:00:00	App	Beta Application	www.beta.com/user/13323438user@gmail.com/34342
22	971552000020	2020-12-24 15:31:00	Web	Alpha Website	www.alpha.com/user/971552345678/34342
23	971552000021	2020-12-23 12:00:00	App	Beta Application	www.beta.com/user/13323438user@gmail.com/34342

10.1.1 View Consents Upload Activity

Users can also download the 'Download Summary' report by clicking the 'File' icon under the action tab. The 'Download Summary' report provides summary details on the consent upload activity on summary count of consents submitted, successful and failed. The file will be exported as a download file to the User.

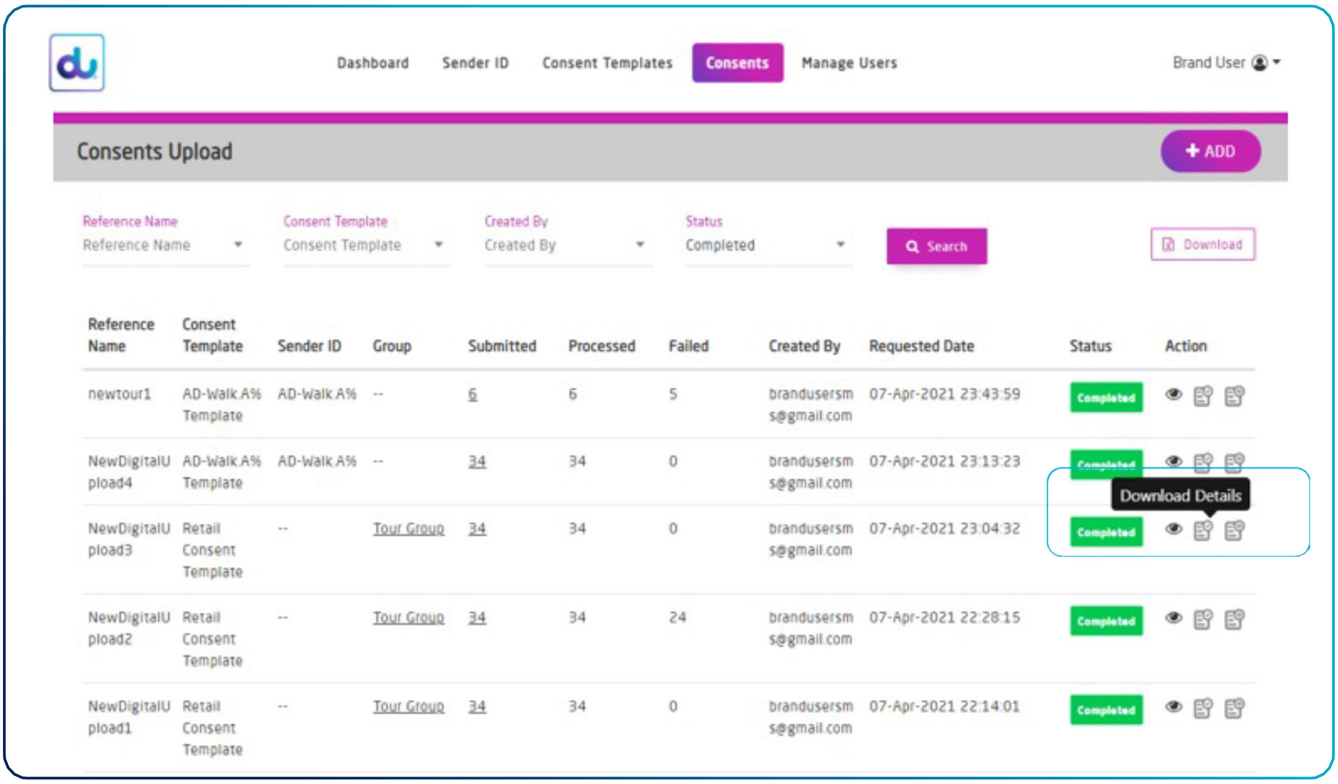


Sample downloaded file:



10.1.1 View Consents Upload Activity

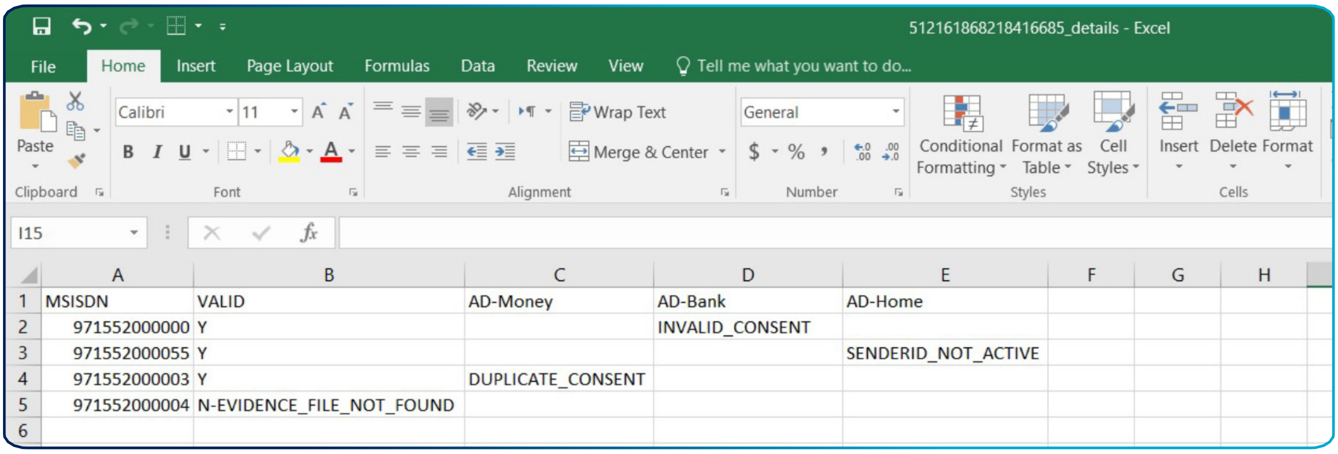
Users can also download the 'Download Details' report by clicking the 'File' icon under the action tab. The 'Download Details' report provides details on the Consents Upload activity for the MSISDNs where consent upload has failed. The report provides the failure reason only for the failed MSISDNs along with Sender ID on which the consents failed to upload. The file will be exported as a download file to the User.



Sample downloaded file as below. In the below example, the 'Consents Upload' activity was done using a Group with multiple Sender IDs tagged to the Group. Where the consent upload has failed for the

mentioned MSISDN, the column under the specific Sender ID will show the specific error code as the reason of consent upload failure. In case the column value is empty, the consent upload was successful against the specific Sender ID.

Only in case of 'Analog' type consent, if the evidence file does not contain the scanned document against a MSISDN, the column 'VALID' will contain error code: 'Evidence_File_Not_Found' and consent upload against all Sender IDs will fail hence no further error codes will be shown under Sender ID columns as shown below.



MSISDN	VALID	AD-Money	AD-Bank	AD-Home
971552000000	Y		INVALID_CONSENT	
971552000055	Y			SENDERID_NOT_ACTIVE
971552000003	Y	DUPLICATE_CONSENT		
971552000004	N-EVIDENCE_FILE_NOT_FOUND			

10.1.2 Understanding Consent Upload Error Codes

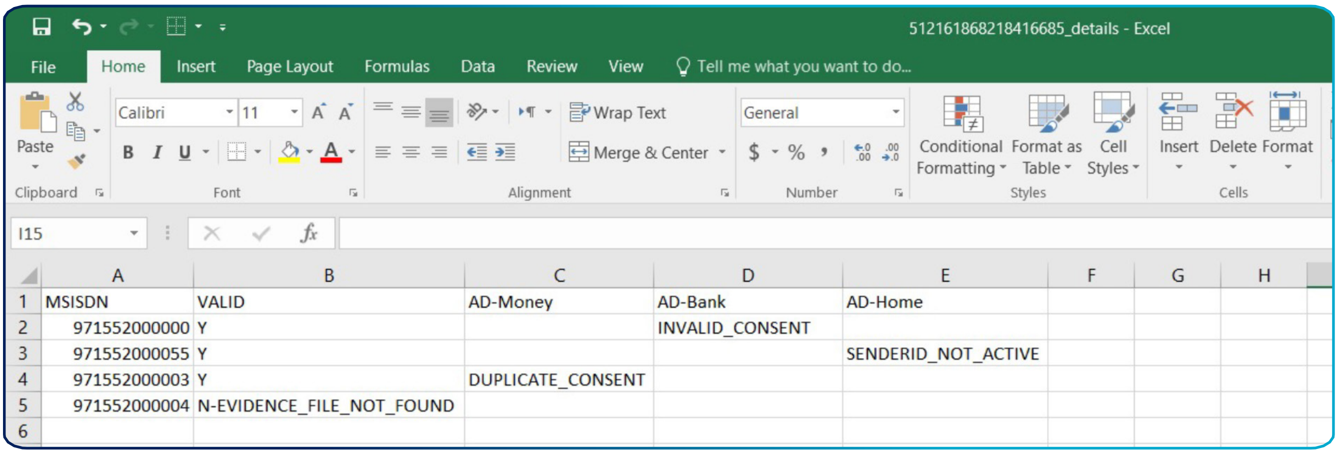
Following are the error codes and their explanation in case of a consent upload failures:

DUPLICATE_CONSENT: System will return this error in case there is an existing consent for the same Sender ID against a particular MSISDN

INVALID_CONSENT: System will return this error code in case an already revoked consent is being uploaded again i.e. the consent date is older than the consent revoke date.

SENDERID_NOT_ACTIVE: System will this return error code in case the Sender ID was disabled by the telecom operator

EVIDENCE_FILE_NOT_FOUND: System will return this error code in case the file name of the scanned document in the CSV file does not match with file name available in the Evidence file (ZIP) or no scanned document is found against the MSISDN in the Evidence file (ZIP). This error code will only be returned for 'Analog' type of 'Consent Upload' activity.



MSISDN	VALID	AD-Money	AD-Bank	AD-Home
971552000000	Y		INVALID_CONSENT	
971552000055	Y			SENDERID_NOT_ACTIVE
971552000003	Y	DUPLICATE_CONSENT		
971552000004	N-EVIDENCE_FILE_NOT_FOUND			

In the above example:

Against 97155200000, consent upload was successful for Sender IDs: AD-Money and AD-Home however consent upload failed for AD-Bank as a previous consent against AD-Bank was revoked and the User was uploading the consent with the old consent date.

Against 971552000055, consent upload was successful for Sender IDs: AD-Money and AD-Bank however consent upload failed for AD-Home as the Sender ID was disabled by the telecom operator at the time of consent upload activity.

Against 971552000003, consent upload was successful for Sender IDs: AD-Bank and AD-Home however consent upload failed for AD-Money as the consent already exists against this subscriber for the mentioned Sender ID.

Against 971552000004, consent upload failed for all Sender IDs since no file name was found in the Evidence file (ZIP). Only the 'VALID' column will reflect the error code in case of 'Analog' type of consent upload activity.

10.1.3 Creating Consents Upload Activity

This module allows Admin and Normal Users to create new Consents Upload request by submitting CSV files against a Sender ID or Group.

Applicable to:

- Admin User
- Normal User

Module Functionalities:

1. Enables User to upload consent information against a Sender ID or Group.
2. Enables User to upload consent in form of Analog or Digital type consent information.
3. Enables User to select a consent template against a Sender ID or a Group.
4. Enables User to upload a single CSV file for the Digital consent type.
5. Enables User to upload CSV file and ZIP Evidence file for the Analog consent type.
6. Enables email notification to User after consent uploading activity is successfully completed.
7. Provides CSV sample file to be downloaded from the portal for each consent type.

Business Rules:

For Analog consent type:

1. Users can upload CSV file with below details:

a. 'MSISDN' column value starting with "971" with a max 12 digit length.

b. 'Date of consent' column value with "YYYY-MM-DD" format.

c. 'File name' column value with name of the scanned document for each MSISDN.

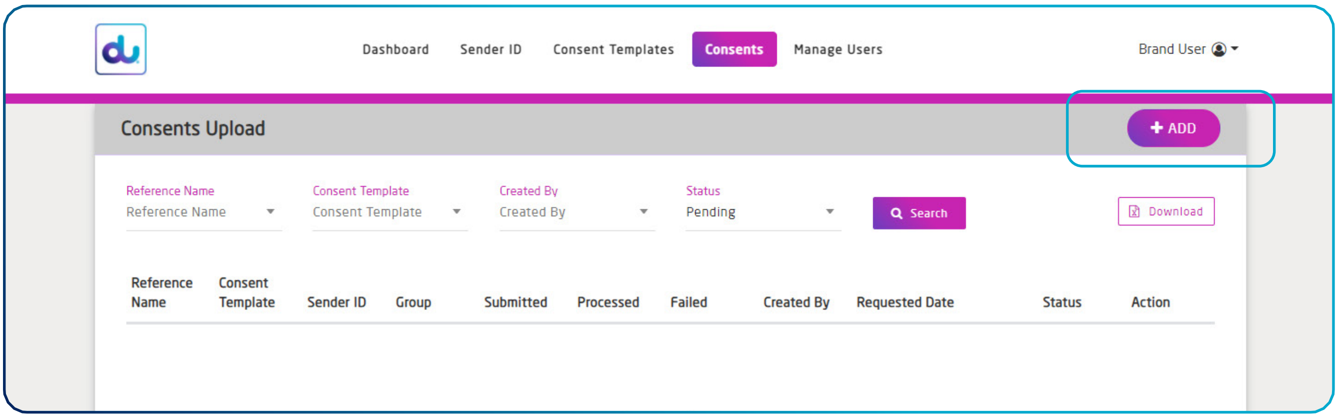
2. The size of the CSV file can be 2 MB maximum and Evidence file (ZIP) can be 50 MB maximum.
3. Evidence file (ZIP) can only contain scanned document in PDF or JPG/JPEG format.
4. Evidence file (ZIP) must contain at least 1 scanned document.
5. Evidence file (ZIP) can only be in format of ZIP.
6. For each MSISDN in CSV file, a corresponding scanned document to be available in Evidence file.
7. The file name of the scanned document in CSV file and Evidence file (ZIP) are case sensitive and must match to successfully upload the consent.

For Digital consent type:

1. User can upload CSV file with below details:
   a. 'MSISDN' column values starting with "971" with a max 12 digit length.
   b. 'DATE-TIME OF CONSENT' column value with "YYYY-MM-DD HH:MM:SS" format.
   c. 'CHANNEL' column value with "Web" or "App".
   d. 'CHANNEL VALUE' column value with name of website or mobile application with maximum length 50 characters.
   e. 'DIGITAL ID' column value with system generated unique ID as evidence of mobile subscriber consent with maximum 500 characters.
2. The size of the CSV file can be 2 MB maximum.

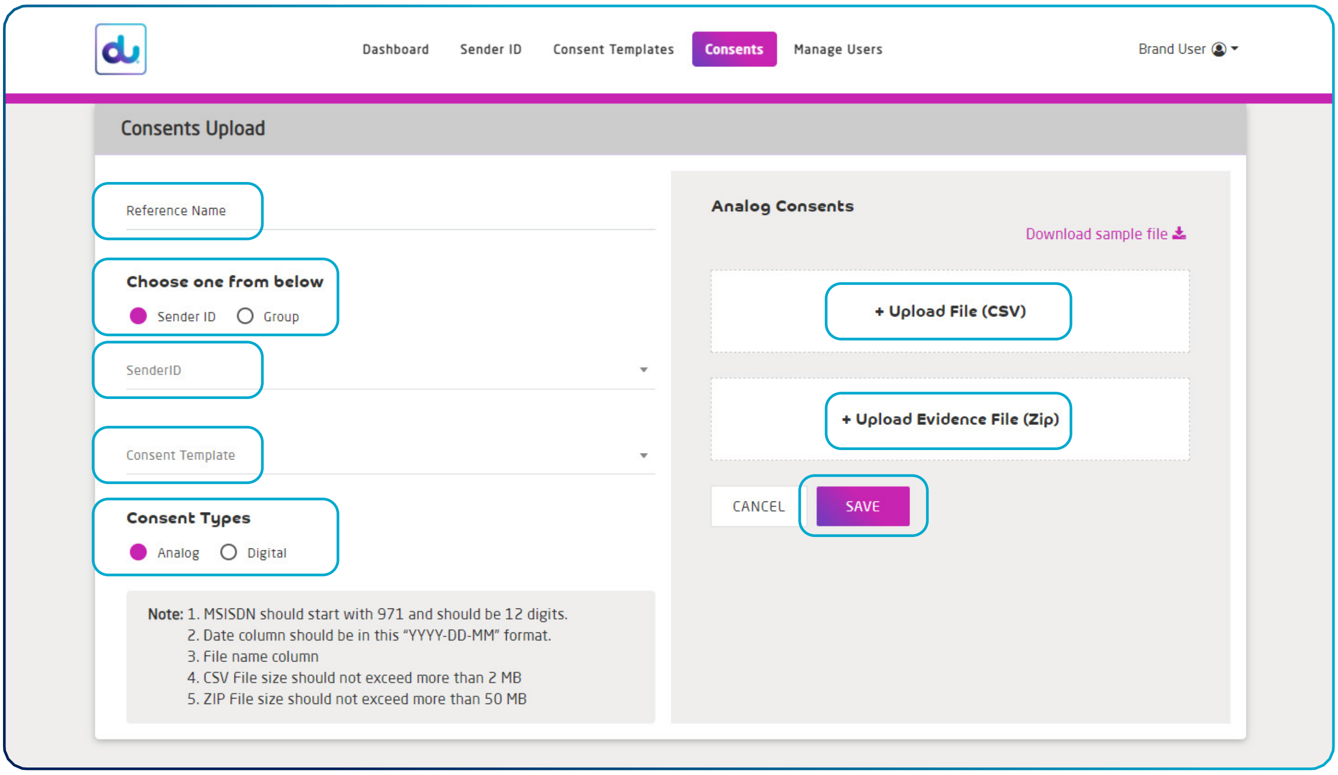
10.1.3 Creating Consents Upload Activity

To create a new Consents Upload activity, the User will click on "+ADD" button on the Consents Upload screen.



Once the "+ADD" button is clicked, the User will be directed to the following menu screen. The User will need to perform the following actions to initiate the activity:

- Insert a reference name in the 'Reference Name' field
- Choose Sender ID or Group option against which the Consent Uploads are required
- Select an active Sender ID or Group against which the Consent Uploads are required
- Select an active Consent Template associated with the Sender ID or Group
- Choose the Consent Type i.e. Analog or Digital
- Upload the CSV and the Evidence File (ZIP) and click "SAVE" button to complete the activity

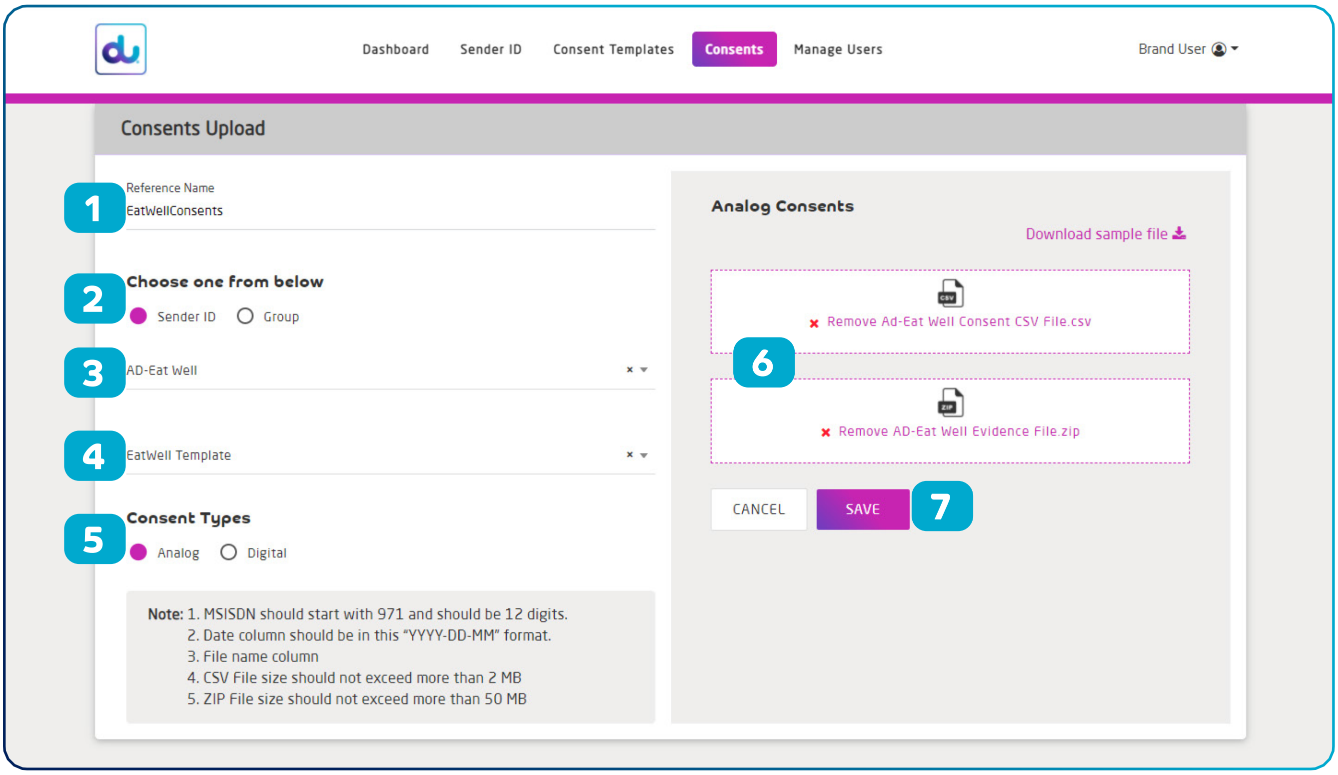


10.1.4 Consents Upload by Analog Type

The Consents Upload activity by Analog type is done when consent information evidence against any mobile subscriber is available in form of a scanned document with signature e.g. signing of an application form the by mobile subscriber. User will be required to upload the scanned document as evidence on the system.

Once the User creates a new Consents Upload activity to upload consents for Analog type, User will be required to perform following steps:

1. Insert a reference name in the 'Reference Name' field.
2. Choose Sender ID or Group option against which the Consents Upload is required.
3. Select an active Sender ID or Group against which the Consents Upload is required.
4. Select an active Consent Template associated with the Sender ID or Group.
5. Choose the Consent Type as Analog.
6. Upload the CSV and the Evidence File (ZIP).
7. Click "SAVE" button to complete the activity.



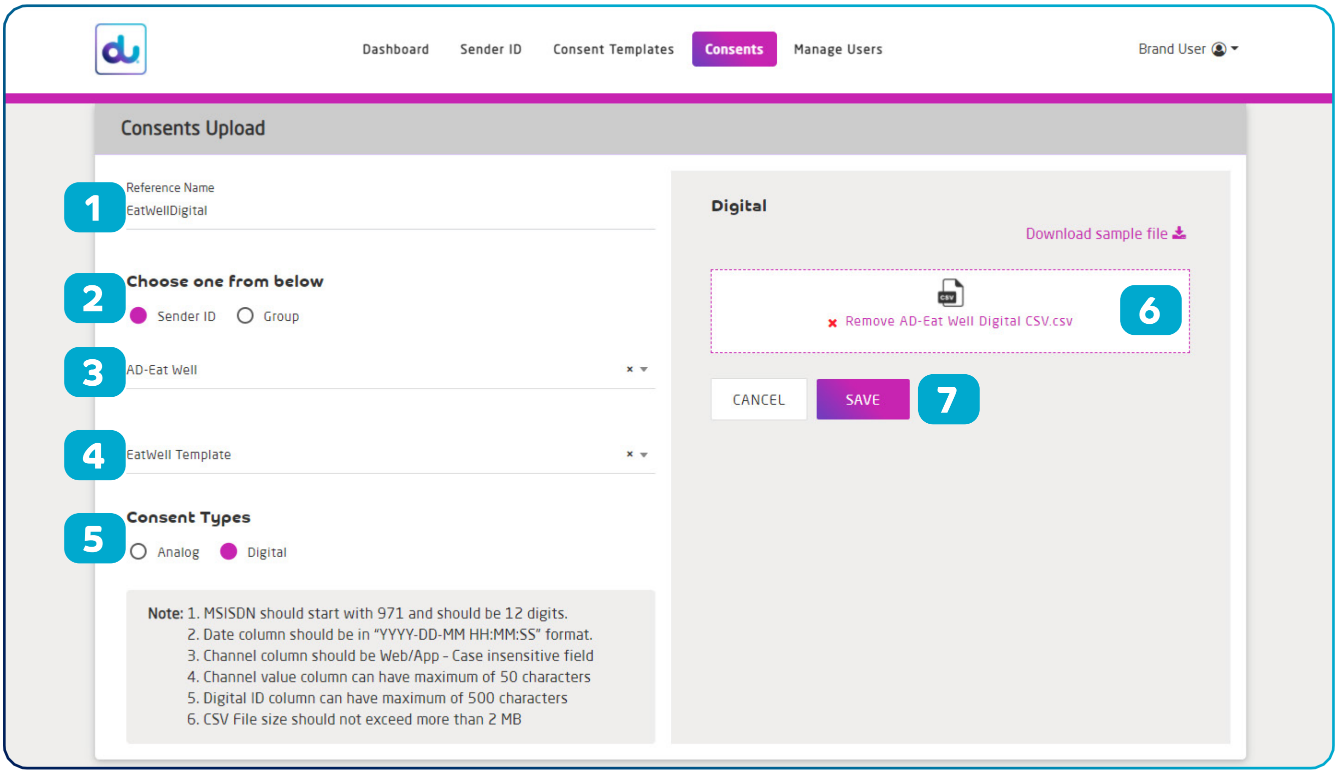
User must prepare the CSV file given the provided business rules as shown above in the menu screen. User can also click "Download sample file" icon in the above screen to download a CSV sample file to fill in the consent information. In case of use of incorrect format, the CSV file will not be uploaded.

10.1.5 Consents Upload by Digital Type

The Consents Upload activity by Digital type is done when consent information evidence against any mobile subscriber is available in any form of digital evidence i.e. the mobile subscriber has not physically signed any application form however subscribed to receive promotional SMS by subscribing to any of the digital channels such as a mobile application or website membership. User will be required to upload only CSV file containing all the evidence in digital form on the system.

Once the User creates a new Consents Upload activity, to upload consents for 'Digital' type User will be required to perform following steps:

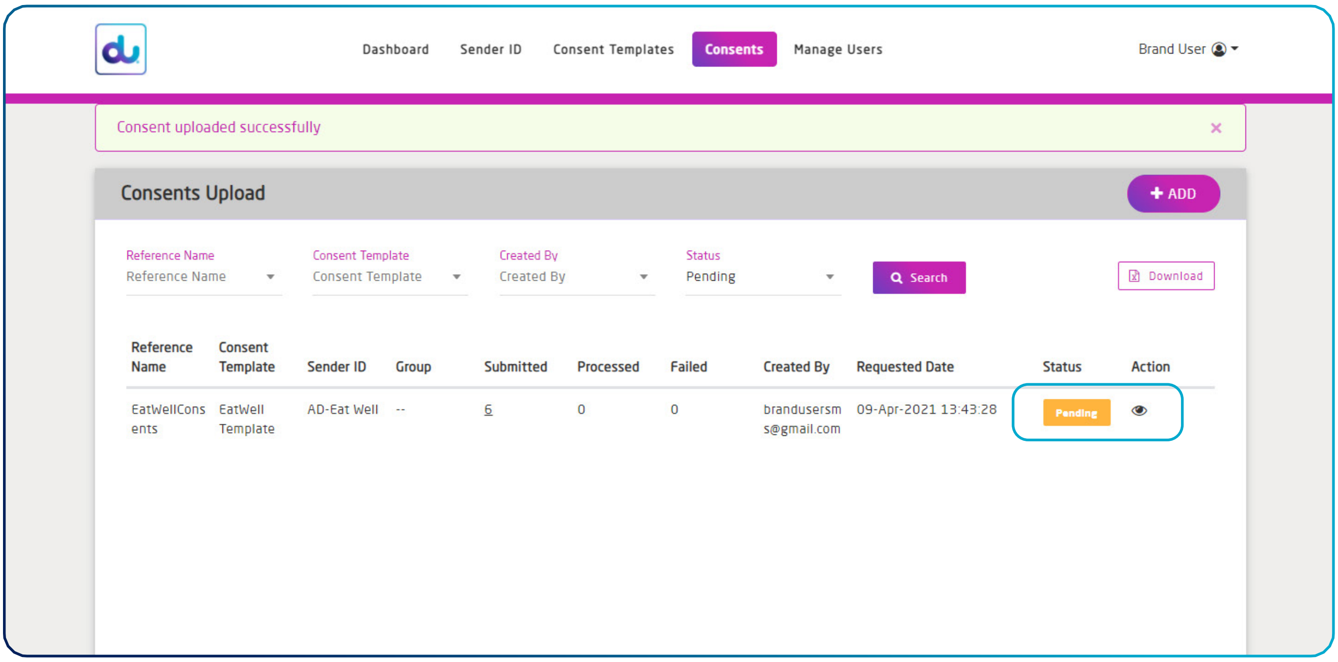
1. Insert a reference name in the 'Reference Name' field.
2. Choose Sender ID or Group option against which the Consents Upload are required.
3. Select an active Sender ID or Group against which the Consents Upload are required.
4. Select an active Consent Template associated with the Sender ID or Group.
5. Choose the Consent Type as 'Digital'.
6. Upload the CSV file.
7. Click "SAVE" button to complete the activity.



User must prepare the CSV file given the provided business rules as shown above in the menu screen. User can also click "Download sample file" icon in the above screen to download a CSV sample file to fill in the consent information. In case of use of incorrect format, the CSV file will not be uploaded.

10.1.6 Creating Consents Upload Activity

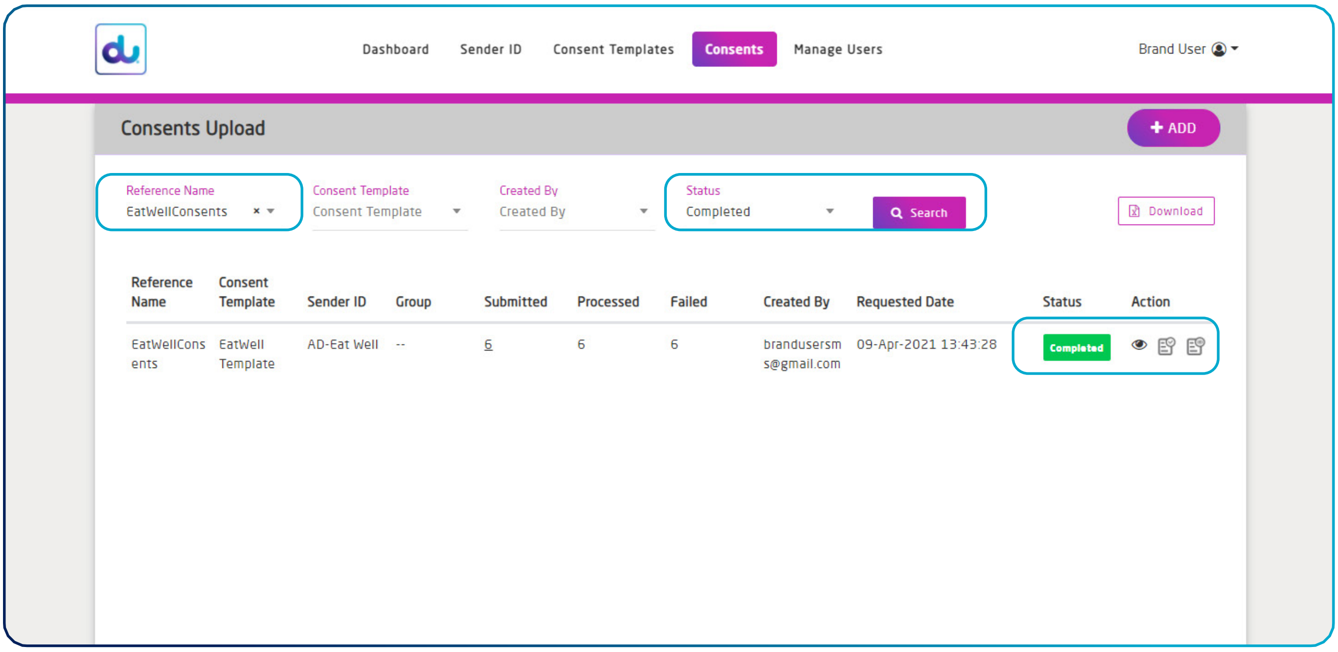
Once the User clicks the "Save" button and all document uploads have been accepted, the activity will be successfully submitted to the system and the User will be directed to activity log screen. The status of the upload activity will appear 'Pending' under the status tab.



Once the upload activity starts to update to the system, the activity log status will change from 'Pending' to 'In progress' status. One all the consents have been successfully updated in the system, then the activity log status will be changed to 'Completed' as show below: At any stage User can view the status details by

clicking the "Eye" icon under the 'Action' tab. To check the 'Consents Upload' activity results, User can click the "Download Details" or "Download Summary" file icon under the 'Action' tab.

At any point of time, if the User wishes to see the current status of any activity, the User can insert the activity reference name in the 'Reference Name' field then choose between different statuses and click search to find the updated status as shown below:



10.1.7 Preparing CSV Files Format

The CSV files for 'Analog' or 'Digital' uploads must be prepared in accordance with the business rules mentioned. Any wrong format will result in the CSV file to be rejected.

For Analog CSV File:

In case User is using Microsoft Excel to prepare for the CSV file, the User must follow the following business rules for CSV File Columns and Values:

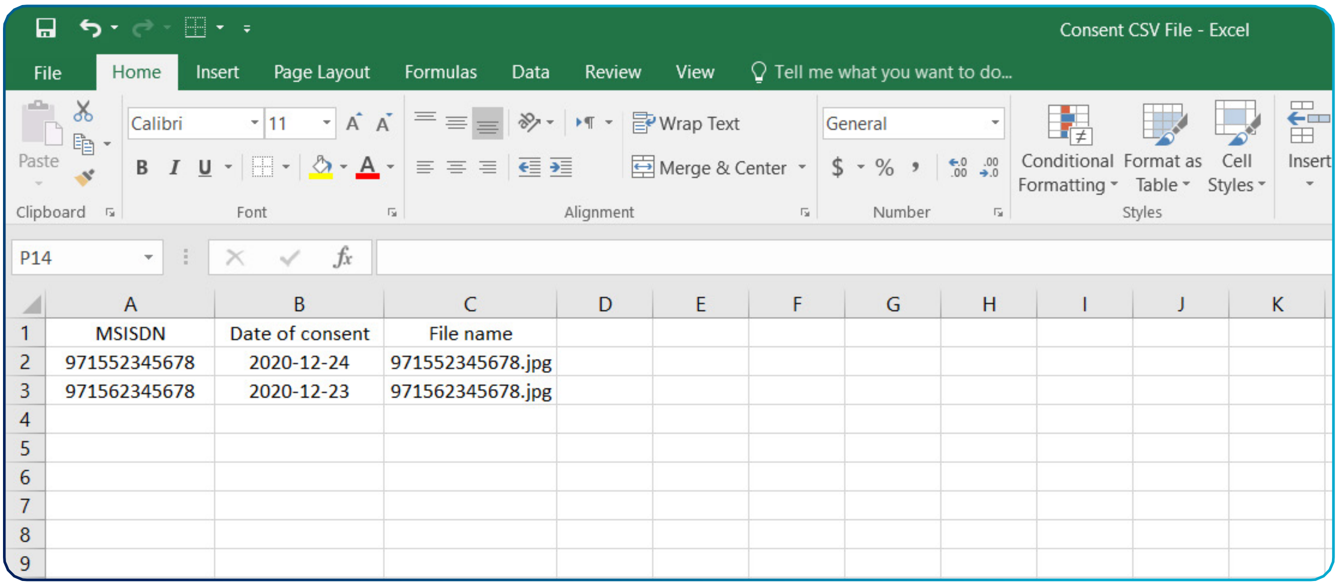
1. 'MSISDN' column value starting with "971" with a max 12 digit length
2. 'Date of consent' column value with "YYYY-MM-DD" format.
3. 'File name' column value as the name of the scanned document in evidence file for each MSISDN
4. For each MSISDN entry in CSV file, Evidence file (ZIP) must contain corresponding scanned document else the consent upload for the particular MSDISN will fail. The file names of the scanned document in CSV file and Evidence file (ZIP) must match and are case sensitive.
5. The size of the CSV file can be 2 MB maximum
6. The first line of the file is the header and must be retained as is. The header values are case sensitive hence must be used in the CSV with same sentence case as mentioned in below sample:

MSISDN	Date of consent	File name
971559512233	2020-12-12	scan971559512233.PDF

Refer table below for detailed rules:

Column Value	Format	Field Properties
MSISDN	971xxxxxxxxx	12-digit mobile number with country code starting with 971 only
Date of Consent	YYYY-MM-DD	Exact date format to be followed
File name	Filename.ext	File name must contain file extension name File name max length is 50 characters including extension name File name can also be mobile number starting with 971 only File name can be alphanumeric however cannot contain any Special Characters except "." (DOT), "_" (underscore), "-" (hyphen) for file extension name File names are case sensitive

Sample CSV File for Analog Type:

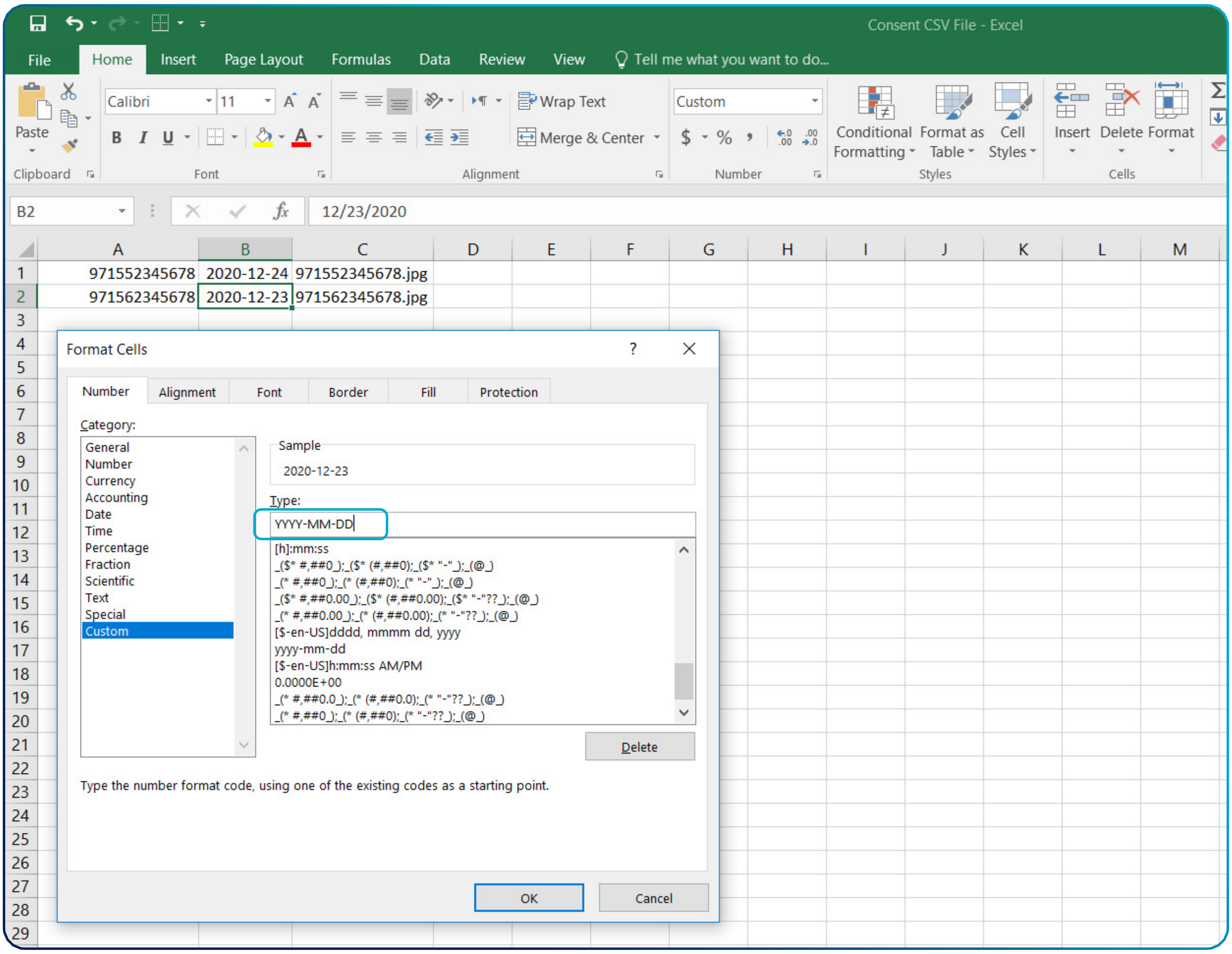


10.1.7 Preparing CSV Files Format

Date Field Formatting for Analog Type:

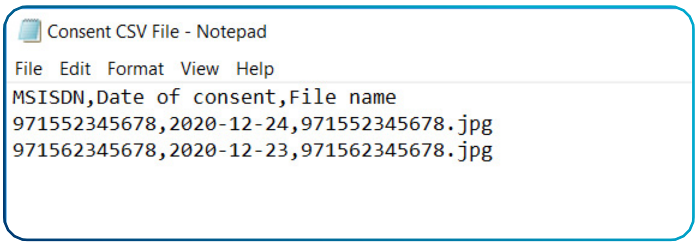
User can use the following instructions to format the date column. The date format has to be defined as a "Custom" format by right clicking "Column B" and selecting "Format Cells" property. Under Category select "Custom" and insert "YYYY-MM-DD" under type: label as shown in blue highlighted box below.

Click 'Ok' to save.



CSV Validation:

To validate if the format has been correctly saved, open the CSV file as a Notepad file. The notepad format should appear as follows. In case any other format is appearing, User must correct the format prior to uploading.


Consent CSV File - Notepad

File Edit Format View Help

```
MSISDN,Date of consent,File name
971552345678,2020-12-24,971552345678.jpg
971562345678,2020-12-23,971562345678.jpg
```

10.1.7 Preparing CSV Files Format

For Digital CSV File:

In case User is using Microsoft Excel to prepare for the CSV file, the User must follow the following business rules for CSV File Columns and Values:

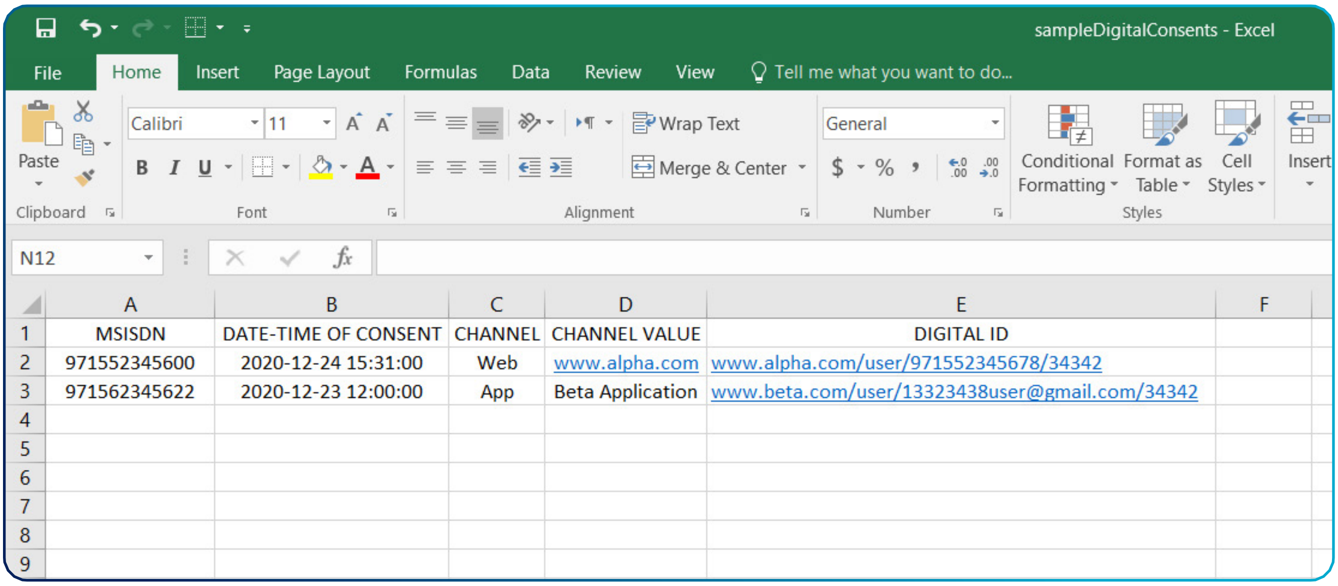
1. 'MSISDN' column values starting with "971" with a max 12 digit length.
2. 'DATE-TIME OF CONSENT' column value with "YYYY-MM-DD HH:MM:SS" format.
3. 'CHANNEL' column value as "Web" or "App".
4. 'CHANNEL VALUE' column value with name of website/mobile app with max length 50 characters.
5. 'DIGITAL ID' column value with system generated unique ID as evidence of mobile subscriber consent with maximum 500 characters.
6. The size of the CSV file can be 2 MB maximum.
7. The first line of the file is the header and must be retained as is. The header values are case sensitive hence must be used in the CSV with same sentence case as mentioned in below sample:

MSISDN	DATE-TIME OF CONSENT	CHANNEL	CHANNEL VALUE	DIGITAL ID
971559512233	2020-12-12 13:12:59	Web	www.alpha.com	alpha.com/12323/Userxxxxx213232?/3231

Refer table below for detailed rules:

Column Value	Format	Field Properties
Mobile Number	971xxxxxxxxx	12-digit mobile number with country code starting with 971 only
Date of Consent	YYYY-MM-DD HH:MM:SS	Exact date format to be followed
Digital Channel Type	Web or App	This field explains which digital channel was used to acquire the con-sent. Value can only be "Web" or "App" and are case insensitive
Channel Value	URL Address/Social Plat-form Name or Application Name	This field provides the name of the digital channel used to acquire the consent. Max character length is 50 characters with all ascii characters allowed.
Digital ID	System generated ID/ Log and/or Email Address	This field provides the evidence with the unique system ID generated by the system as part of acquiring consent. Email address can also be provided along with system ID as evidence. Max character length is 500 characters with ascii characters allowed.

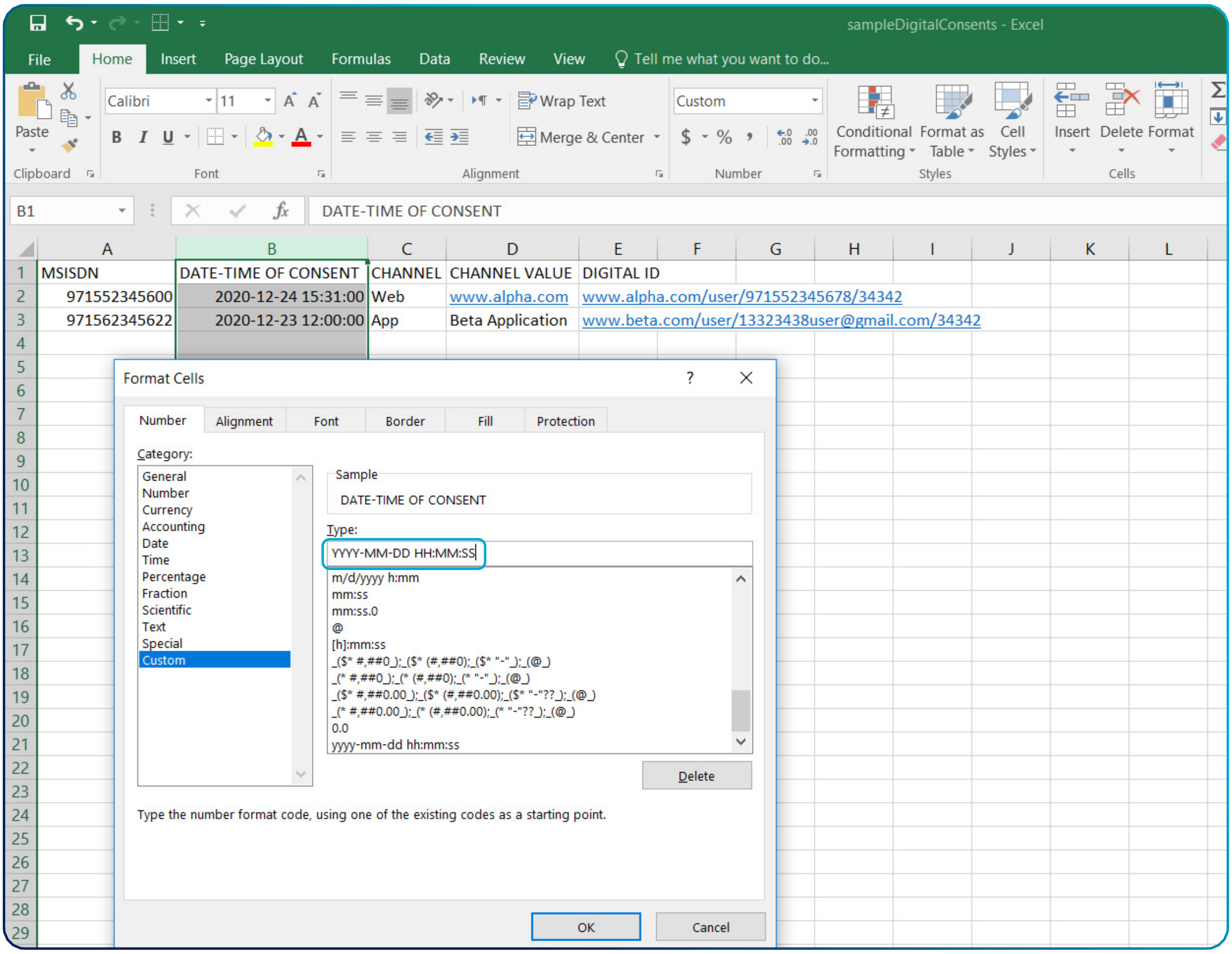
Sample CSV File for Digital Type



10.1.7 Preparing CSV Files Format

Date Field Formatting for Digital Type:

User can use the following instructions to format the date column. The date format has to be defined as a "Custom" format by right clicking "Column B" and selecting "Format Cells" property. Under Category select "Custom" and insert "YYYY-MM-DD HH:MM:SS" under type: label as shown in blue highlighted box below: Click 'Ok' to save.



CSV Validation:

To validate if the format has been correctly saved, open the CSV file as a Notepad file. The notepad format should appear as follows. In case any other format is appearing, User must correct the format prior to uploading.


sampleDigitalConsents - Notepad

File Edit Format View Help

```
MSISDN,DATE-TIME OF CONSENT,CHANNEL,CHANNEL VALUE,DIGITAL ID
971552345600,2020-12-24 15:31:00,Web,www.alpha.com,www.alpha.com/user/971552345678/34342
971562345622,2020-12-23 12:00:00,App,Beta Application,www.beta.com/user/13323438user@gmail.com/34342
```

10.1.8 QRCode Consents Uploads by Digital Type

Consents acquired via QR Code scanning will be directly uploaded in the system. In case of loss of consent data acquired via QR Code e.g. revocation by mistake or deletion of sender ID by mistake all consent data will be revoked against a particular sender ID. Such consent data cannot be reinstated in the system however the Portal provides consent data download functionality via "Consent Downloads" (refer to Section 11. Consent Downloads). In case User has previously downloaded QR Code consent data, such data can be uploaded again to the portal via use of Consent Upload by Digital Type. Manual re-upload of QR Code consents via Consent Upload by Digital Type activity will only be considered as "Digital Type" of consents and will no more be considered "QR Code Type" of consents anymore.

In case User is manually uploading QR Code consent data using Consent Upload by Digital Type, the User will follow the same steps and use the same Digital CSV file format with the following fields:

1. 'MSISDN' column values starting with "971" with a max 12 digit length.
2. 'DATE-TIME OF CONSENT' column value with "YYYY-MM-DD HH:MM:SS" format.
3. 'CHANNEL' column value as "QRCode".
4. 'CHANNEL VALUE' column value with QR Code Template ID with max length 50 characters.
5. 'DIGITAL ID' column value with First and Last Name with OTP value with maximum 500 characters.
6. The size of the CSV file can be 2 MB maximum.
7. The first line of the file is the header and must be retained as is. The header values are case sensitive hence must be used in the CSV with same sentence case as mentioned in below sample:

MSISDN	DATE-TIME OF CONSENT	CHANNEL	CHANNEL VALUE	DIGITAL ID
971559512233	2020-12-12 13:12:59	QRCode	1209167536527	John Doe|OTP = 941468

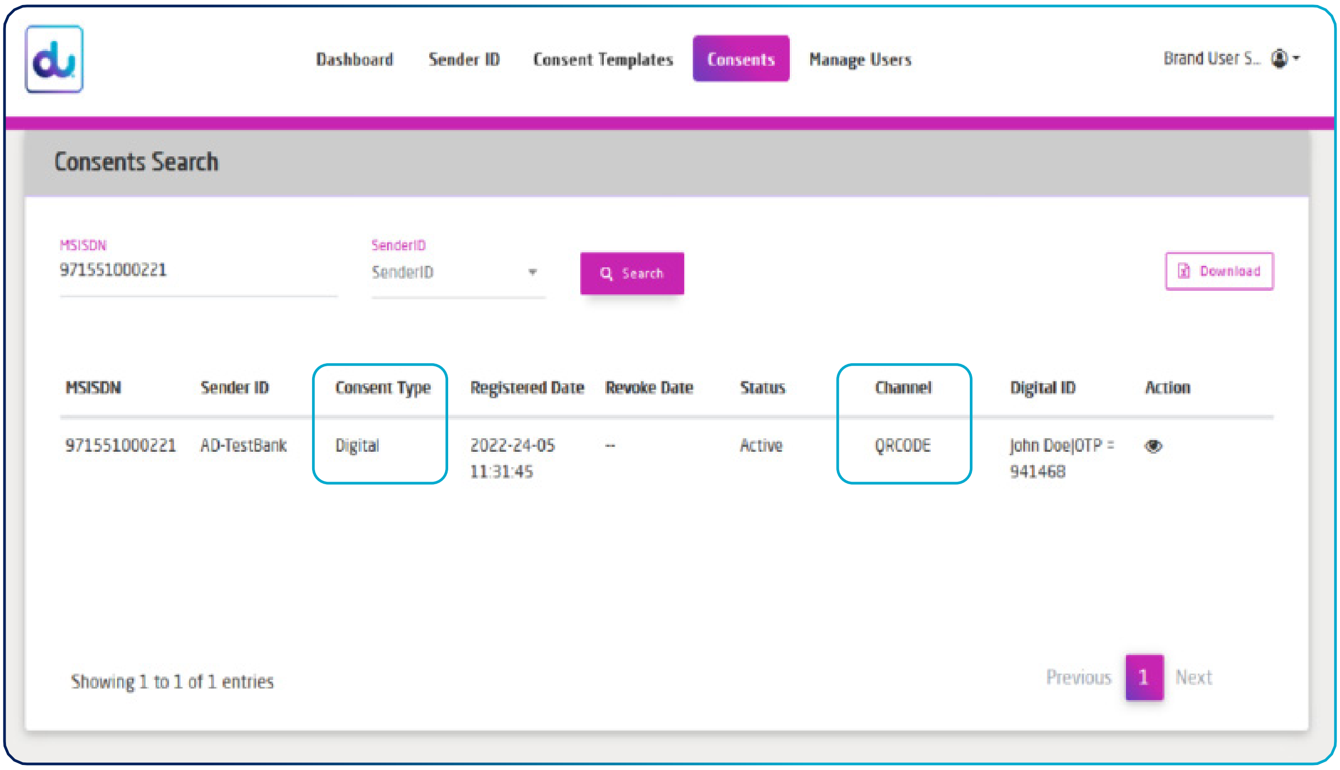
Refer table below for detailed rules:

Column Value	Format	Field Properties
Mobile Number	971xxxxxxxxx	12-digit mobile number with country code starting with 971 only
Date of Consent	YYYY-MM-DD HH:MM:SS	Exact date format to be followed
Digital Channel Type	QRcode	This field explains consent was originally acquired using QRCode. Value can only be "QRCode" and is case insensitive
Channel Value	Template ID Number	QR Code Template ID Max number length is 50 characters with all ascii characters
Digital ID	First Name Last Name | OTP = 123456 value	This field provides first and last name with OTP value captured at the time of QR Code Scanning Max character length is 500 characters with

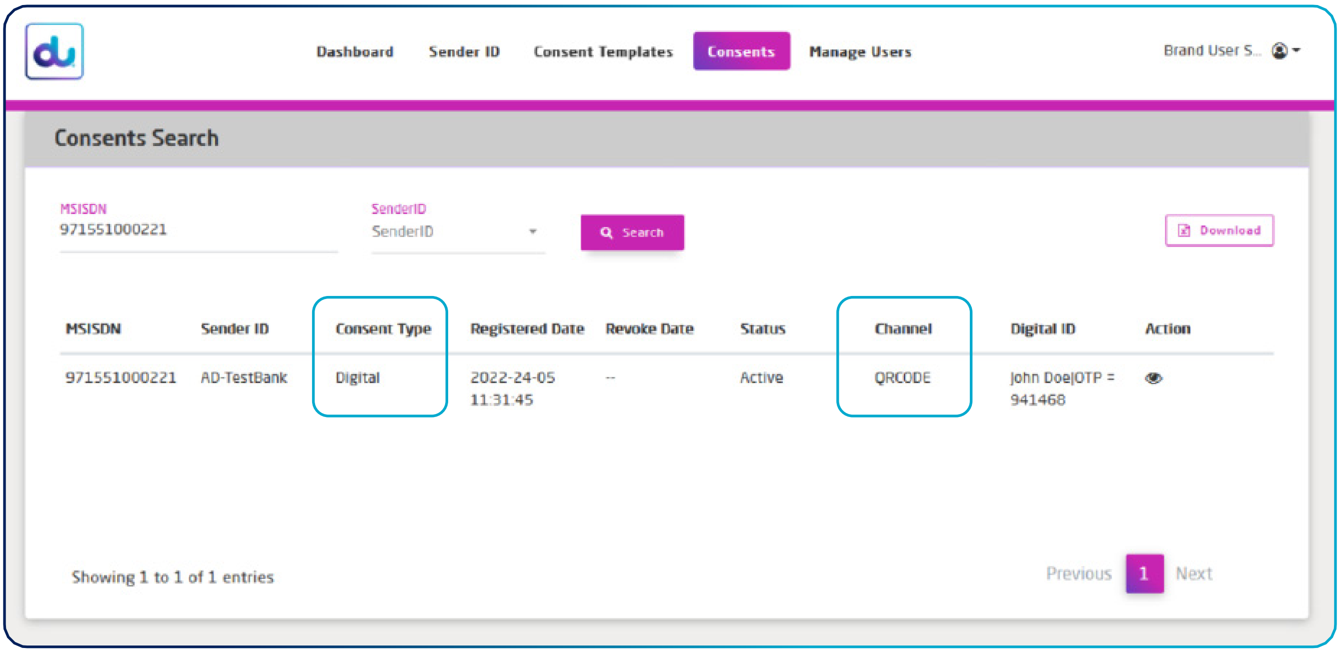
10.1.8 QRCode Consents Uploads by Digital Type

How to differentiate if an upload consent was done directly via QR Code scanning or manual upload via Consent Upload by Digital Type?

In case of QR Code consent data is manually uploaded via Consent Upload by Digital Type, the uploaded consent in the portal will reflect Consent Type: "Digital" while Channel: "QRCODE" as shown below.



In case the uploaded consent was uploaded directly via QR Code Scanning, the uploaded consent in the portal will reflect Consent Type: "QR Code" while Channel: "QRCODE" as shown below.



The different value in Consent Type parameter will differentiate if the consent was uploaded via QR Code scanning or via Consent Upload via Digital Type.

10.2 Consents Revoke

This module allows Users to view information on all Consents Revoke activities done by the User.

Applicable to:

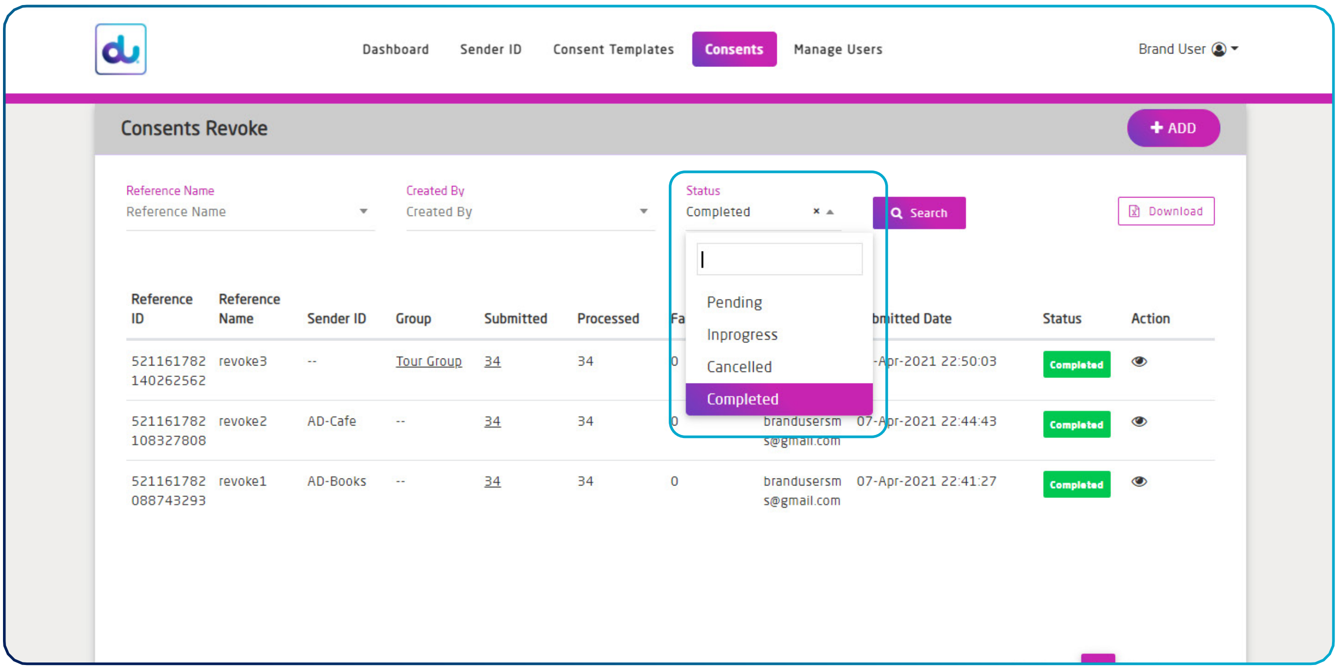
- Admin User
- Normal User
- Reporting User

Module Functionalities:

1. Enables User to filter revoke activity logs by reference name, created by and status filters.
2. Enables User to download the list of Consents Revoke activity logs.
3. Enables User to view the summary results of Consents Revoke activity.
4. Enables User to download the list of MSISDN for any of the Consents Revoke activity.
5. Enables admin and normal Users to create new Consents Revoke activities.
6. Enable User to download the list of tagged Sender IDs under a Group used for the revoke activity.

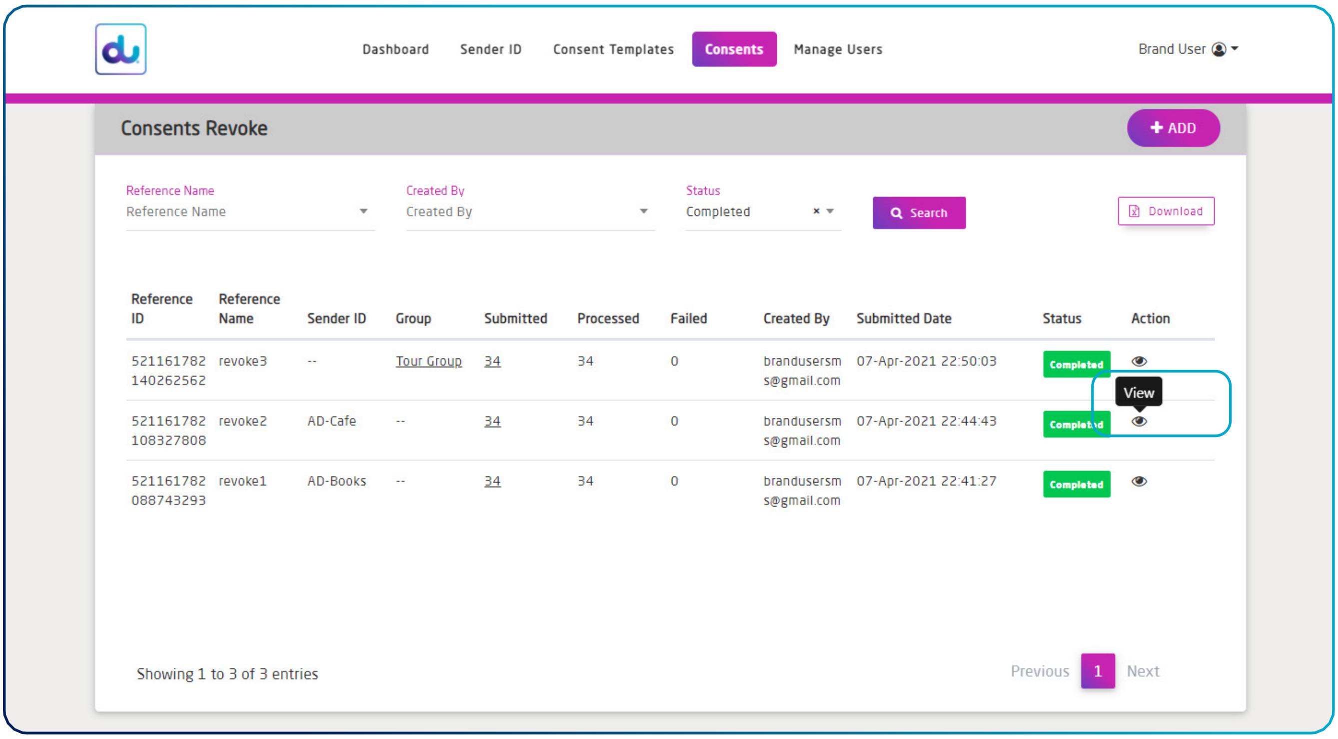
Business Rules:

1. All Users can view details for Consents Revoke activity logs.
2. Admin and Normal Users are only allowed to create new Consents Revoke activities.
3. User will be able to view each request as a separate row.
4. Activity logs of any one status will be show at any one point of time.
5. Activity status: 'Pending' means that Consents Revoke activity has been submitted to the system.
6. Activity status: 'In progress' means that consents are in the process of revoke on the system.
7. Activity status: 'Completed' means that Consents Revoke activity is successfully completed.
8. Activity status: 'Cancelled' means that the revoke activity failed due to system issue.
9. Admin User will receive email notification once the status is completed.
10. User is able to view details of consents by clicking on the "EYE" icon under 'Action' tab.
11. User can download the list of MSISDN's upon clicking on the submitted column hyperlink.
12. User can download the list of Sender IDs tagged to a Group by clicking on the Group column hyperlink.

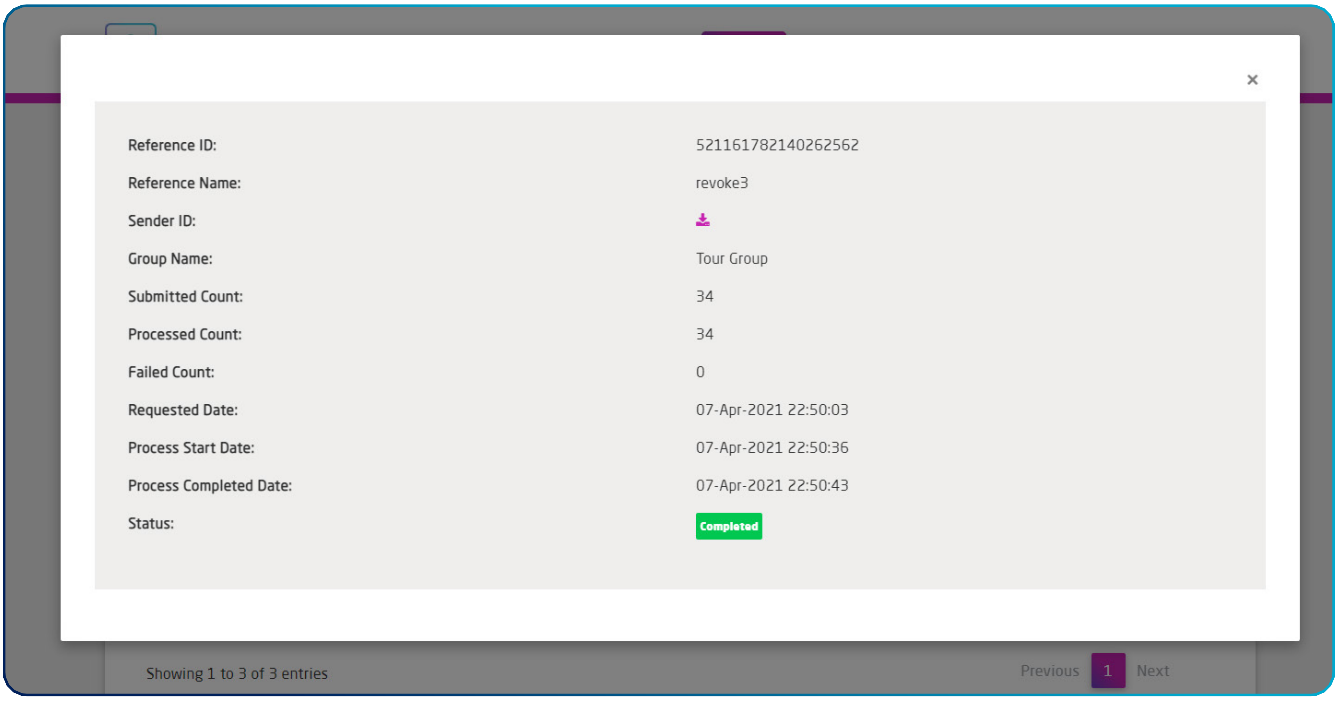


10.2.1 View Consents Revoke Activity

To view the consent revoke activity summary, click on the "Eye" icon under the 'Action' tab.

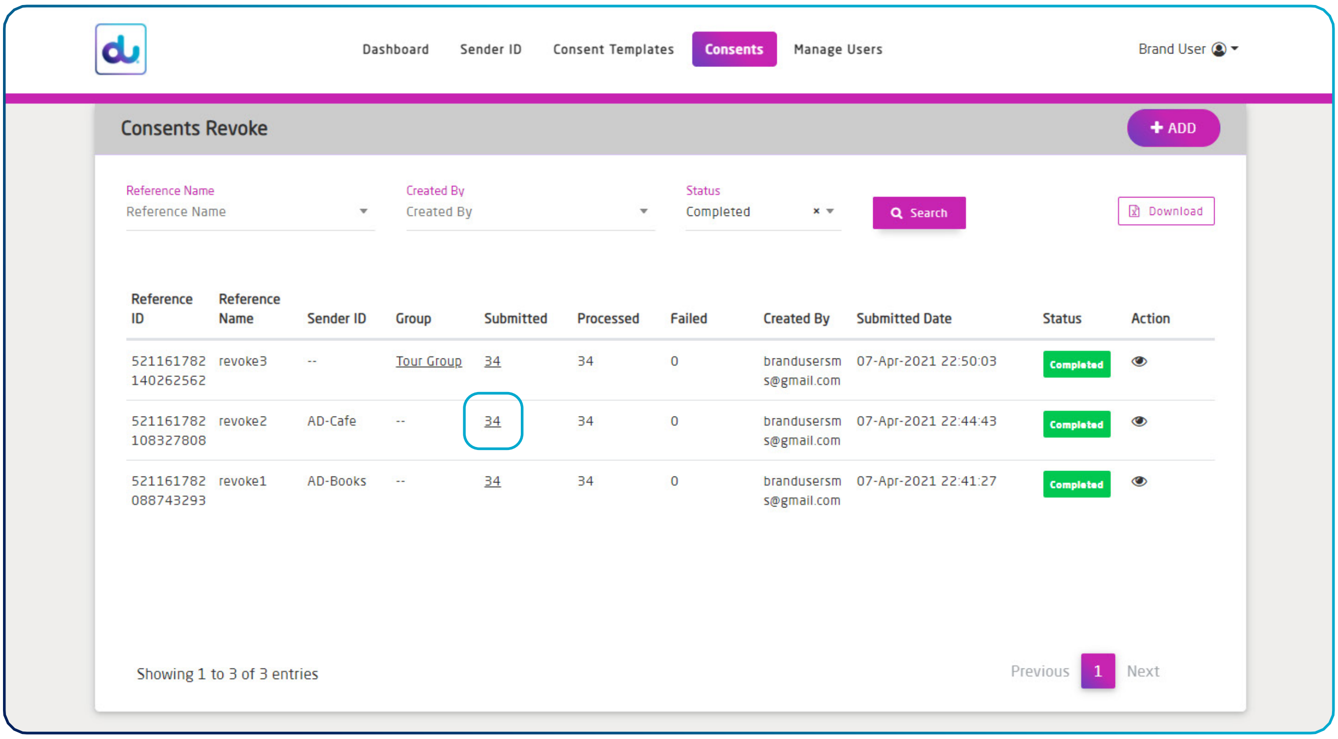


Once the "Eye" icon is clicked, the following summary page is displayed. The User can review the Consents Revoke activity details including the count of total MSISDNs submitted, the total count of MSISDNs processed and the failed count. Also information on the status of the activity and activity start and end time is shown.

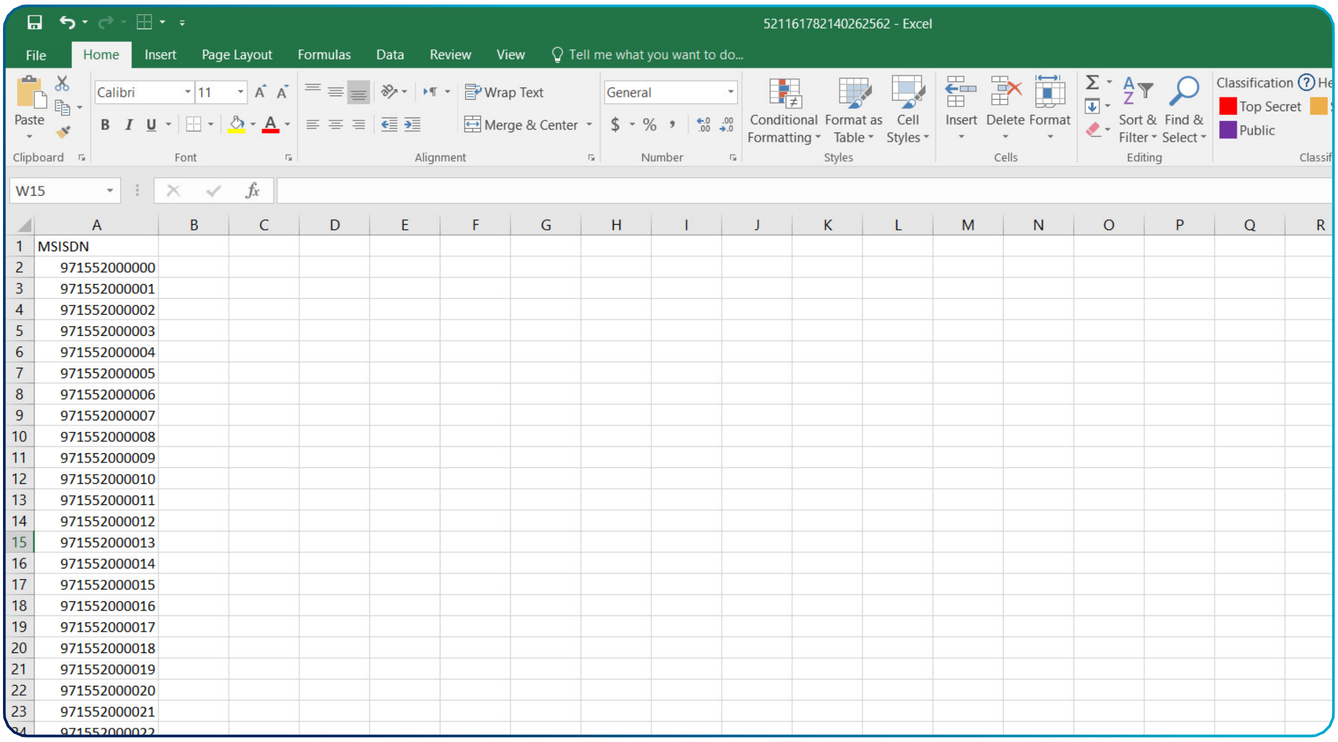


10.2.1 View Consents Revoke Activity

To download the Consents Revoke activity CSV file for each row, the User can click on the on the hyperlink under the 'Submitted' column tab. The CSV will be available as a download file to the User.



Sample downloaded file:



10.2.2 Create Consents Revoke Activity

This module allows admin and normal Users to create new Consents Revoke request by submitting a CSV file against a Sender ID or Group.

Applicable to:

- Admin User
- Normal User

Module Functionalities:

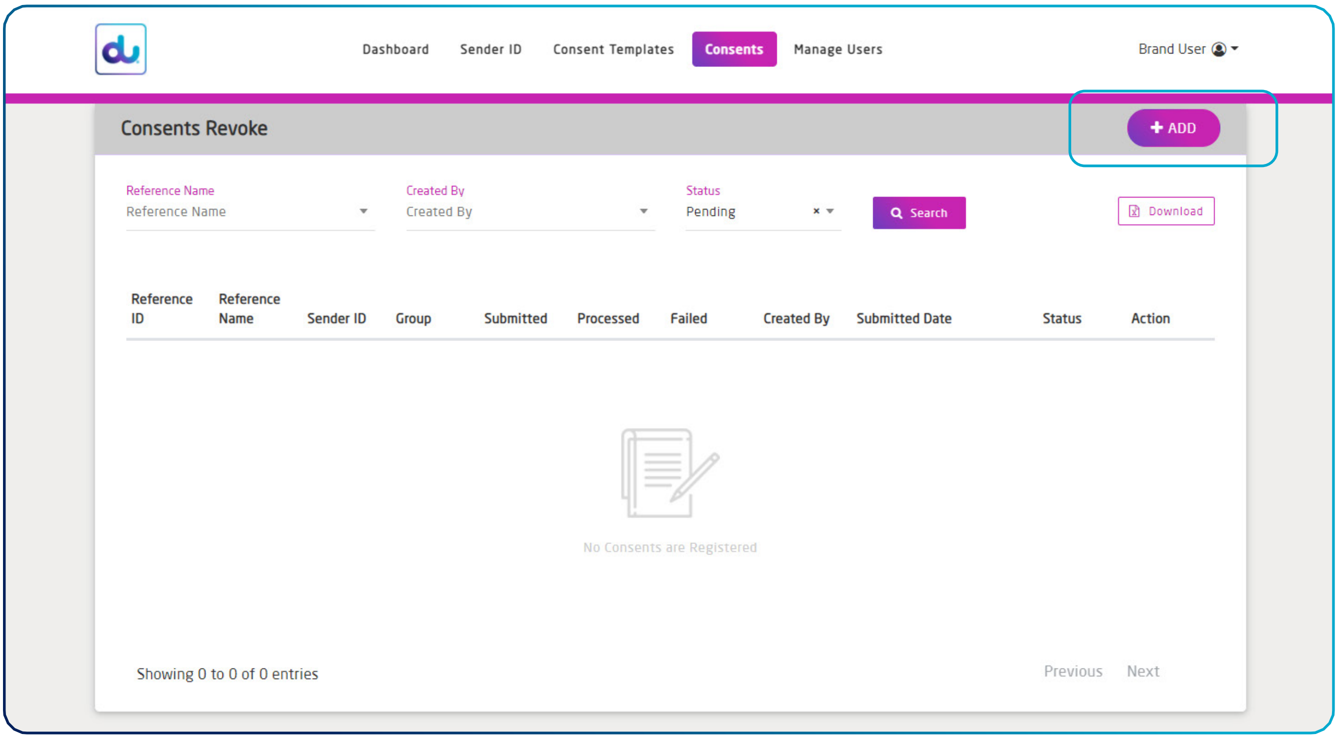
1. Enables User to revoke consents against a Sender ID or Group.
2. Enables User to upload CSV file containing list of MSISDNs.
3. Enables User to download a sample CSV file.

Business Rules:

1. Only Admin and Normal Users can create a Consents Revoke activity.
2. The CSV file can only contain list of MSISDNs starting with "971" with max 12 digit length.
3. The maximum size of CSV file can only be 2 MB.
4. Consents Revoke can only be done for Sender IDs in 'Active' or 'Suspended' states.
5. Admin and Normal User receives an email notification after revoke request is completed.
6. The 'Reference Name' field minimum length of 4 characters and a maximum length of 20 characters.
7. Once a consent is revoked from system, promotional SMS cannot be sent to the mobile subscriber against whom consent has been revoked.

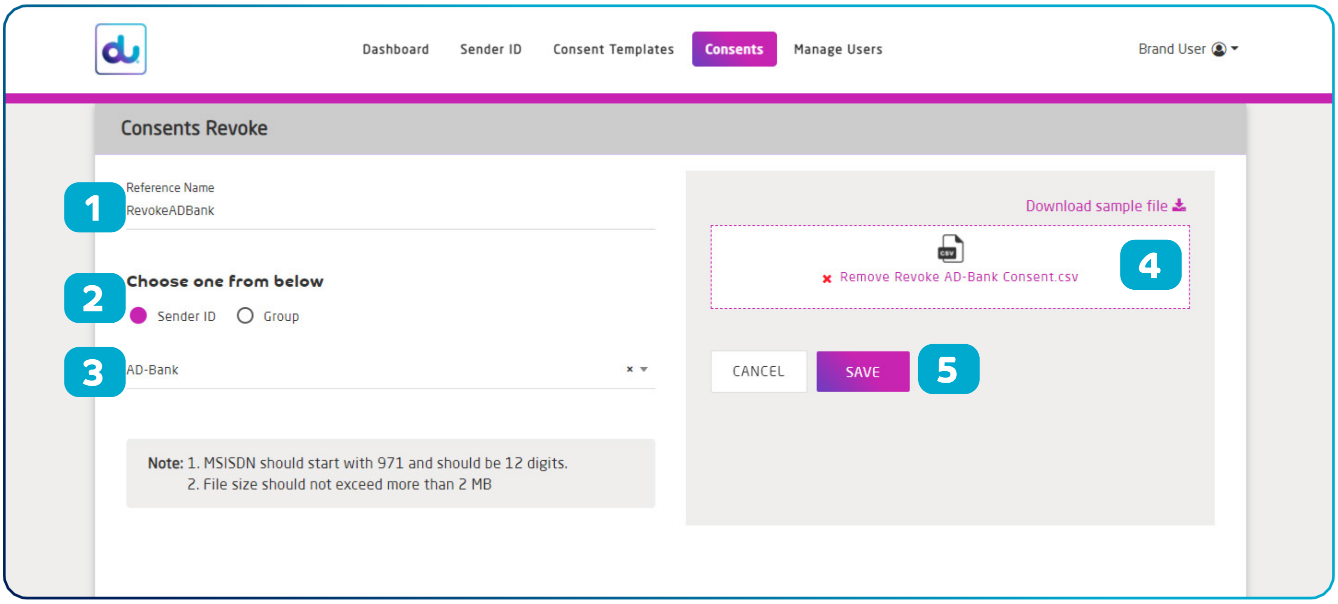
10.2.2 Create Consents Revoke Activity

To create a new Consents Revoke activity, the User will click on "+ADD" button on the Consents Revoke screen.



Once the "+ADD" button is clicked, the User will be directed to the following menu screen. The User will need to perform the following actions to initiate the activity:

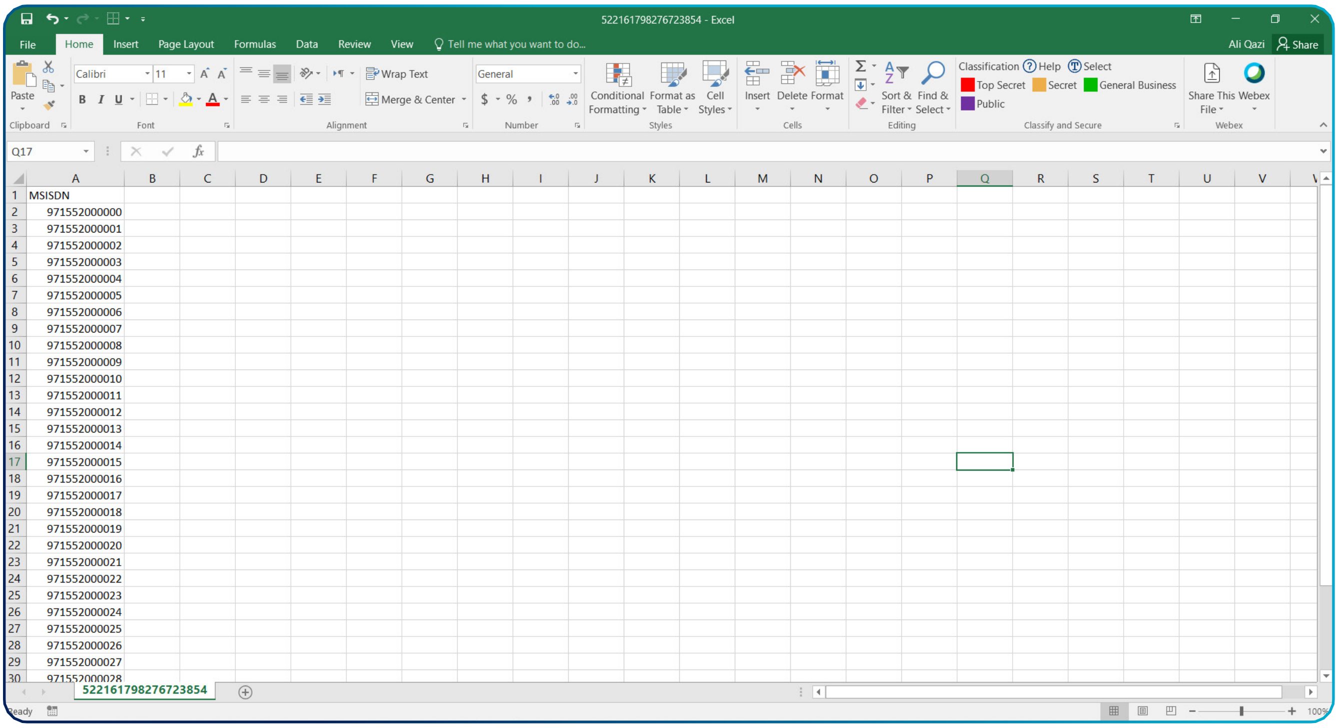
1. Insert a reference name in the 'Reference Name' field
2. Choose Sender ID or Group option against which the consents need to be revoked
3. Select an active Sender ID or Group against which the consent uploads are required
4. Upload the CSV file containing the list of MSISDNs
5. Click "SAVE" button to complete the activity



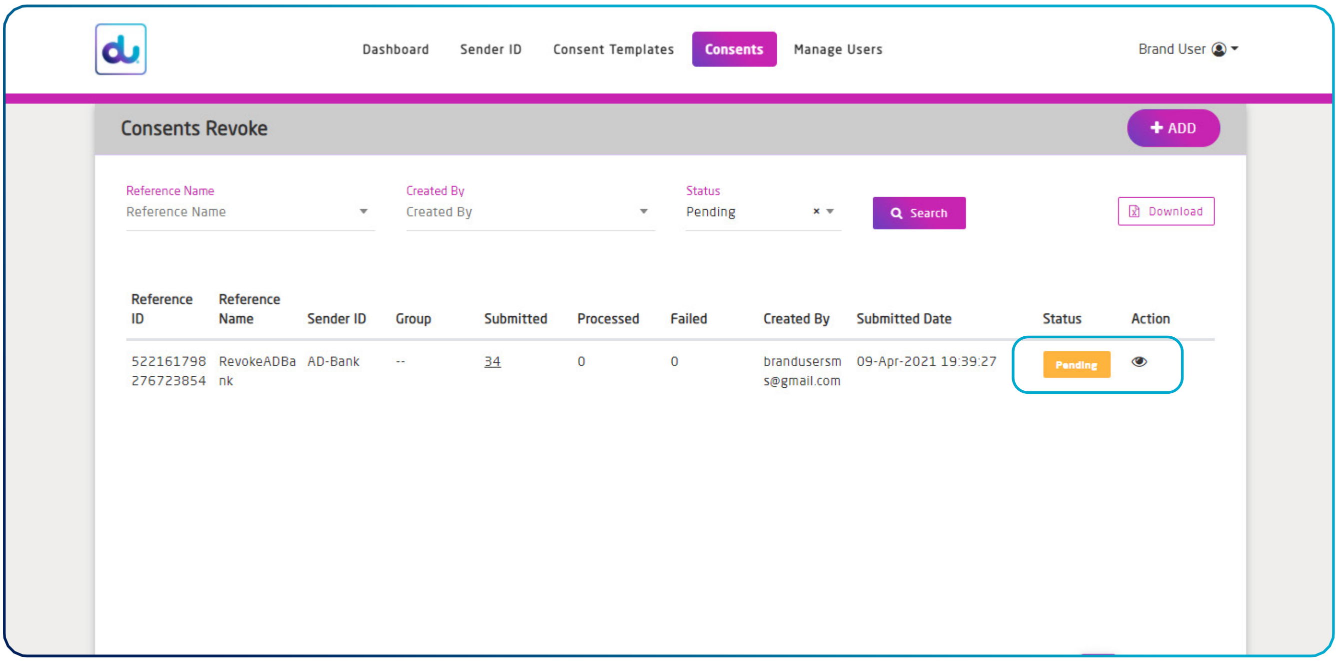
10.2.2 Create Consents Revoke Activity

User must prepare the CSV file given the provided business rules as shown above in the menu screen User can also click “Download sample file” icon in the above screen to download a CSV sample file to fill in the MSISDN list. In case of use of incorrect format, the CSV file will not be uploaded.

Sample Consent Revoke CSV File:



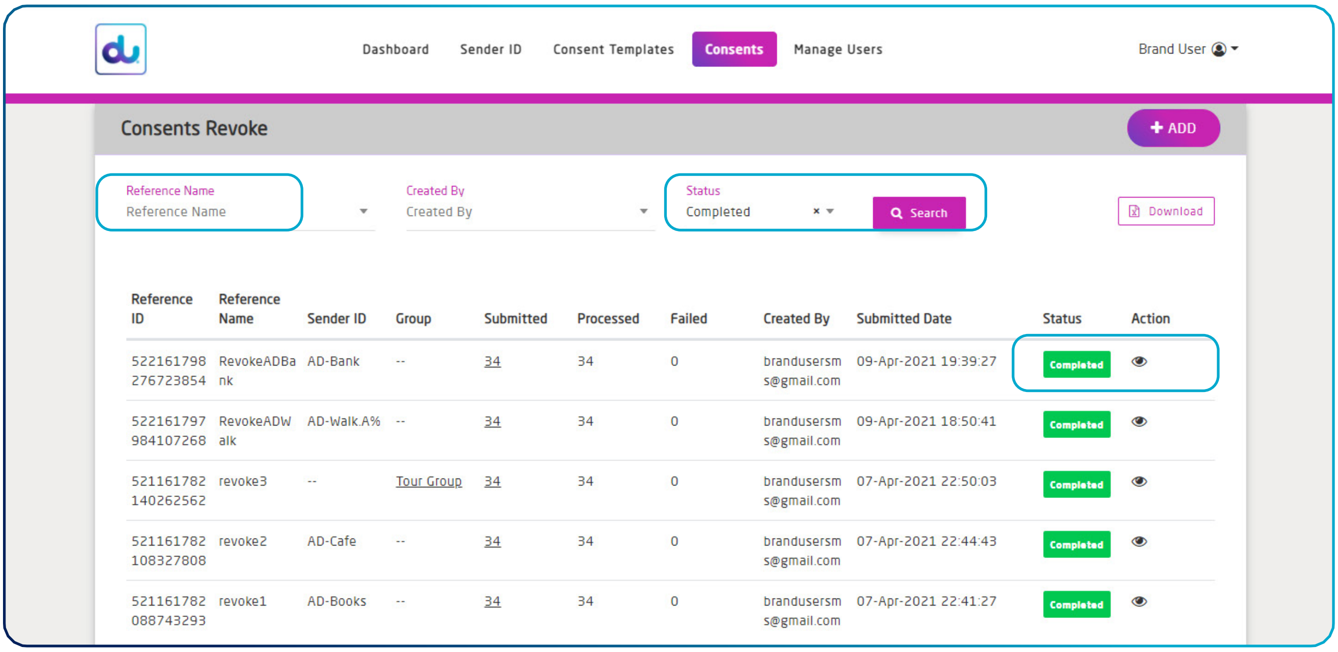
Once User click “SAVE” button and the CSV file has been accepted, the activity will be successfully submitted to the system and the User will be directed to the activity log screen. The status of the revoke activity will appear ‘Pending’ under the ‘Status’ tab.



10.2.2 Create Consents Revoke Activity

Once the revoke activity starts to update to the system, the activity log status will change from 'Pending' to 'In progress' status. One all the consents have been successfully revoked in the system, then the activity log status will be changed to 'Completed' as show below. At any stage User can view the status details by clicking the "Eye" icon under the 'Action' tab.

At any point of time, if the User wishes to see the current status of any activity, the User can insert the activity reference name in the 'Reference Name' field then choose between different statuses and click search to find the updated status as shown below:



11. Search Consent

This module allows the Users to view all the consents and their evidence information stored against a mobile subscriber and a Sender ID.

Applicable to:

- Admin User
- Normal User
- Reporting User

Module Functionalities:

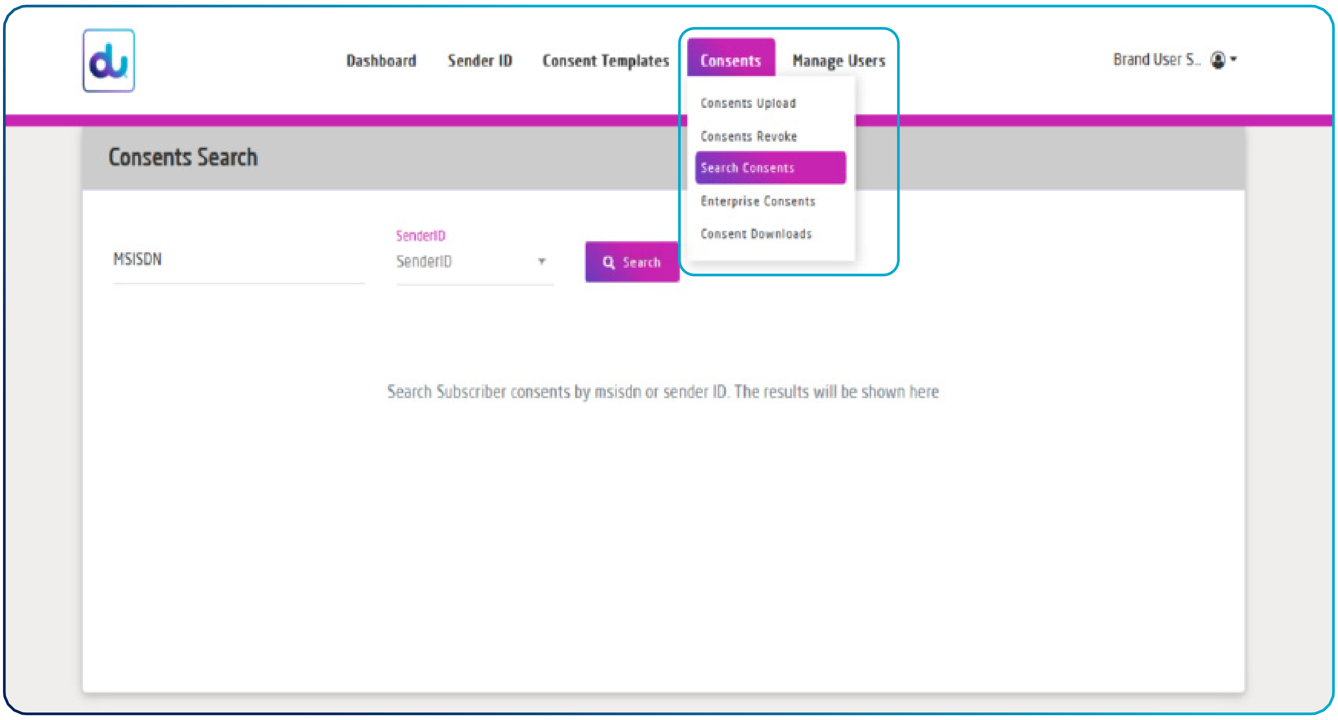
1. Enables User to view consent information and evidence against a mobile subscriber MSISDN and Sender ID.
2. Enables User to download the consent information and associated evidence.
3. User can view all consent details including:
    - MSISDN: (Mobile number of the customer).
    - SENDER ID: (Sender ID the customer has subscribed).
    - CONSENT TYPE: (Digital, Analog or QR Code).
    - REGISTERED DATE: (Date & Time when consent was uploaded on the system).
    - REVOKE DATE: (Date & Time in case the consent was revoked from the system).
    - Status: (If consent is 'Active' or 'Revoked').
    - CHANNEL: ('WEB' or 'APP' or 'QRCODE' value in case of 'Digital' type of consent).
    - DIGITAL ID: (Digital ID provided by the User in the CSV as digital evidence).
    - More information available by clicking "EYE" icon under 'Action' tab:
    - CONSENT ID: (System ID of the stored consent).
    - TEMPLATE ID: (System ID of the Consent Template).
    - TEMPLATE NAME: (Consent Template Name).
    - KEYWORDS: (Keywords stored in the Consent Template).
    - CONSENT DATE & TIME: (Timestamp of the customer subscribing to Sender ID).
    - DIGITAL CHANNEL VALUE: (Name of Channel in case of 'Digital' consent.
    - EVIDENCE FILE: (Scanned document as evidence in case of 'Analog' consent.

Business Rules:

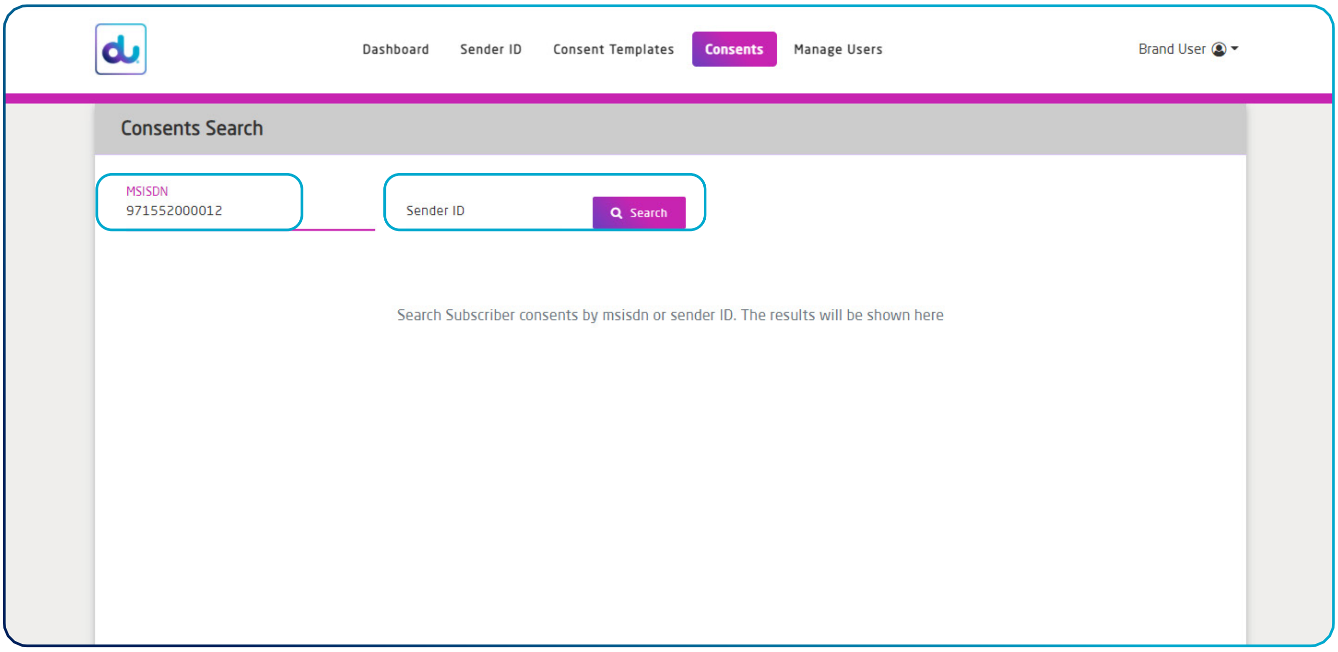
1. All Users are able to view consent information of their customers.
2. Users can search consent information for their customers using their MSISDN and Sender ID.
3. In case consent is of 'Analog' type, then Channel, Digital Channel Value and Digital ID will be blank.
4. In case mobile subscriber consent is of 'Digital' or 'QR Code' type, then Evidence File will be blank.
5. In case mobile subscriber consent is in 'Active' status, then Revoke Date will be blank.
6. In case mobile subscriber Revoke Date is present, then subscriber consent is disabled in the system however all consent related information will still be available for record purposes.
7. In case a consent was revoked and then uploaded again against the same customer, then the search result will return multiple rows for the revoke and re-upload activities.

11. Search Consent

To search consent against any mobile subscriber, the User will click "Search Consent" in the 'Consents' menu on the dashboard page as show below:

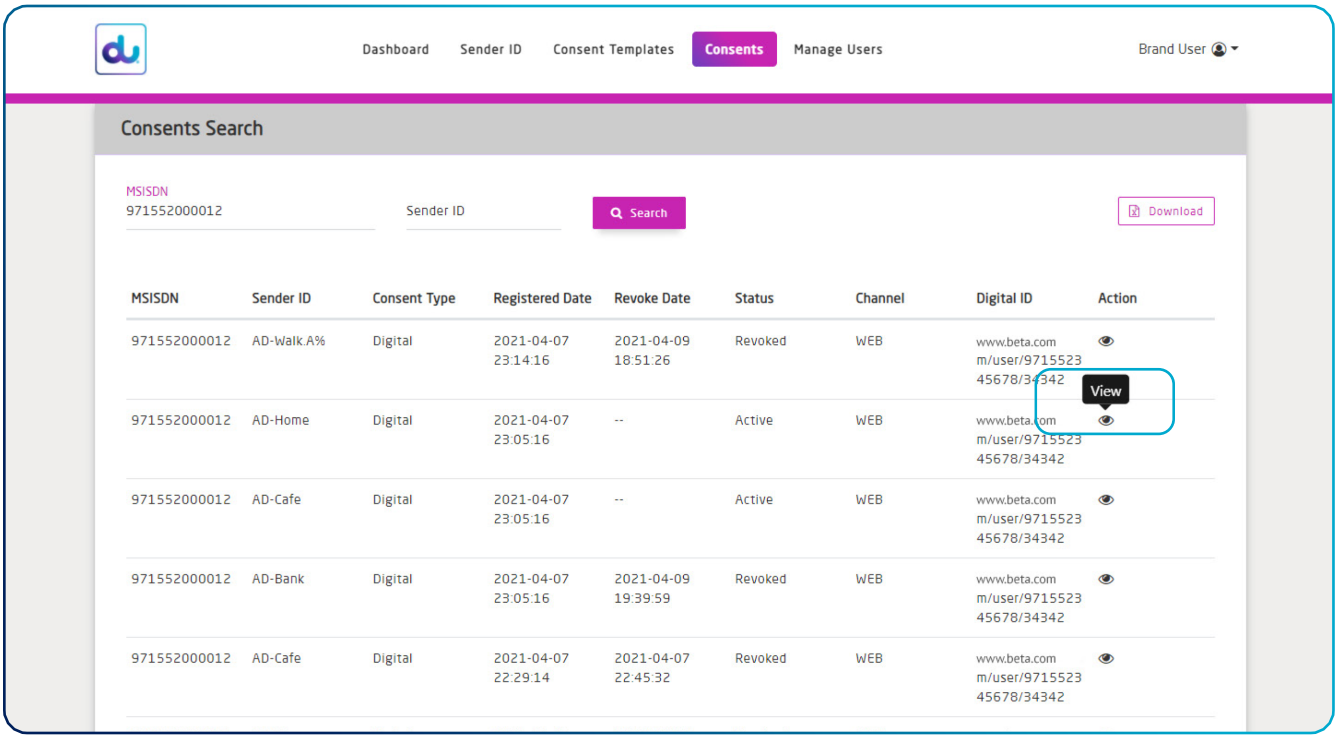


The User can then enter MSISDN or the Sender ID to search for a consent. In case only MSISDN is entered, then the search result will return, consent information against all Sender IDs that a User has subscribed to. In case the search is limited to a particular Sender ID, then the User can enter MSISDN and Sender ID together to return consent information only for the specific Sender ID.



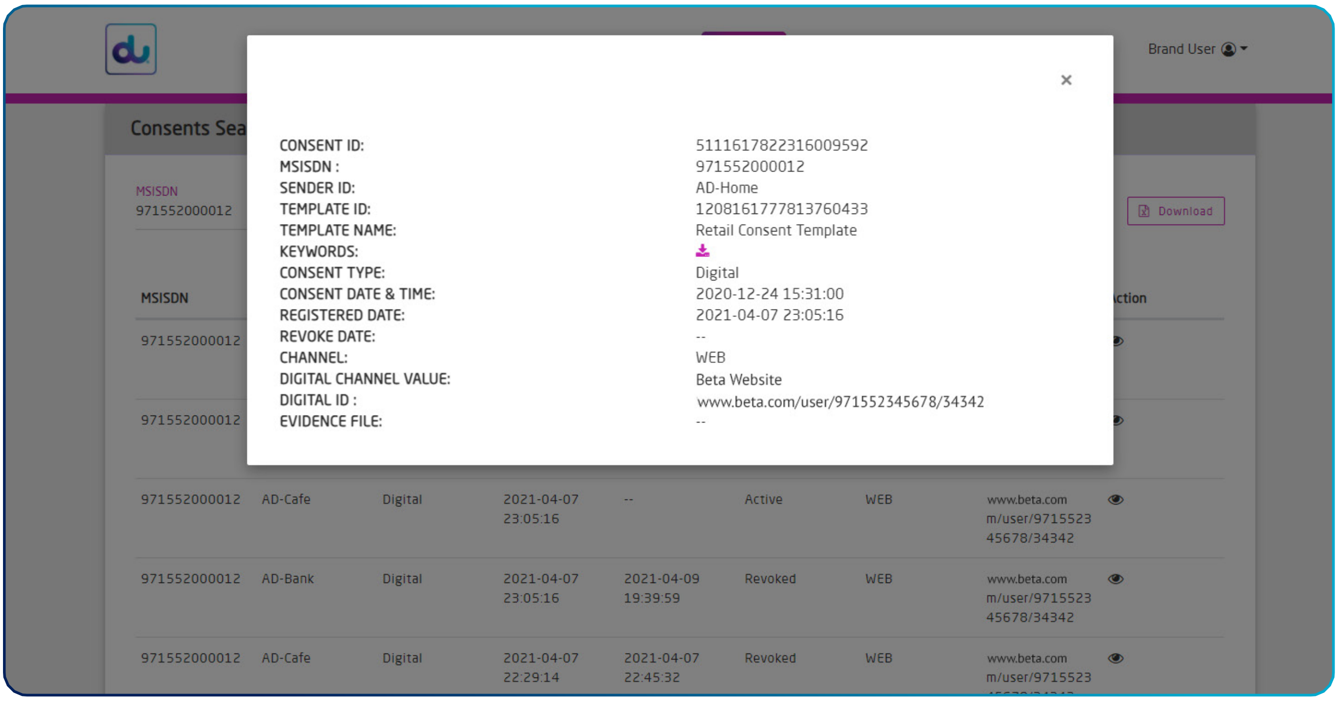
11. Search Consent

Once a User clicks "Search", the user will be able to review all consent records against the mobile subscriber.



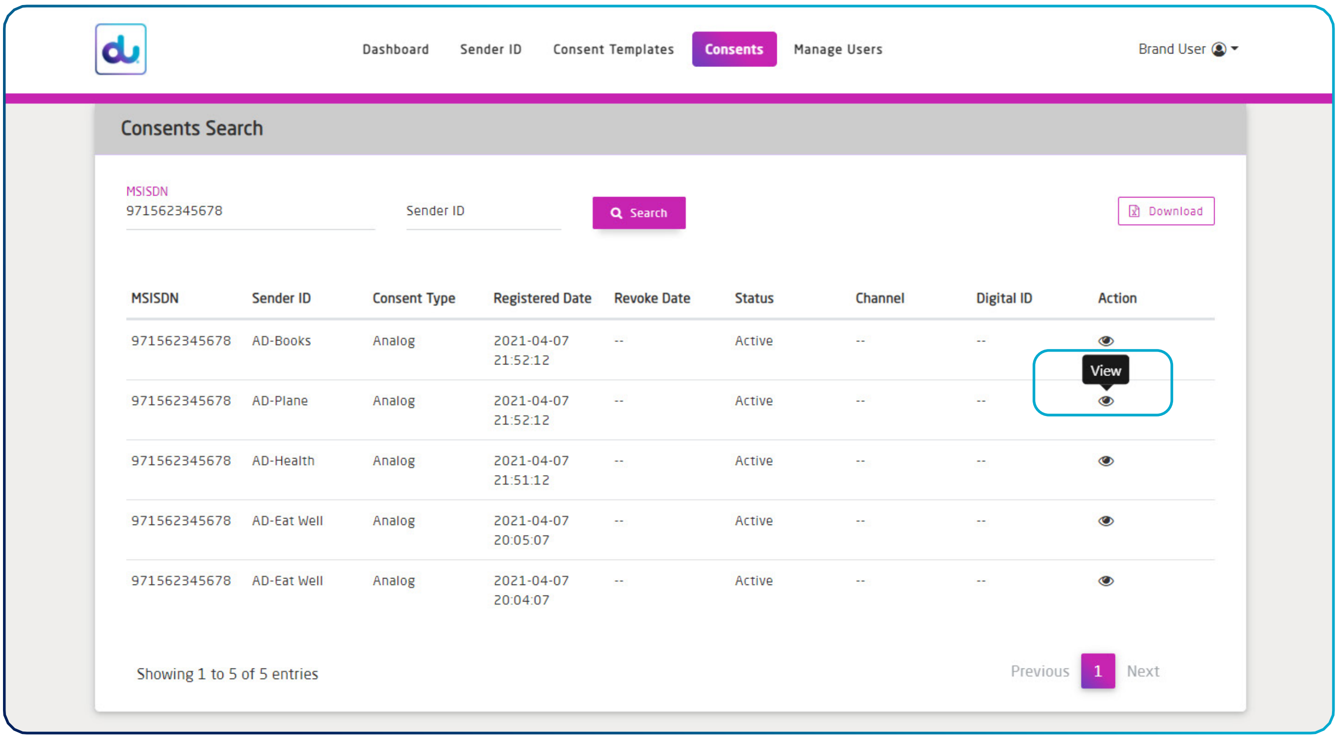
By clicking the "EYE" icon under the 'Action' tab, the customer can view more information and will be able to down to the "Keywords" and the scanned document evidence in case of 'Analog' consent.

Note: Below sample is for a 'Digital' consent type with consent status as 'Active'. The 'Evidence File' and Revoke date is blank.

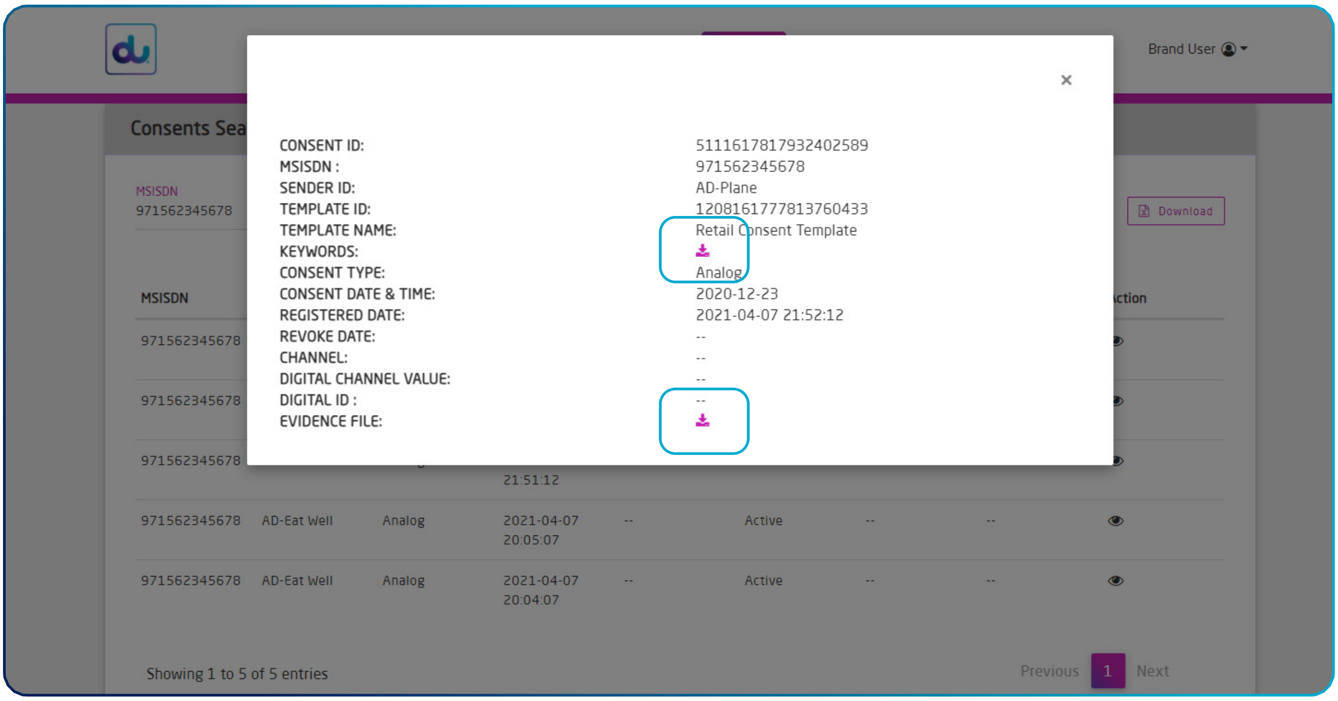


11. Search Consent

Below is a sample of 'Analog' consent type with consent status as 'Active'. To view more information and download scanned document, the User can click on the "EYE" icon under the 'Action' tab.



The User can download the list of 'Keywords' and the scanned document by clicking on the download link as shown in the below screen.



12. Enterprise Consents

This module allows Users to view the summary count of total active consents against any Sender ID in the system. The module provides separate count of 'Analog' and 'Digital' consents against the respective Sender IDs.

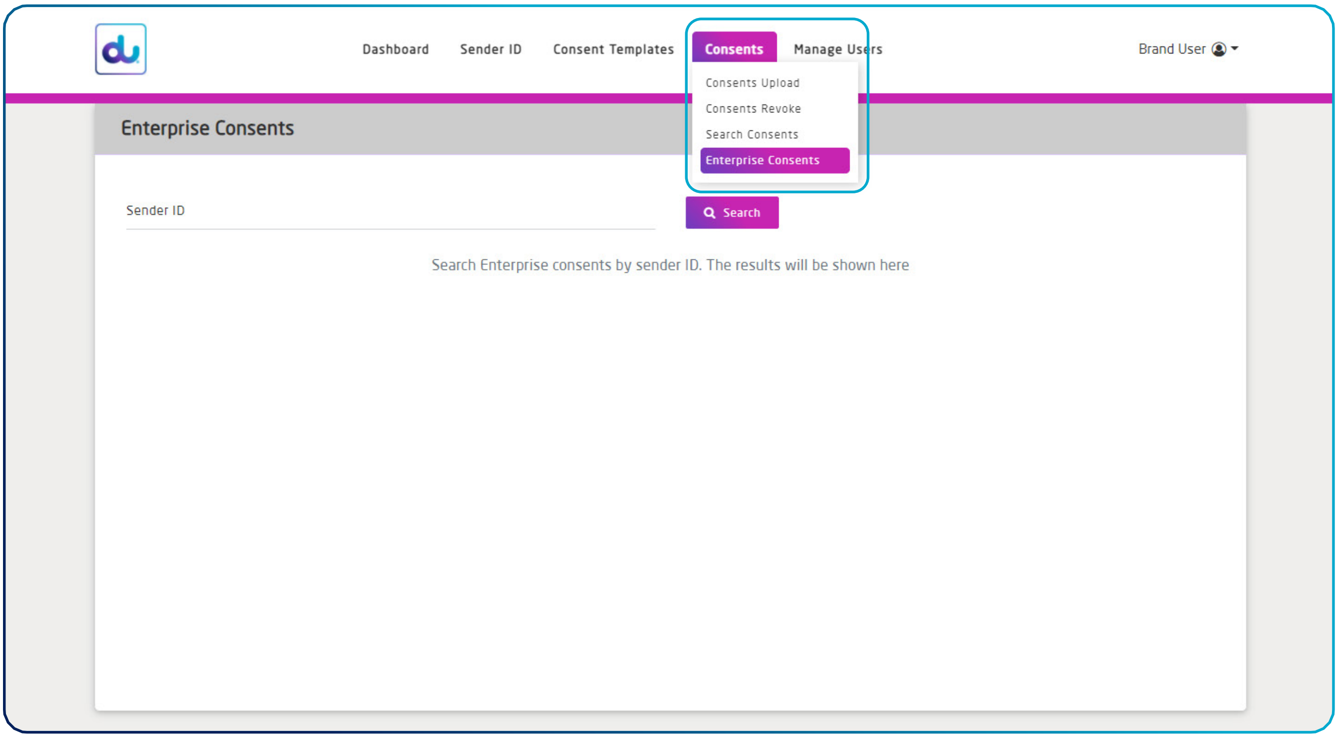
Applicable to:

- Admin User
- Normal User
- Reporting User

Module Functionalities:

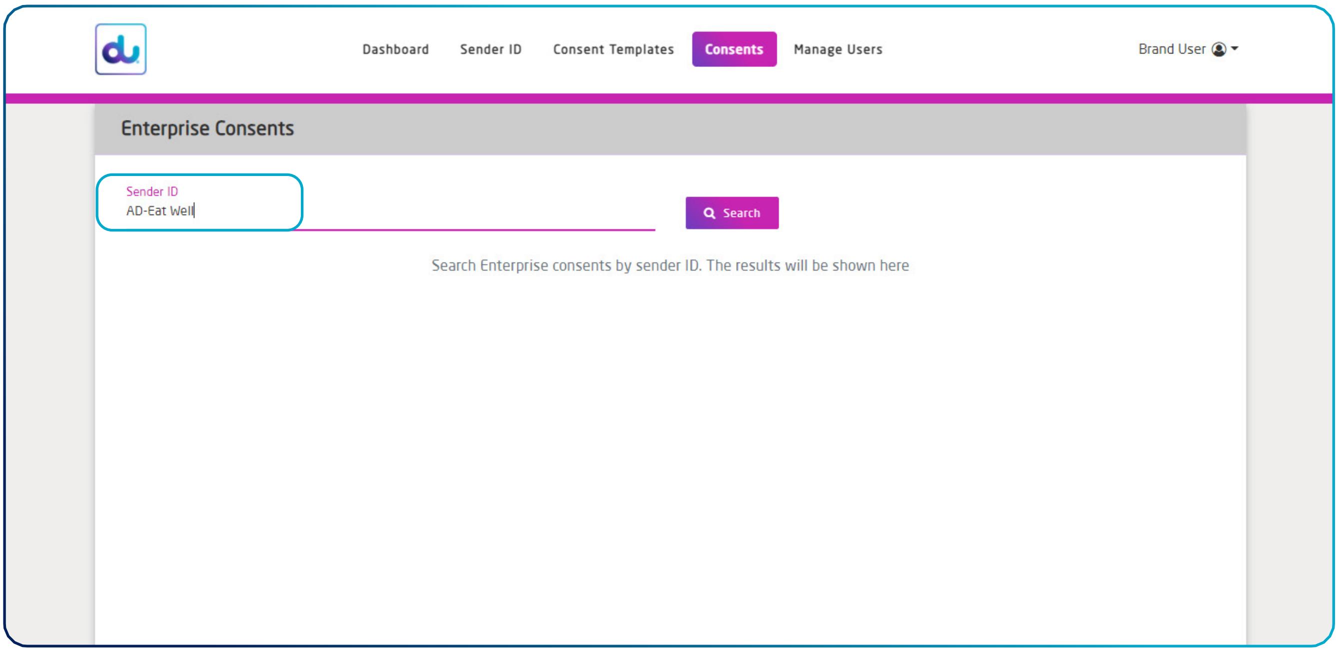
1. Enables User to search 'Active' status consent counts against a Sender ID
2. Enables User to download the count of 'Analog' and 'Digital' consents for the respective Sender ID
3. Consent Type: 'QR Code' and Consent Type: 'Digital' consents are collectively shown under 'Digital' consents in the report. In case of consents uploaded in the system via API, they will also reflect collectively under 'Digital' consents

To search the consent count details against any Sender ID, the User will click "Enterprise Consents" under the 'Consents' menu on the dashboard page as show below:

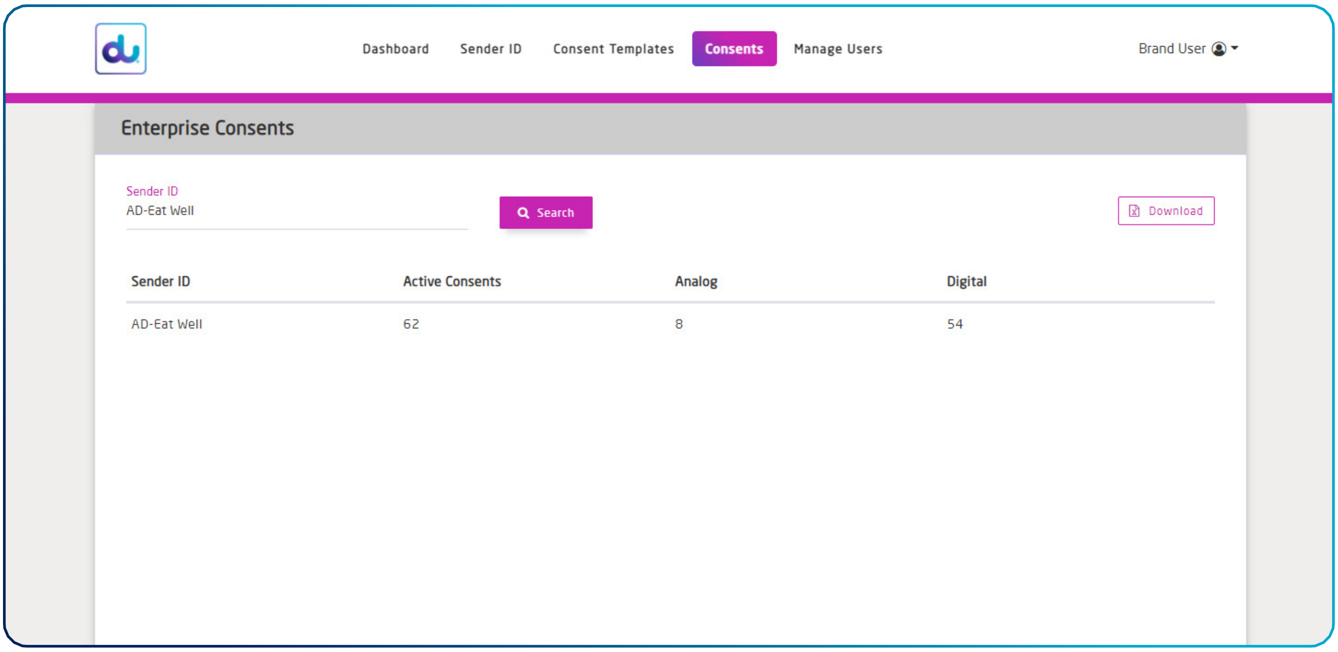


12. Enterprise Consents

The User can enter the specific Sender ID in the search box and click "Search" to get summary count details.



Once the User clicks "Search", the summary count of consents only in 'Active' status against the specific Sender ID will be shown as below: User can click the "Download" button to download details.



13. Consents Downloads

This module allows the Users to download consent information for active consents stored against a mobile subscriber and a Sender ID.

Applicable to:

- Admin User
- Normal User

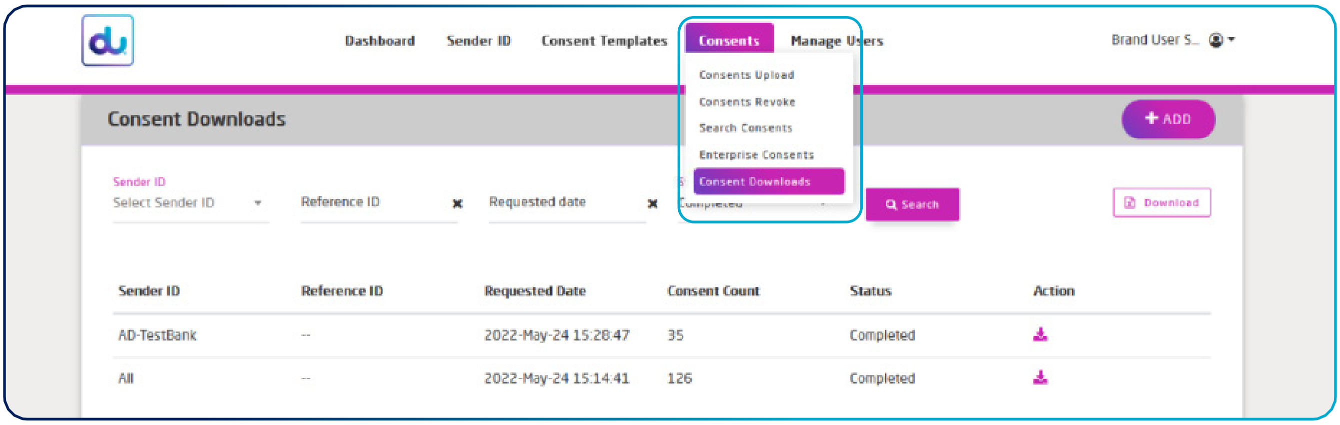
Module Functionalities:

1. Enables User to generate a consent information download report against mobile subscriber MSISDN and Sender IDs based on a single Sender ID selection, all Sender IDs or against any particular Consent Upload activity.
2. Enables User to re-download the consent download reports generated in the past 24 hours.
3. Details included in the download file will be:
   - MSISDN: (Mobile number of the customer).
   - ACQUISITION DATE & TIME: (Timestamp of the customer subscribing to Sender ID).
   - REGISTERATION DATE: (Date & Time when consent was uploaded on the system).
   - TEMPLATE NAME: (Consent Template Name).
   - CONSENT TYPE: (Digital, Analog or QR Code type).
   - SENDER ID: (Sender ID the customer has subscribed).
   - CHANNEL TYPE: ('WEB' or 'APP' or 'QRCODE' value in case of 'Digital' type of consent).
   - DIGITAL CHANNEL VALUE: (Name of Channel provided by the User in the CSV in case of 'Digital' type of consent or QR Code Template ID in case of 'QR Code' consent type).
   - DIGITAL ID: (Digital ID provided by the User in the CSV as digital evidence or First & Last Name with OTP Value in case of QR Code consent).

Business Rules:

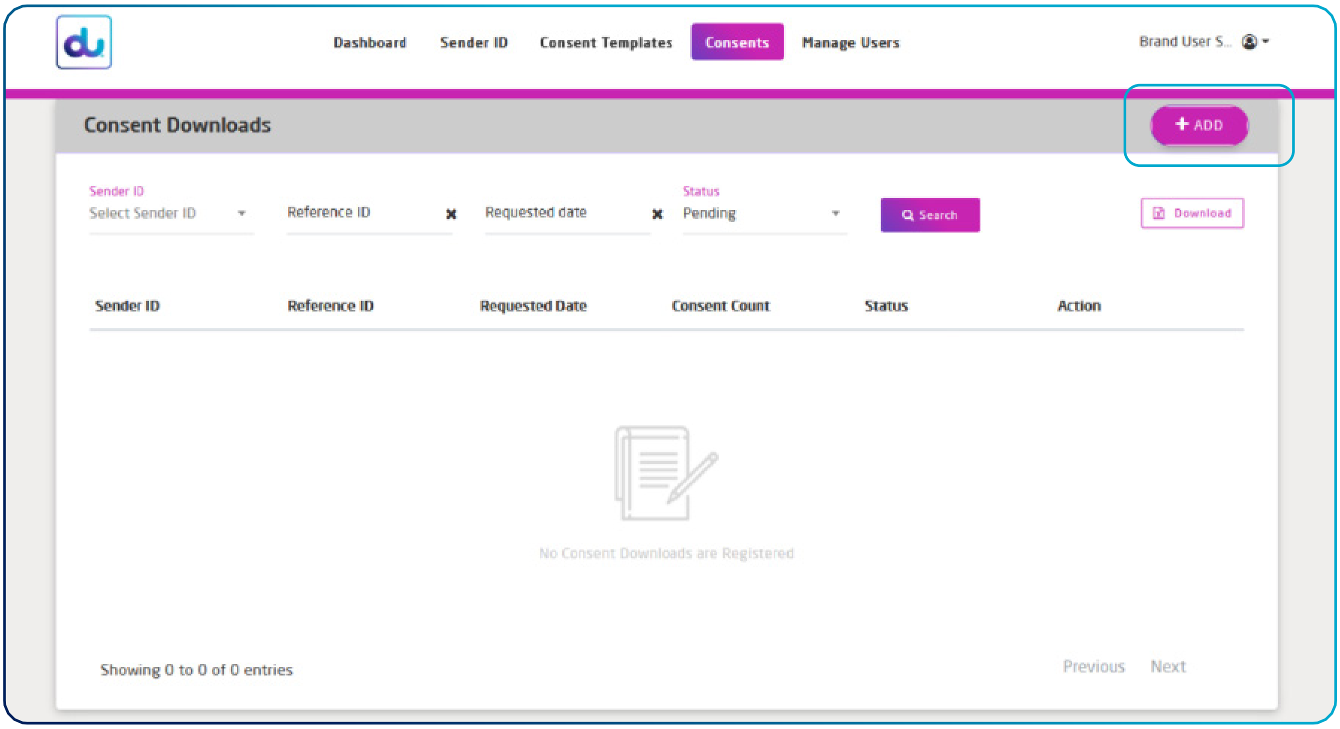
1. Only Admin and Normal Users are able to download consent information report.
2. Users can download consent information using a particular Sender ID or All (keyword used when download is for all sender IDs) or Reference ID generated by a Consent Upload activity.
3. In case consent is of 'Analog' type, then Channel Type, Channel Value and Digital ID will be blank.
4. Consent information for only active consents will be downloaded.
5. Downloaded reports will only be available for 24 hours after which the row will be removed and User will have to reinitiate a new download request.

To download the consent information report against any or all Sender IDs, the User will click "Consents Download" under the 'Consents' menu on the dashboard page as show below:

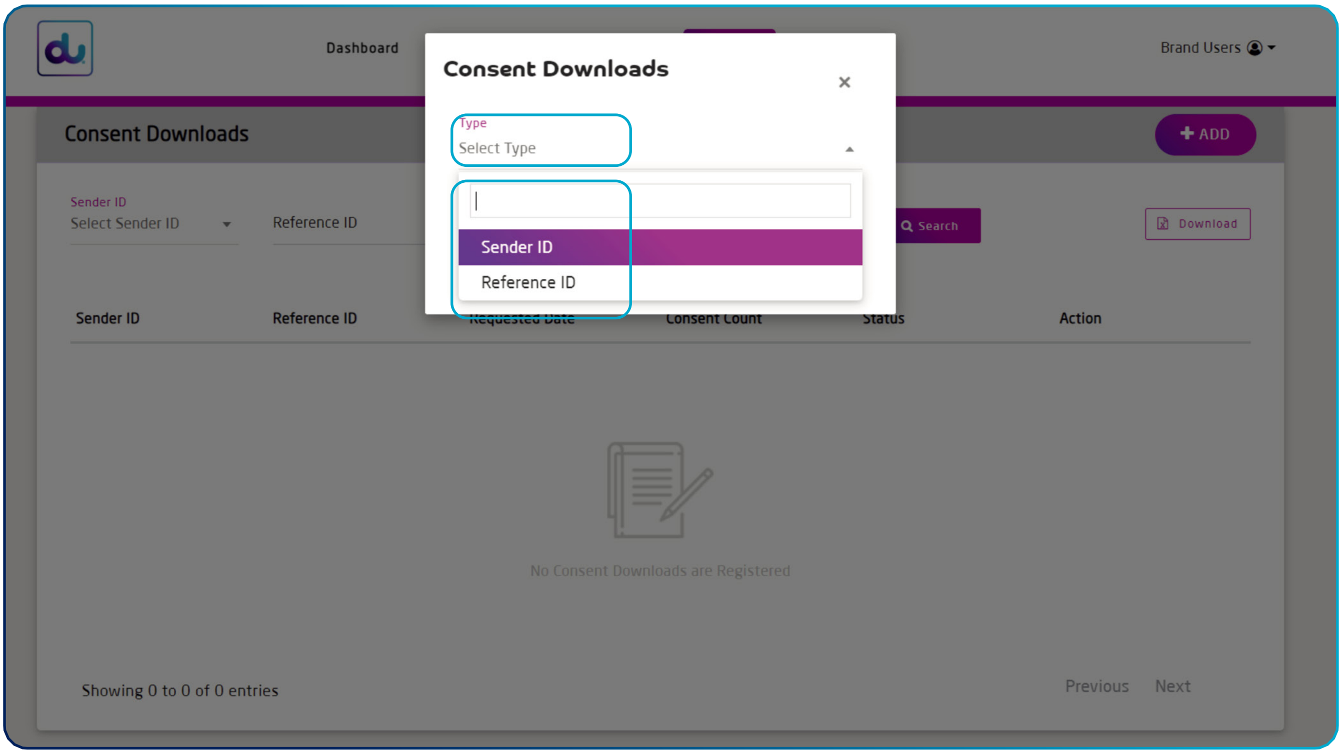


13. Consents Downloads

In order to download consent report, User will click the "+ADD" button on the 'Consent Downloads' page as shown below:



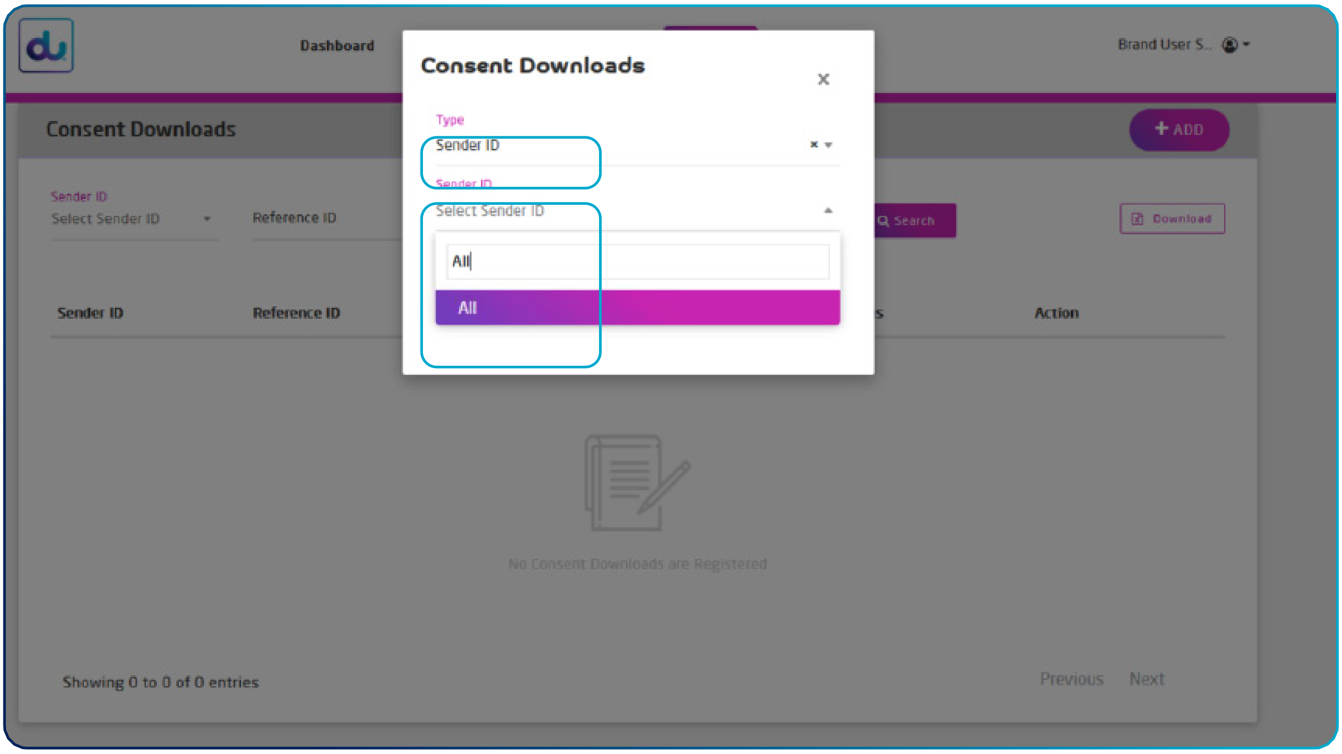
Once the "+ADD" button is clicked, a Consent Downloads pop-up box will appear on the screen. User will select "Select Type" under the 'Type' drop down box. User can download a report by selecting either a Sender ID selection or Reference ID selection.



13. Consents Downloads

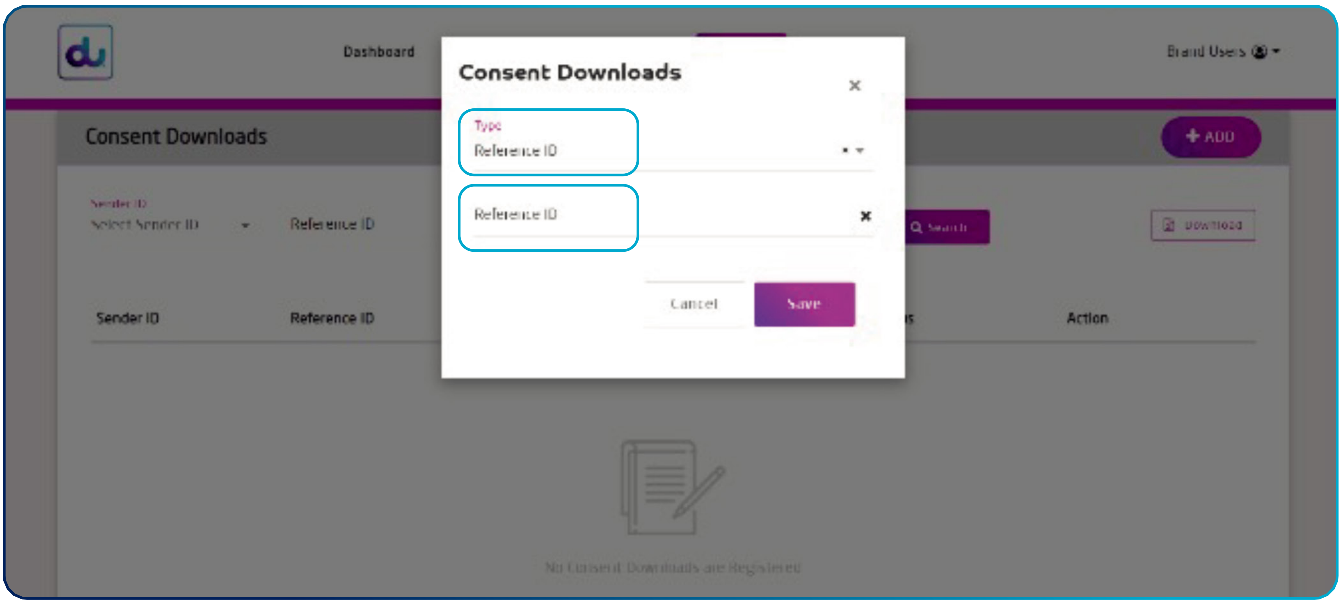
Consent Downloads by Type: Sender ID

In case User selected Type: Sender ID, User can then input any particular Sender ID in the 'Sender ID' text box to download data for the particular Sender ID or input value "All" as shown below to download data for all Sender IDs.



Consent Downloads by Type: Reference ID

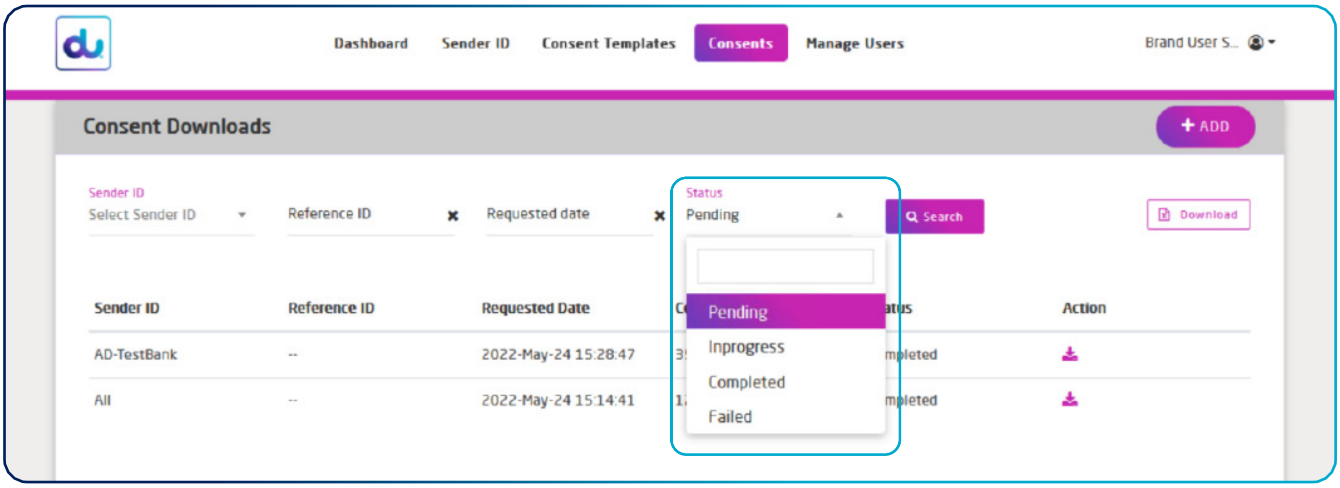
In case User selected Type: Reference ID, User can then input Reference ID in the 'Reference ID' text box to download data for the particular Reference ID as shown below to download data for all Sender IDs. Each Consent Upload activity generates a Reference ID upon completion which can be viewed under the "Consent Upload" page by clicking the 'Eye' icon. Refer to section 10.1 .1 View Consents Upload Activity section for details.



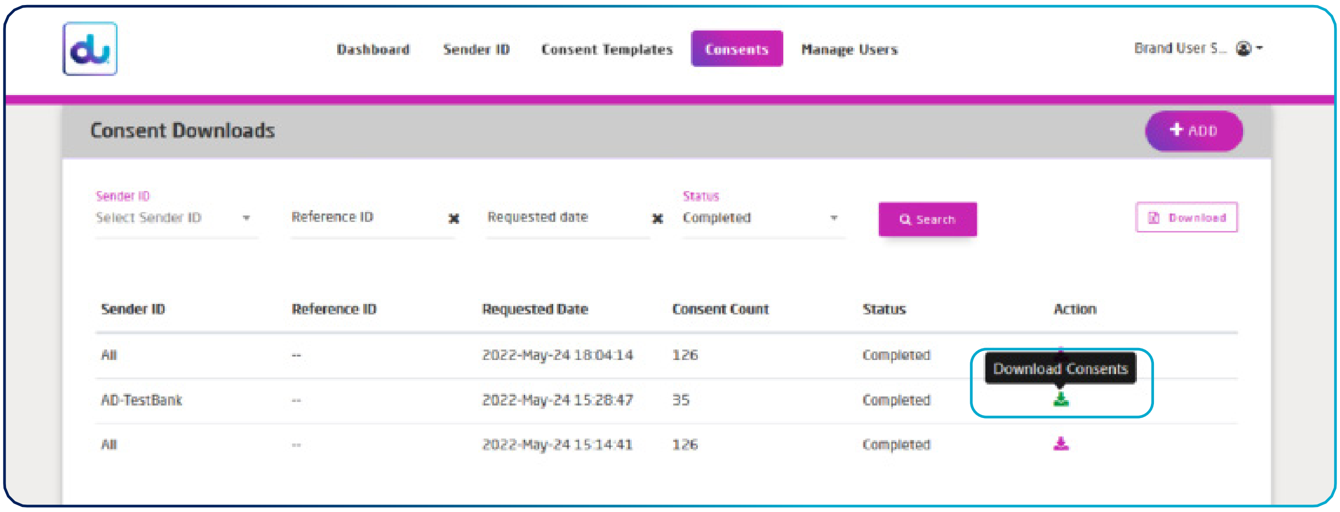
13. Consents Downloads

Once a 'Consent Downloads' activity has been created, User will be able to view each request as a separate row. Activity logs of any one status will be shown at any one point of time.

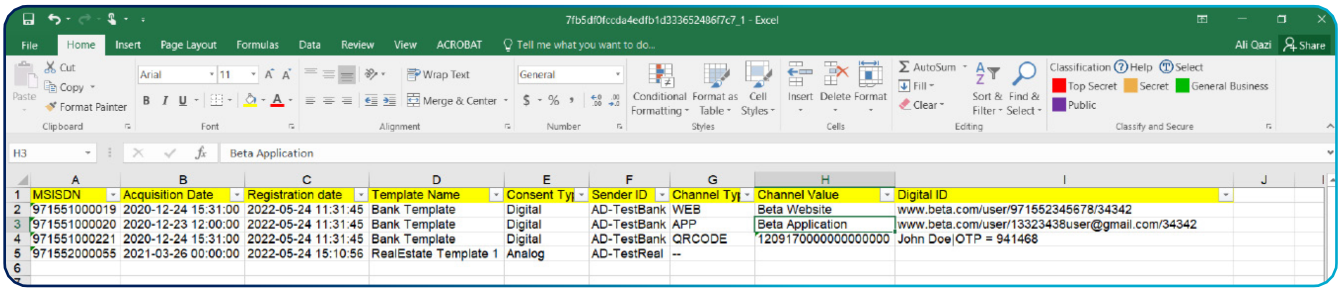
1. Activity status: 'Pending' means that activity has been submitted to the system.
2. Activity status: 'In progress' means that consent download is being processed on the system.
3. Activity status: 'Completed' means that consent download activity is successfully completed and report can be downloaded
4. Activity status: 'Failed' means that the activity failed due to system issue.



Once a download activity is completed, User can click the "Download Icon" under the 'Action' tab to download the file as shown below.



The downloaded file will be exported in ZIP format. User can extract the excel file from the ZIP format. Following is a sample of excel file containing consent information from the download report.



14. Manage Users

This module allows Admin User to perform User Management activities on all the Active/Inactive/Pending/ Deleted Users.

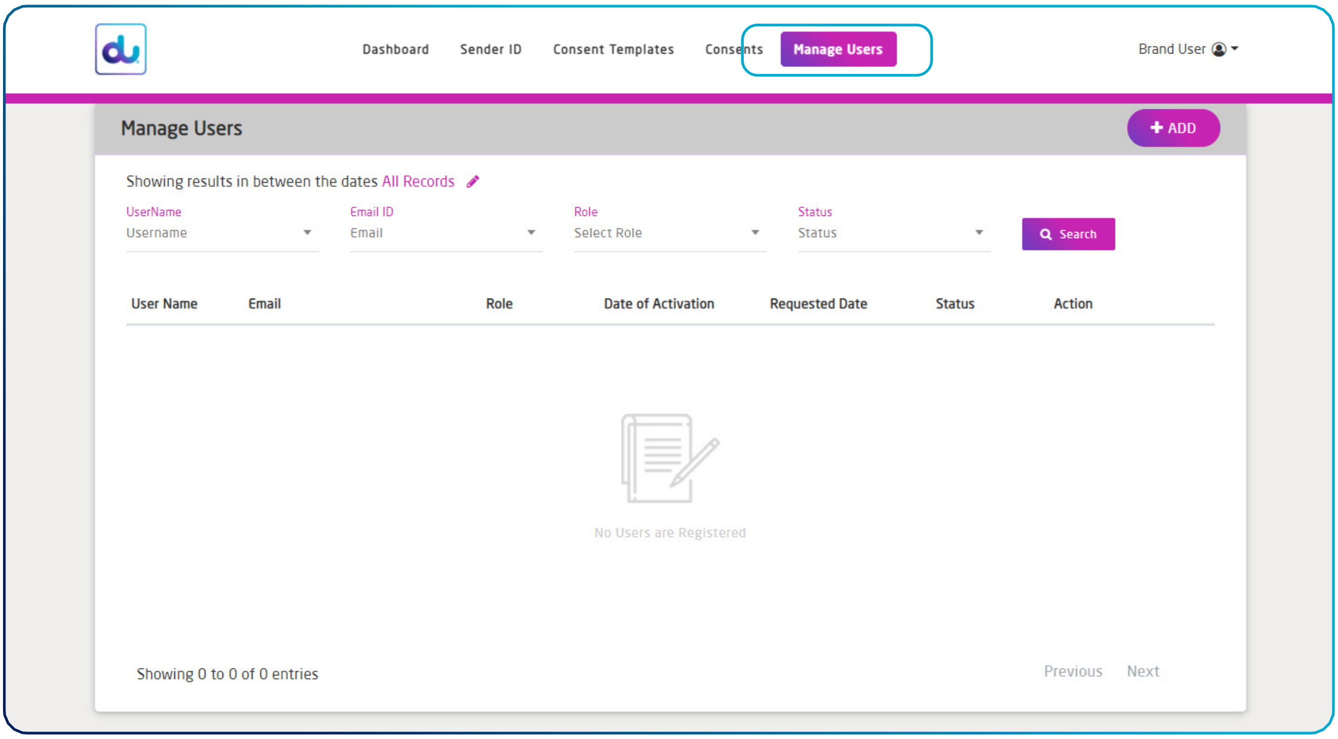
Applicable to:

- Admin User

Module Functionalities:

1. Enables Admin User to create/delete/suspend new Normal, Reporting or API users.
2. Enables Admin User to resend the activation link for Users in 'Pending' state.
3. Enables Admin User to search for any user based on Username, Email address, User role or status.
4. Enables Admin User to provide deleting reason in confirmation popup screen upon deleting a user.
5. Enables Admin User to refresh existing API user password and update API user Email Address

To manage Users, the Admin User will click "Manage Users" tab in on the main dashboard page as show below. The User will be taken to the 'Manage Users' page as show below:



14.1 Adding a new User

This module allows Admin User to create new Normal, Reporting or API user.

Applicable to:

- Admin User

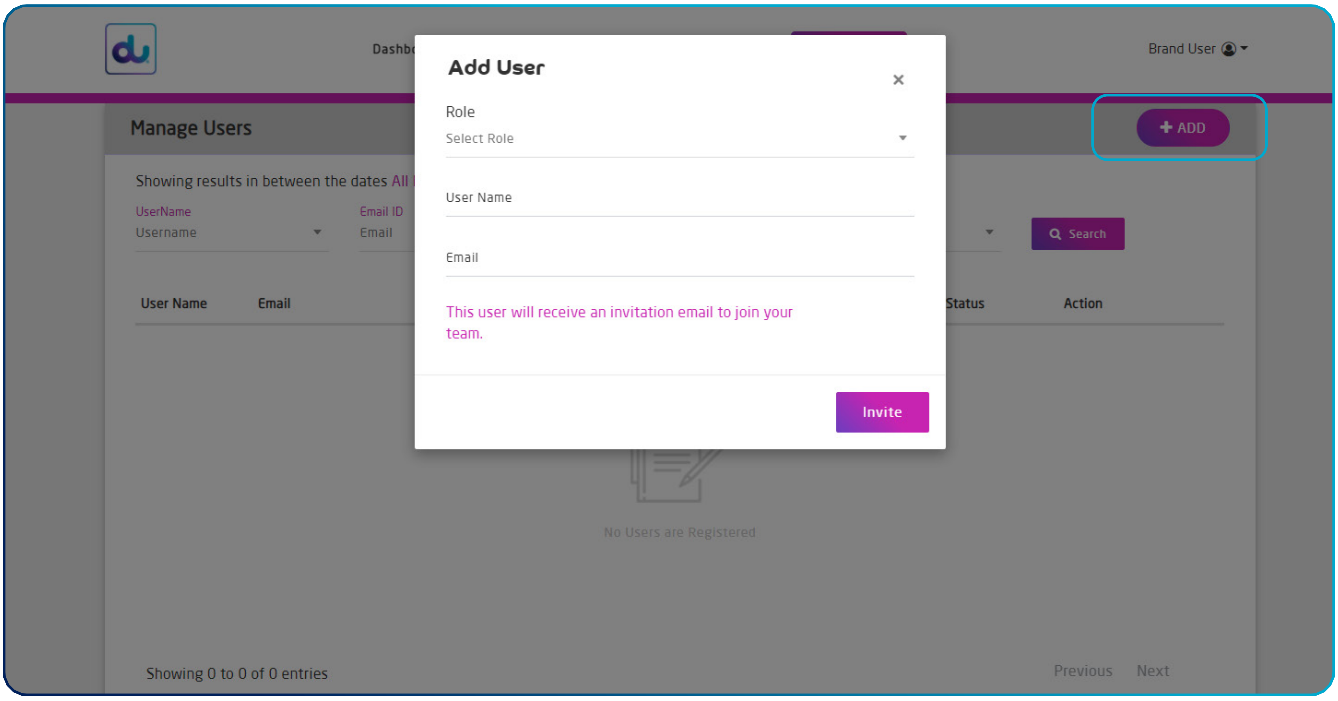
Module Functionalities:

1. Enables Admin User to select a particular role for the new user.
2. Enables Admin User to add the email ID of the new user.
3. Enables Admin User to add username of the new user.
4. Enables Admin User to submit the request.
5. Enables Admin User to receive a confirmation email upon submission of new request.

Business Rules:

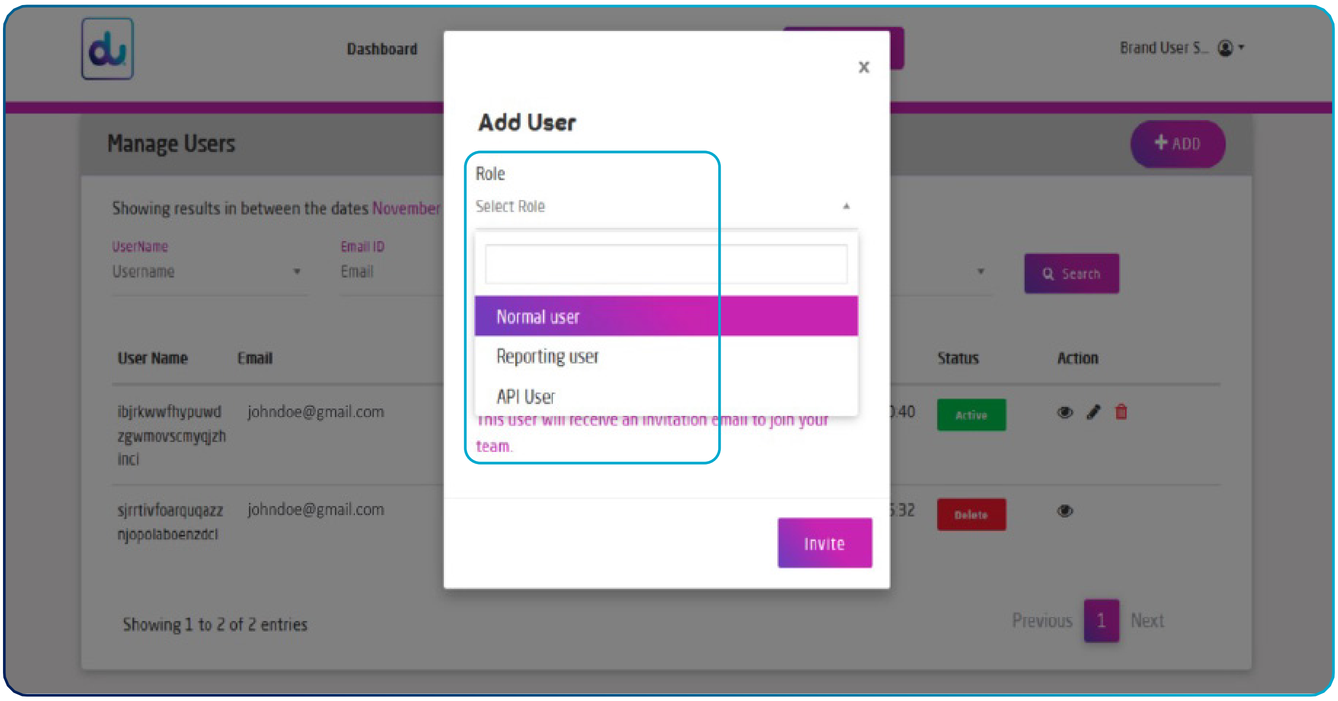
1. Admin User can only create a Normal, a Reporting or API User.
2. Admin User cannot create another Admin User.
3. Admin User is allowed to enter a maximum of 100 character in username field.
4. Admin User is allowed to enter email ID field with standard international guidelines RFC 8398 only.
5. Admin User will only receive confirmation email upon creating a new user request.
6. Normal or Reporting User will receive account activation email and a confirmation email once their account is successfully activated.
7. API User cannot be used to login into the Portal and is only used for API transactions.
8. Only one API User can be created at any one point of time.
9. API User will receive an email on the provided email address with the confirmation that consent upload or consent revoke reports for API transactions will be sent over this email address

To create a new User, the admin will click the "+ADD" button on the on the 'Manage Users' page as shown below. The 'Add User' popup screen will appear to create a new user.

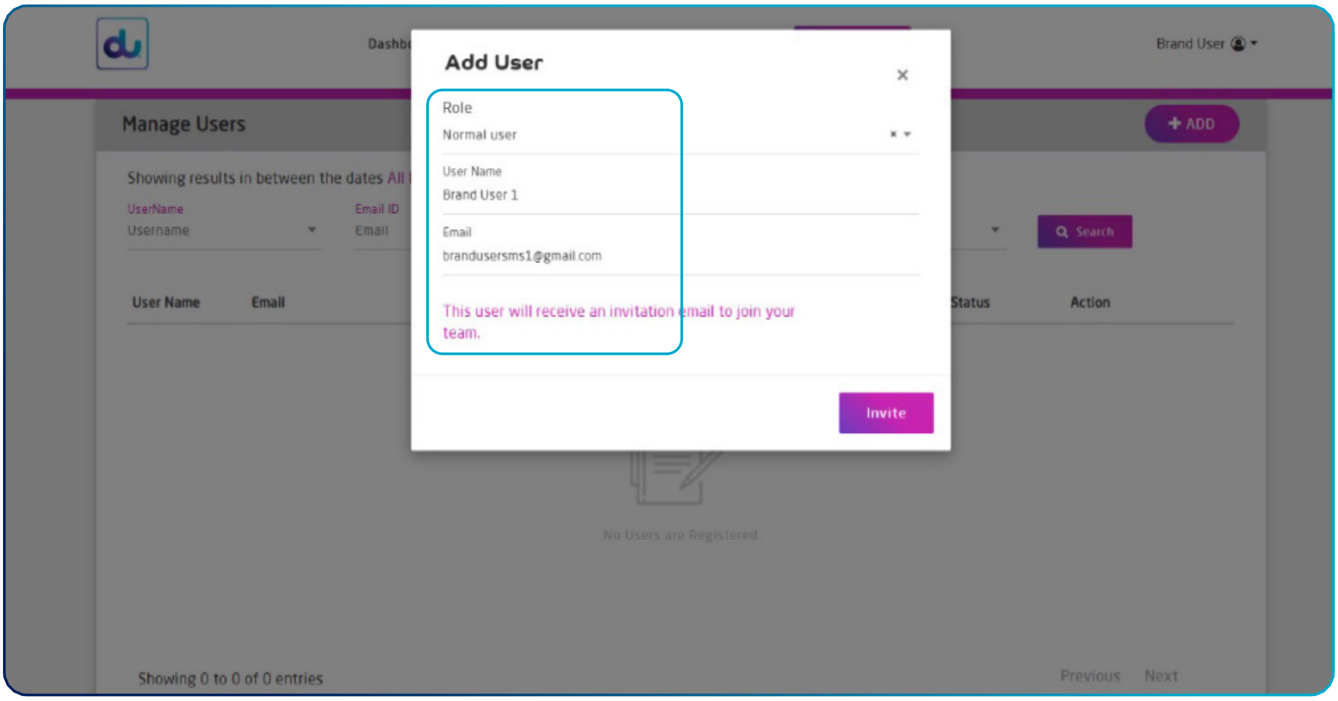


14.2 Adding a new Normal/Reporting User

The Admin User will choose a 'Role' from the 'Select Role' drop down menu to create the specific role for the new User. The Admin User can create a Normal User or a Reporting User for its employees to login into the Portal.

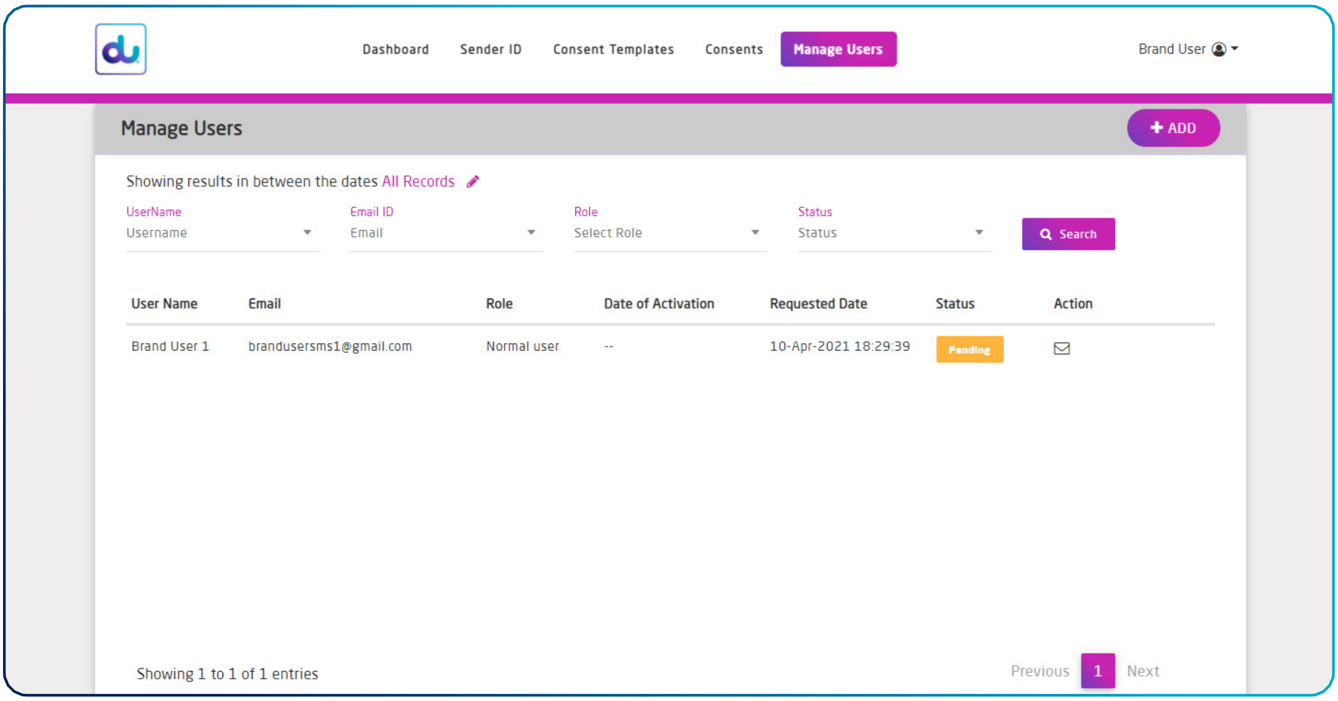


After selecting the required role, the Admin User will enter the User Name and the email address of the new User to be created and click "Invite".

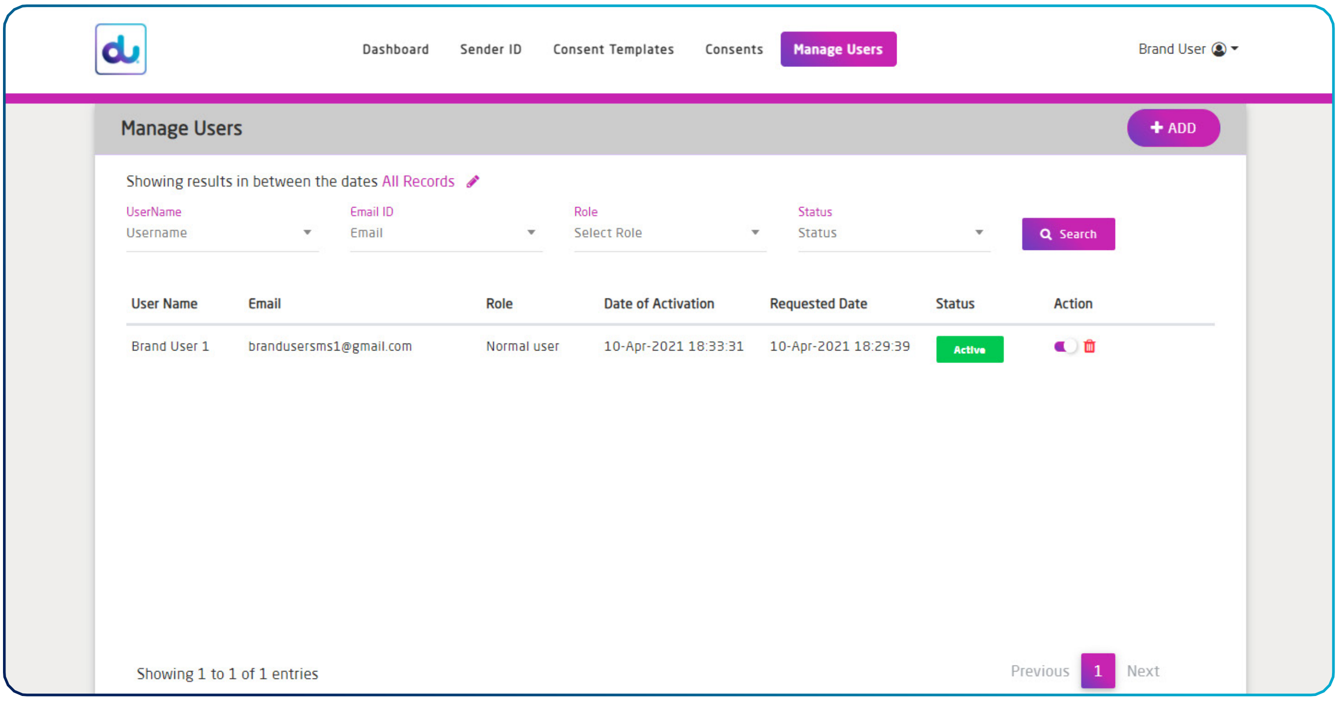


14.2 Adding a new Normal/Reporting User

Once the Admin User clicks "Invite", an invitation link will be sent the new user's email address and the new User will be created in the system with status "Pending" as shown below:

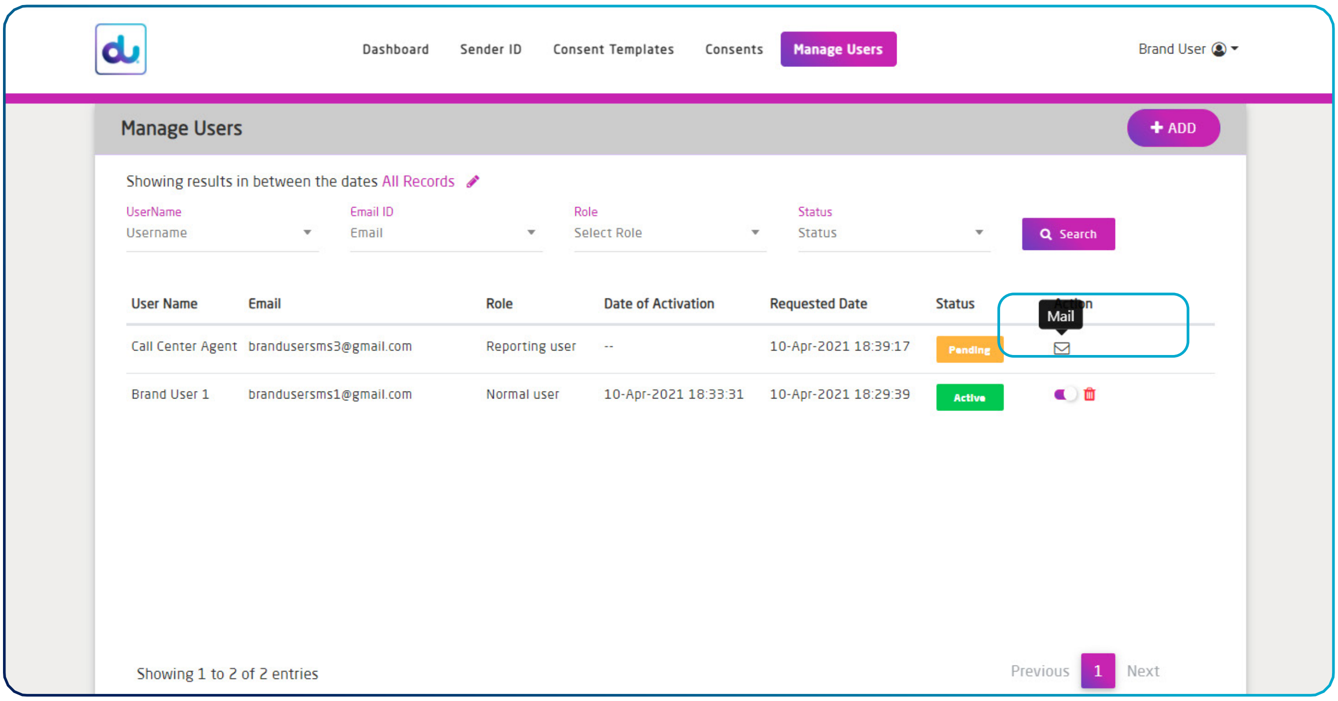


Once the user activates his login by clicking on the activation link sent in the email, the user will be asked to create a new password. Once password is created, new user will be able to login on the system. The status of the new user will turn 'Active' as shown below:

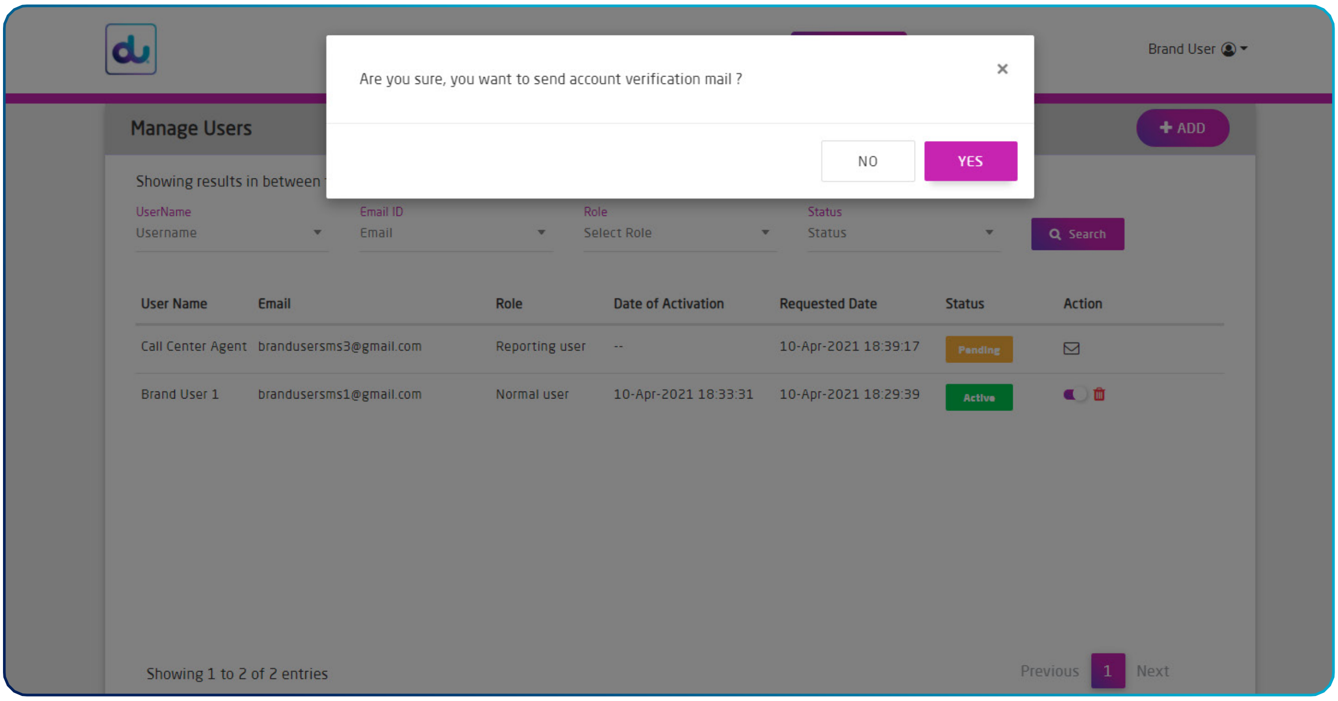


14.3 Resending Activation Link

Once a new User is created, the activation link sent in the email address to the new user will expire after 72 hours. In case the activation link is expired, the Admin User can resend the activation link by clicking the "Mail" icon under the 'Action' tab. The "Mail" icon will only be visible for users in the 'Pending' state.

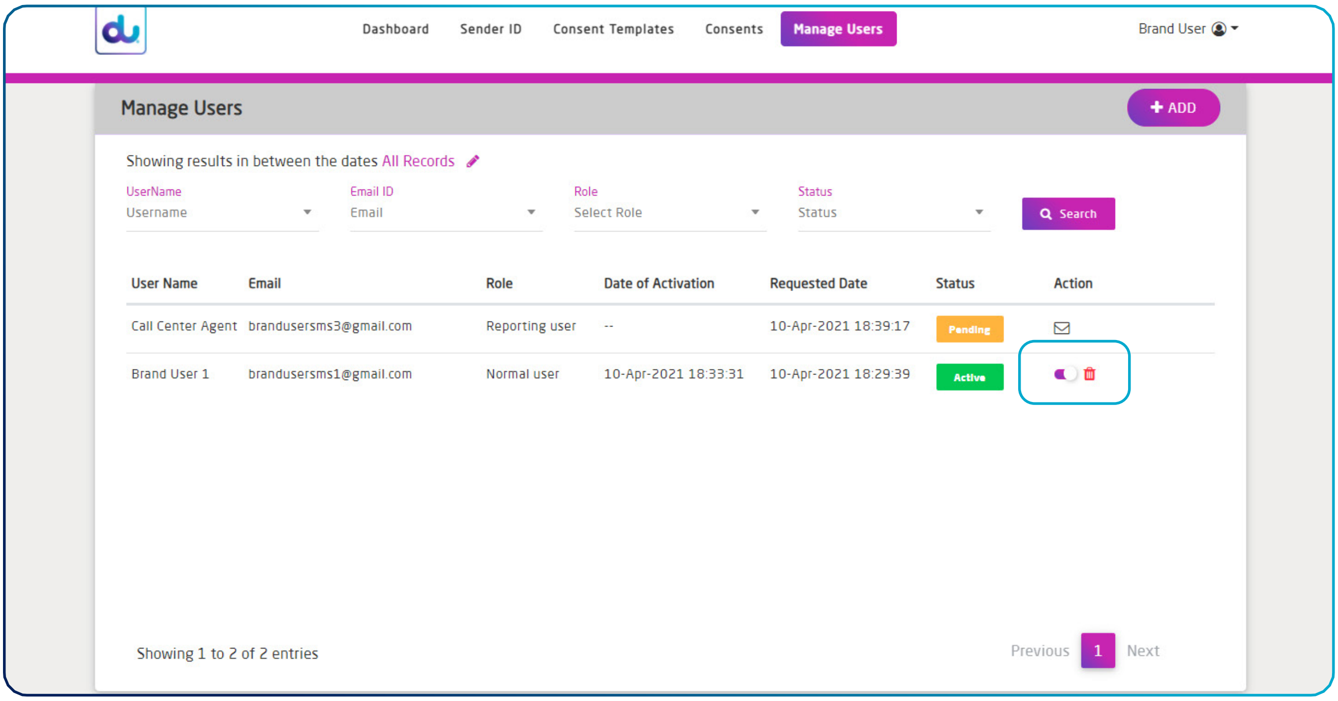


Once the Admin User clicks the "Mail" icon button, the Admin User will be will be asked to reconfirm sending the activation link. Once the Admin User clicks "Yes" on the below popup, the activation link will be sent automatically to the new user registered email address.

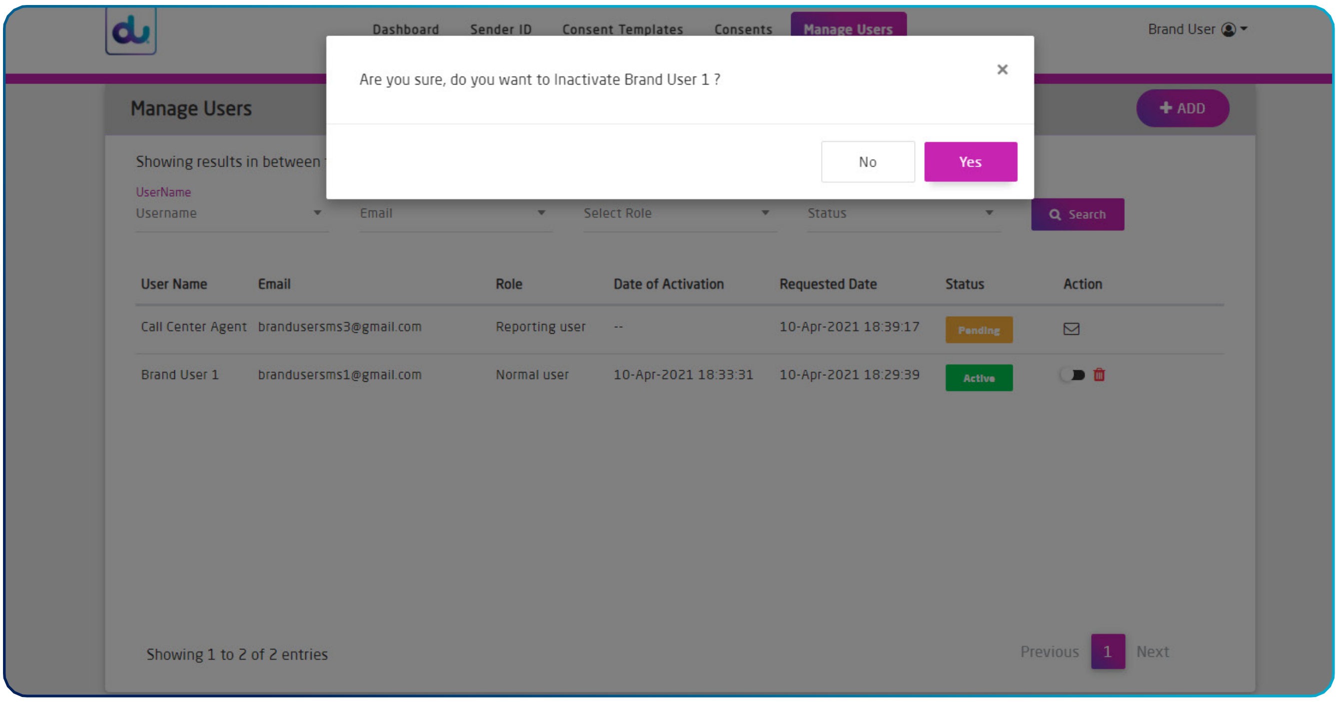


14.4 Suspending a User

Admin User can suspend a Normal or Reporting User by clicking on the "Toggle" switch under the 'Action' tab as shown below: Only a user in an 'Active' state can be suspended.

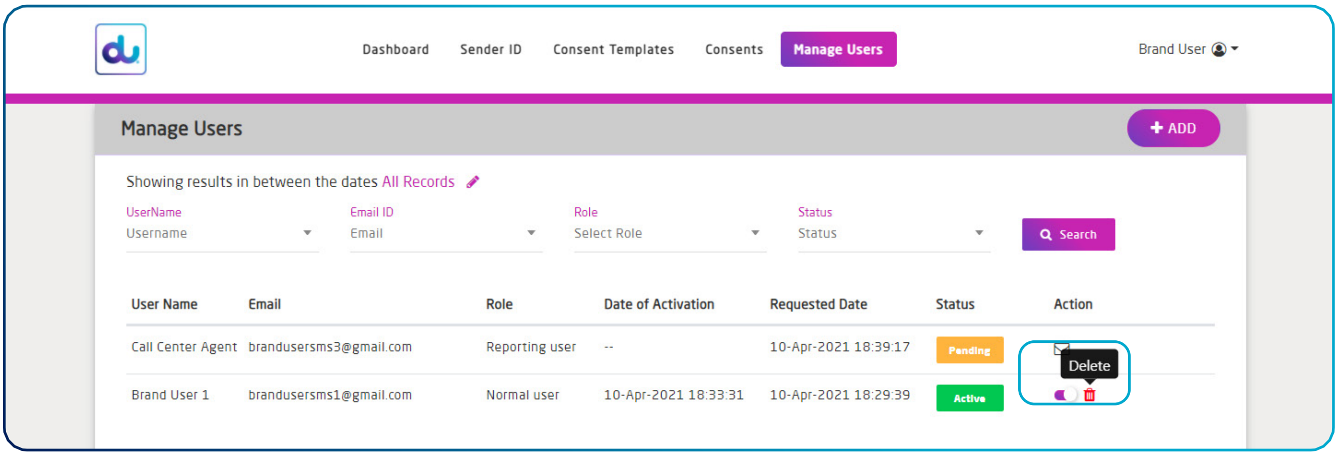


Once an Admin User clicks on the "Toggle" switch, the User will be asked to reconfirm suspension. Upon clicking "Yes", the Normal or the Reporting account will be suspended. Once an account is suspended, the User will not be able to access the account.

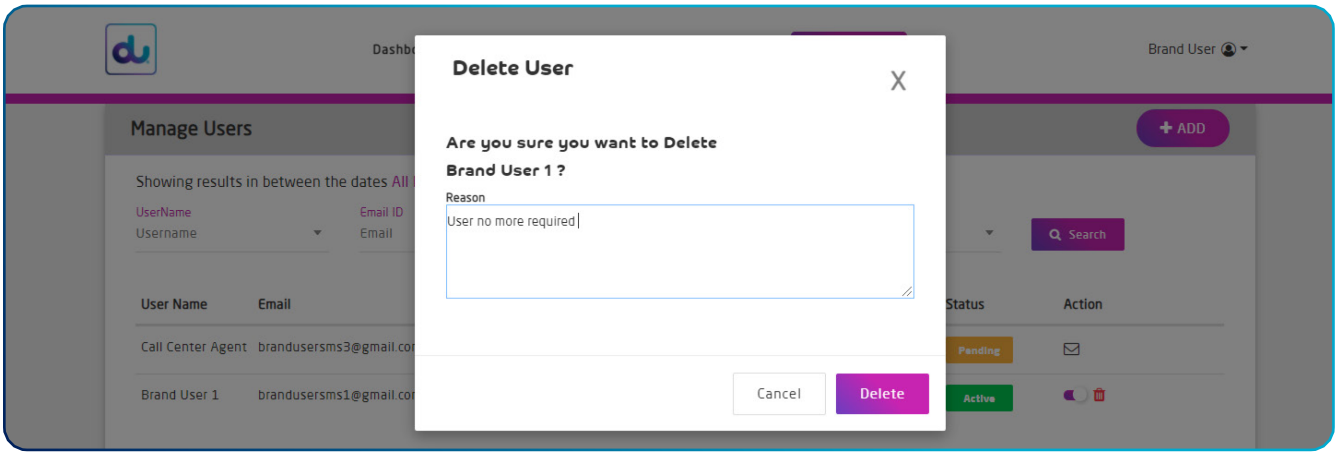


14.5 Deleting a User

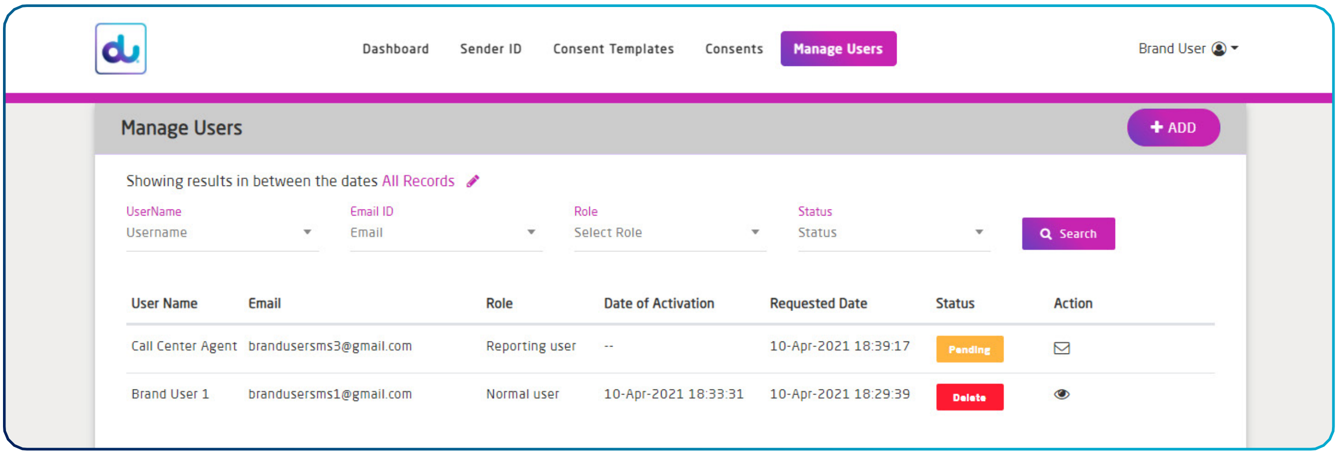
Admin User can delete a Normal or Reporting User by clicking on the "Bin" icon under the 'Action' tab as shown below: Only a user in an 'Active' state can be deleted. In case a user is already suspended, the user cannot be deleted. To delete a suspended user, the Admin User will first have to make the suspended user in 'Active' state and then proceed to delete.



Once the Admin User, clicks the "Bin" icon to delete the user, a popup screen will open as shown below and Admin User will be required to input the delete reason before clicking the "Delete" button. Once a User has been deleted, the same email address cannot be used to recreate the User again.

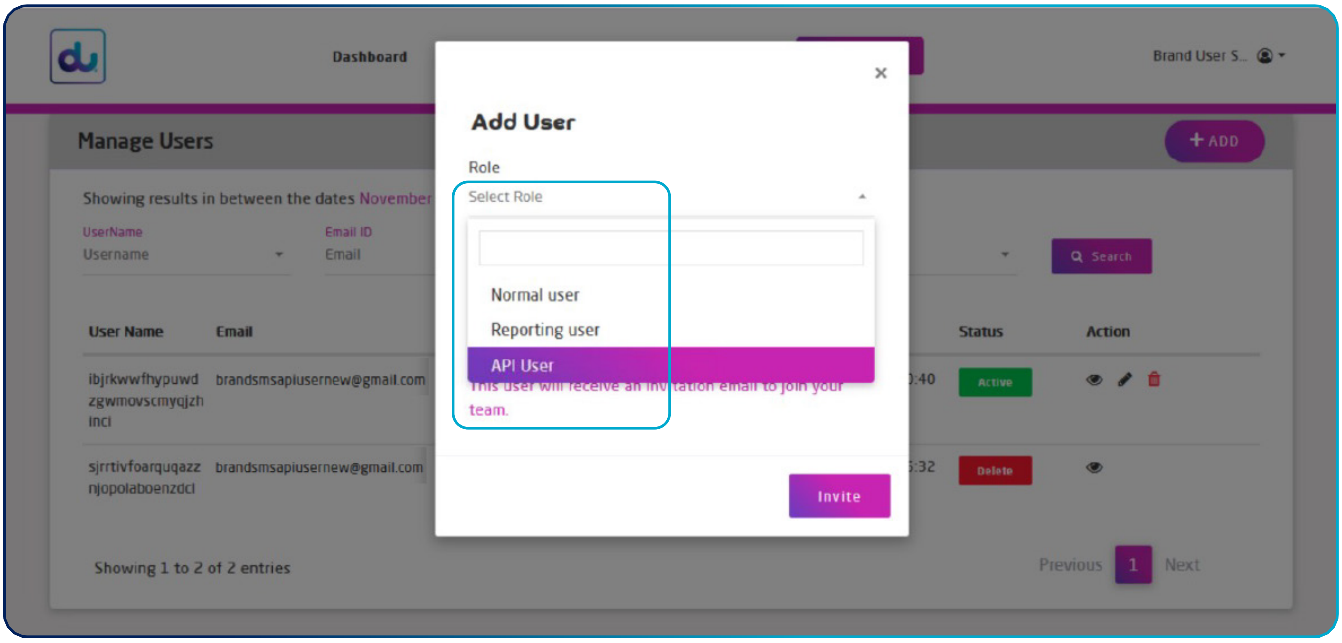


Once a user has been deleted, the status of the deleted user will be changed to 'Delete' as shown below: The Admin User can click the "EYE" icon under 'Action' tab to see the deleted reason.

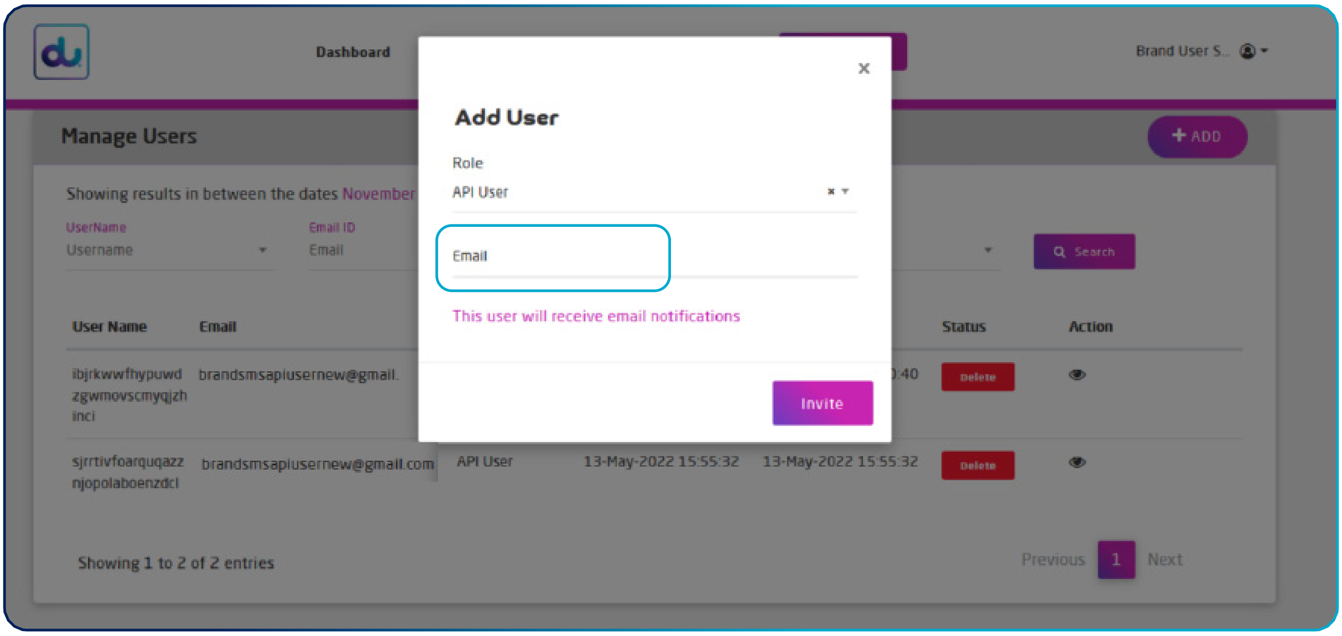


14.6 Adding an API User

To create an API User, the Admin User will choose the 'API User' role from the 'Select Role' drop down menu.

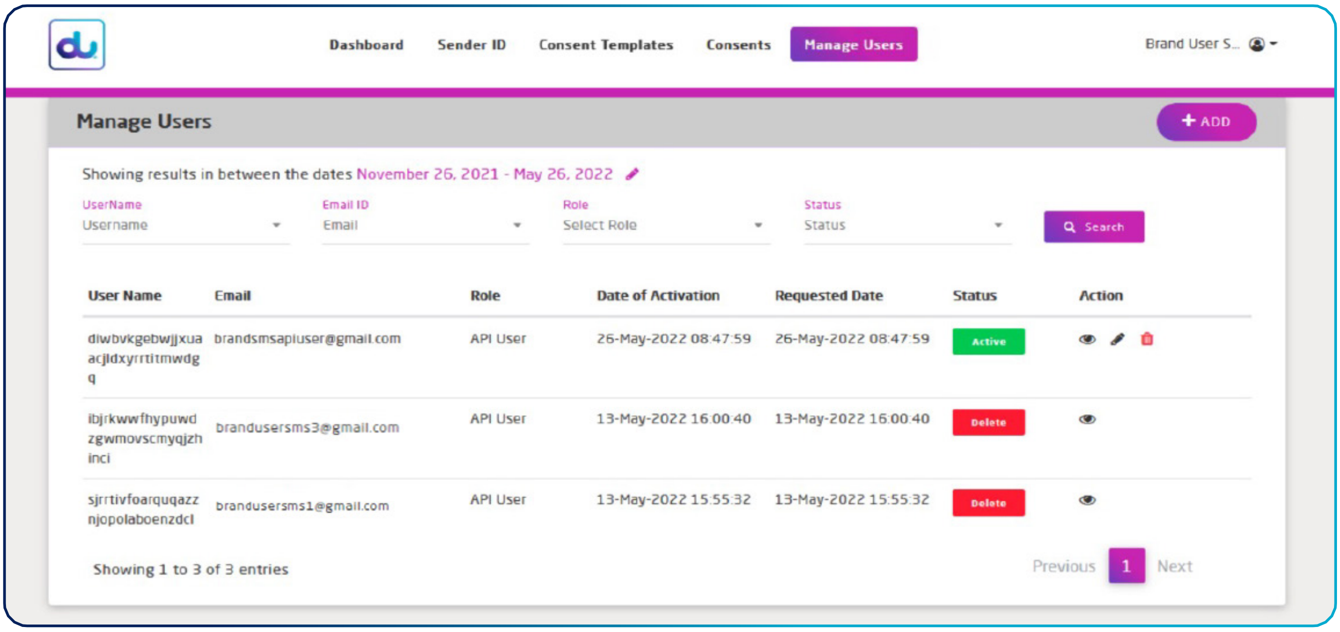


After selecting the API role, the Admin User will only enter an email address for the API User and click "Invite".

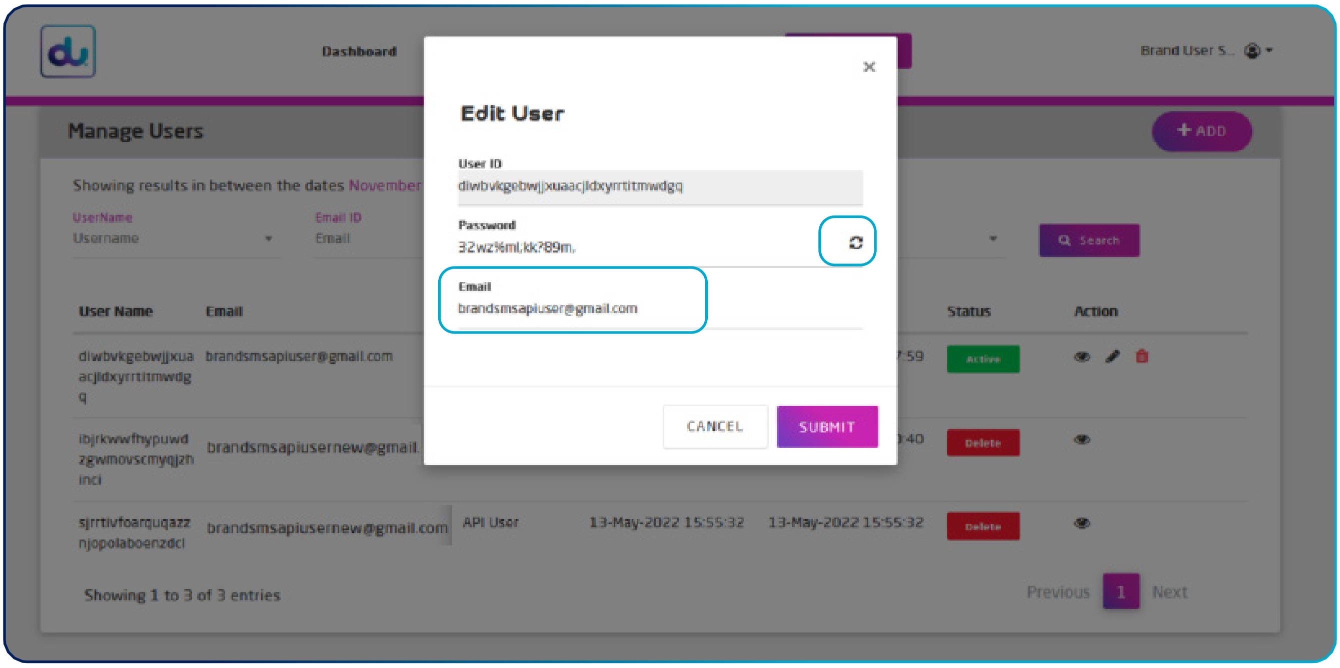


14.7 Viewing/Editing an API User

Once the Admin User clicks "Invite", an API User will be created on the Portal as show below. The username and password of the API User will be automatically created that will be required to be used with API transactions. The API User username and password can be viewed by clicking the "Eye" icon under the 'Action' tab .



In case Admin User wants to modify API User credentials, they can click the "Pen" icon under the 'Action' tab. Admin User can refresh the password of the API User by clicking the 'Refresh' icon or update the email address only on the 'Edit User' screen as shown below. Admin User cannot modify the user name of the API User. In case Admin User want to modify the API User name, Admin User can delete the existing API User and recreate a new one with a new username.



Note: In case an email address was used for an API User that is already deleted, the same email address cannot be reused for a new API User. In case Admin User wants to reuse an existing API User email address, the Admin User must update the email address of the current API User to any dummy email address prior to deleting the current API User.

15. Profile

This module allows Users to view and update their account details.

Applicable to:

- Admin User
- Normal User
- Reporting User

Module Functionalities:

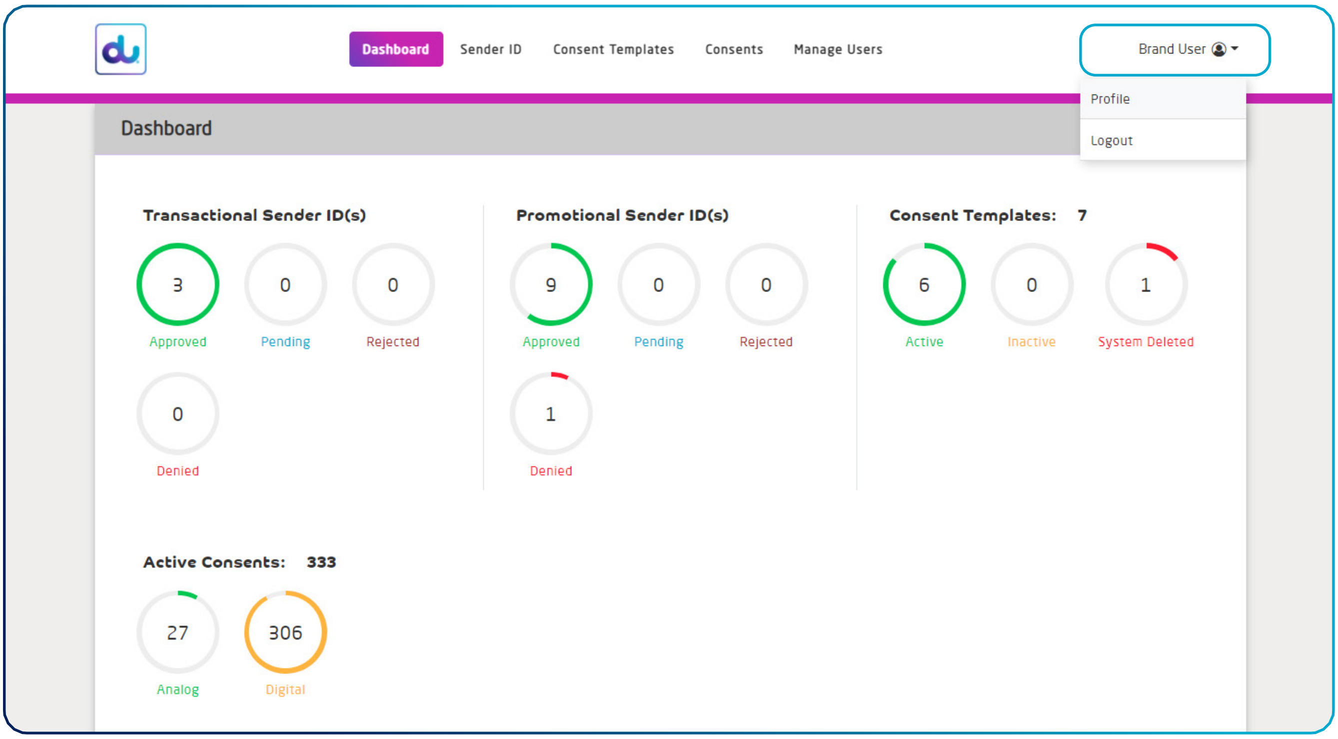
1. Enable Users to view their account details.
2. Enables all Users to update their account password.
3. Enables Admin User to update company documentation.
4. Provides a link to download the Enterprise SMS Portal User Manual.
5. Email notification sent on account update activities to the Users.

Business Rules:

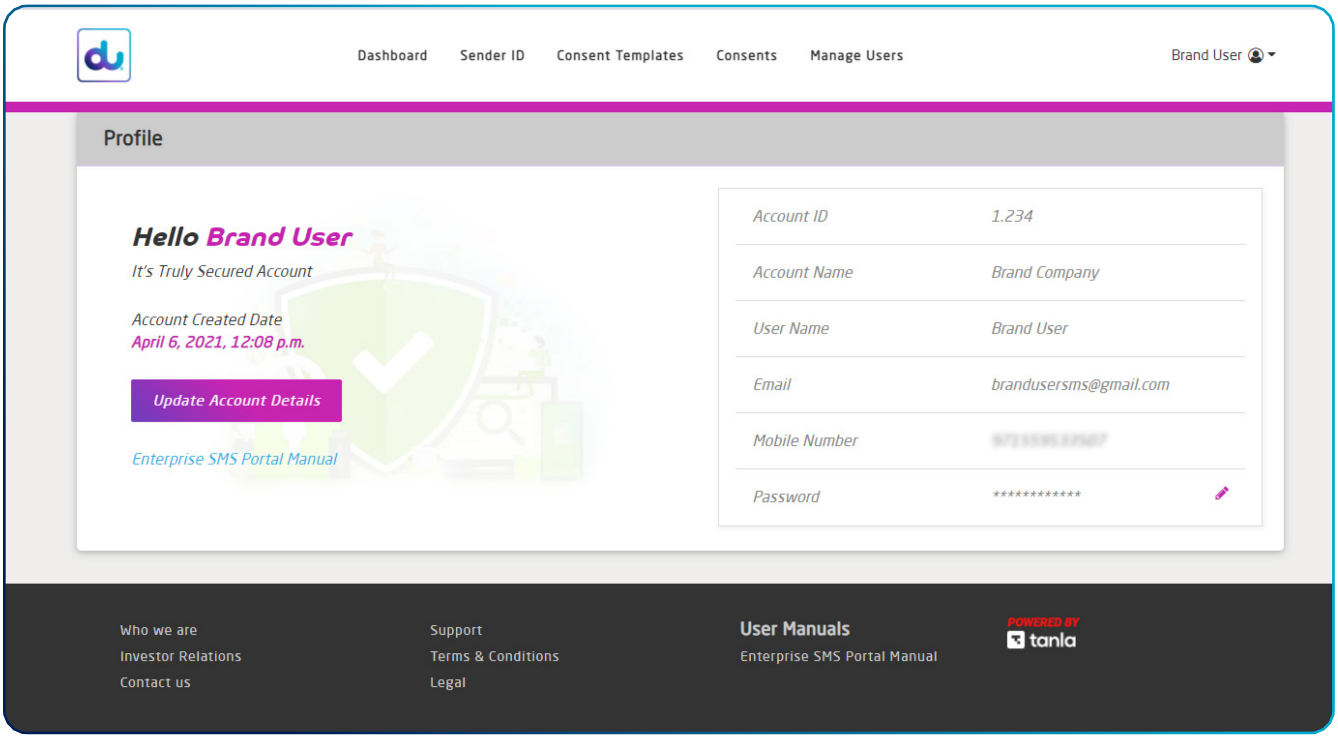
1. Any of the company details cannot be edited by any type of User.
2. Admin User is able to view Account ID, Account name, Username, Email ID, Mobile number and password details.
3. Normal and Reporting Users are able to view Account name, Username, Email ID and password details.
4. For Admin User only, for password change, an OTP is sent to the registered mobile number.
5. The password change OTP expires in 2 minutes.
6. No password OTP is required to change password of Normal or Reporting Users.
7. Admin User can only upload new documents to the account. Uploaded documents cannot be edited or removed from the account.
8. The following list of documents should be uploaded on the system by Admin User:
    a. Trade Licence/Establishment Card/Decree.
    b. Owners Emirates ID or Passport and Visa documents.
    c. Trademark documents.

15. Profile

Users can click the 'Profile' icon on the Dashboard page to access profile page.

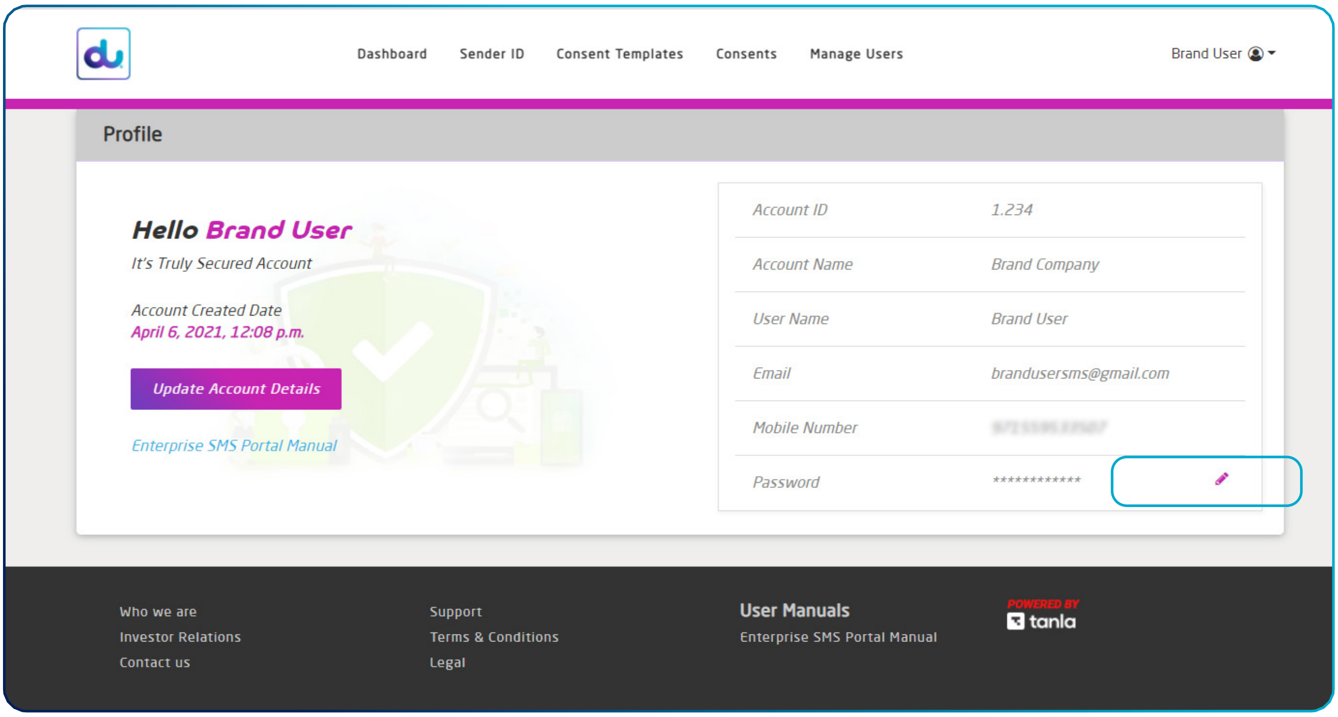


Once User clicks on the 'Profile' button, the User can review his user profile details as shown below:

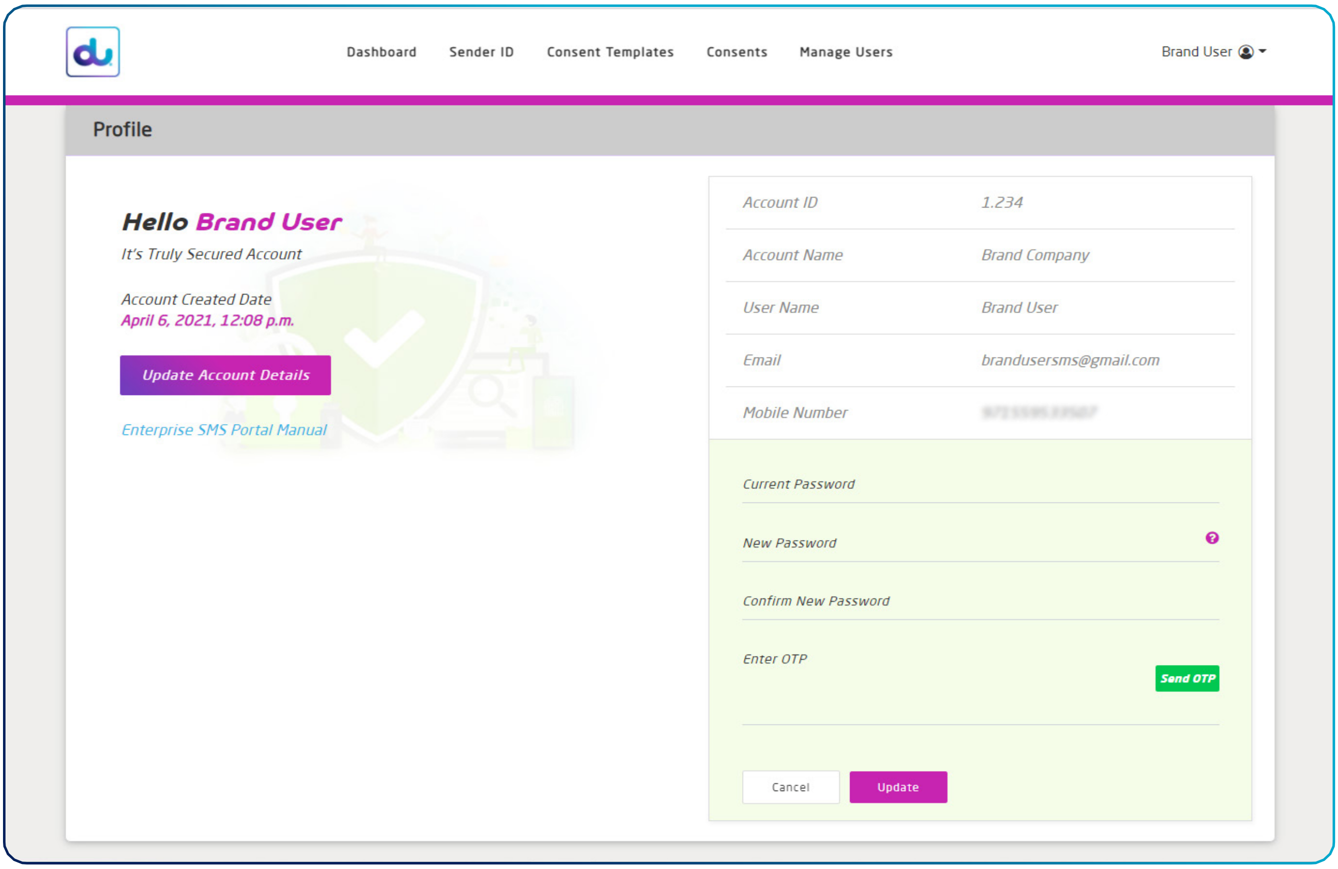


15.1 Update Password

The Users can change the password of their account by clicking on the "Pen" icon on the password field.

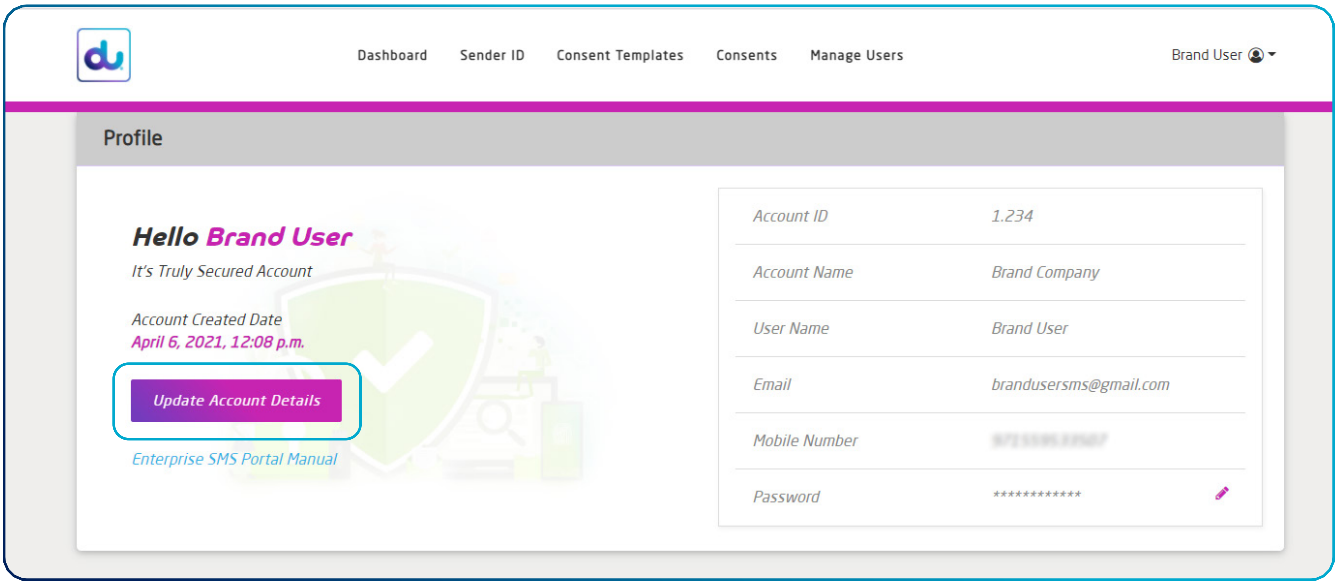


Once the User clicks on the "Pen" icon, the User can then enter new password. Admin Users will be required to generate the OTP to update the password. The OTP will be sent to the registered mobile number against the user account.

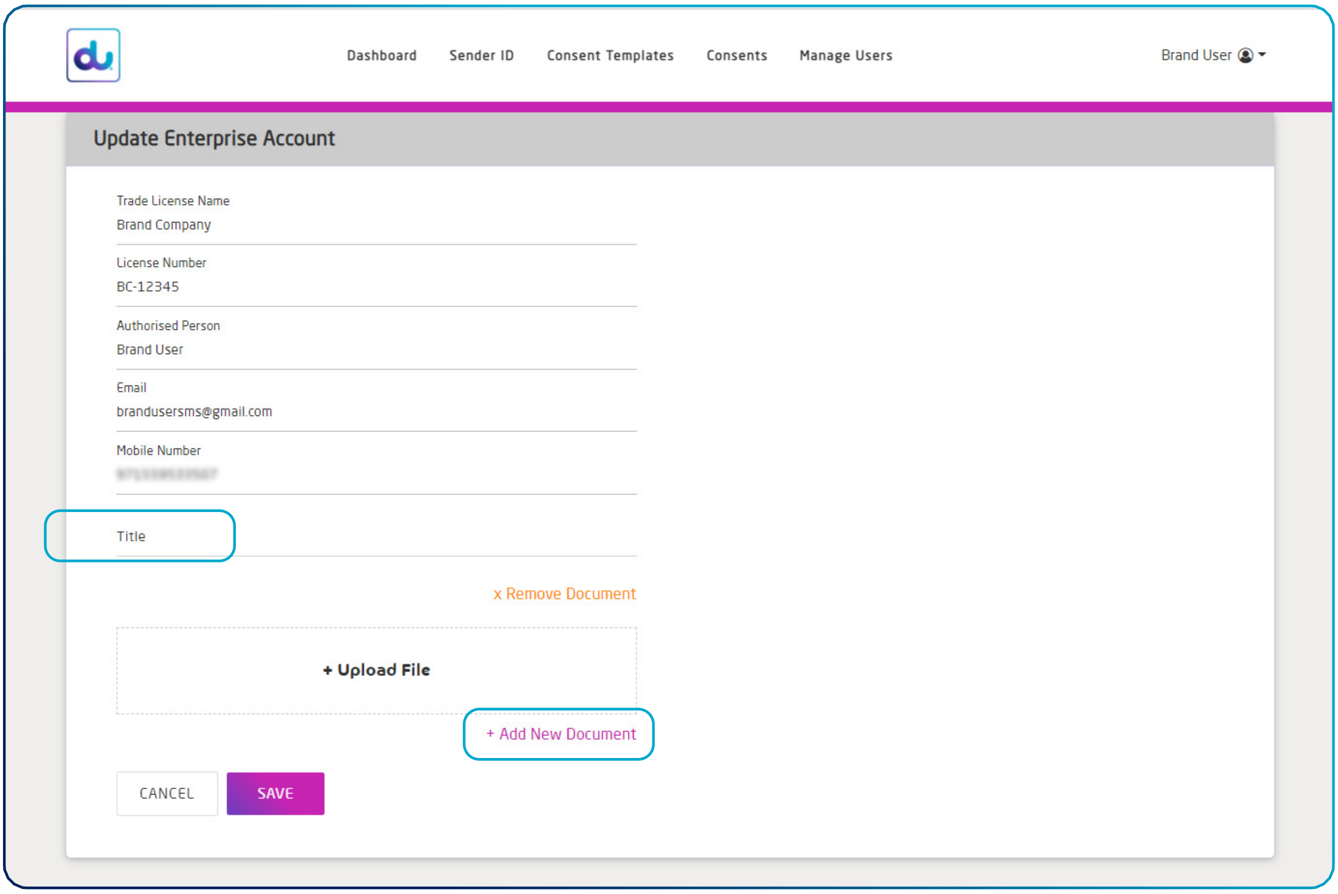


15.2 Update Account Details

The Admin User can update the account details by clicking on the "Update Account Details" button as shown below:



Once the Admin User clicks the "Update Account Details" button, the User will be able to add updated documents to the account by clicking "Add New Document" button. The User can add the title of the new document in the "Title" field and click "Save" button to complete the upload process.



16. API Documentation

Enterprise SMS Portal API

16. API Documentation

Enterprise SMS Portal API

Version:	**1.0**
Date:	June 1, 2022

16. API Documentation

Contents

General Scenarios	3
Transport Overview	3
Service Overview	3
Client Onboarding	3
API Specifications	3
Authentication API	3
Consent Register	5
Consent Revoke	8
Error Codes/Status	10
Email Notification	12
API Operational Support	14

16. API Documentation

1. General Scenarios

The general scenarios provide the conceptual description of common services that will be part of the solution regardless of the number and type of transactions that the solution will implement.

2. Transport Overview

This section describes the communication mechanism to be followed for this API.

1) The communication will be over HTTPS.
2) The client authentication will be done via oauth2.0 protocol.

3. Service Overview

This section describes the API's, the input and output parameters of each API along with the error code. The API's are used to upload and revoke the mobile customer consent on the Enterprise SMS Portal.

API Base URL:

Production: **https://api.du.ae:9141/**

4. Client Onboarding

Client to request to collect Client Secret and Client Key from du as part of following on-boarding process.

1. Client must have an account open on Enterprise SMS Portal
2. Client's Technical SPOC must email from the registered email address to **MSGing@du.ae** requesting for API Client Secret and Client Key
3. The subject of the email to be: "Request for API Credentials: Client Name | Entity ID"
4. Client to mention Client Name, Entity ID, SPOC Name, SPOC Email Address and SPOC Mobile number in the email body as well
5. The email must be sent from the registered Technical SPOC email address only
6. API credential SLA is 3 WDs and will be replied back on the requester' email address
7. Once API credentials have been shared with the Client, the Client must create an API User by logging into Enterprise SMS Portal and clicking "Manage Users". The API ID and Password generated by the Client will be used to authenticate API requests. Client can refer to the "Manage Users" section of the User Guide for additional details on how to create an API User.

5. API Specifications

This section describes the API's, the input and output parameters of each API.

5.1 Authentication API

Provider	du
Consumer	Client

API	Description
POST v1/accesstoken	This API is used to get the access token from APIGW for this API access by passing the necessary client credentials. (client secret and client key) as request arguments, the Token needs to be secured for each call from the client and passed in next method callouts. grant_type=client_credentials.

URL: **https://api.du.ae:9141/v1/oauth/token/client-credentials**

Method: POST

16. API Documentation

Headers:

Header	Meaning	Sample	Mandatory	Comments
Authorization	Base 64 encoded client key & secret	Authorization: Basic {BASE 64 encoded string}	Yes	
Content-Type	Request Content Type	application/json	Yes	

Parameters:

Parameter	Value	Mandatory	Comments
grant_type	client_credentials	Yes	Always this value to be sent

Request Body Formats

NA

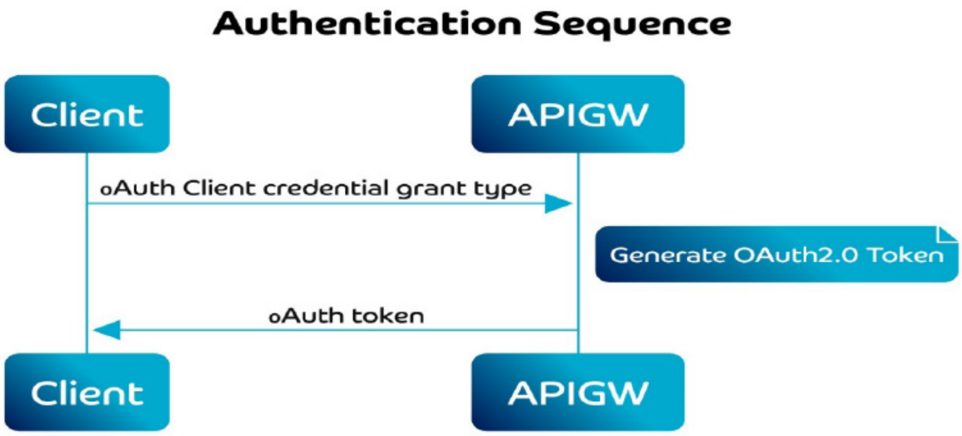
Response Body (success)


```
{
  "refresh_token_expires_in": "0",
  "api_product_list": "[Tanla]",
  "api_product_list_json": [
    "Tanla"
  ],
  "organization_name": "nonproductioncrs",
  "developer.email": "lintu.cherian2@du.ae",
  "token_type": "BearerToken",
  "issued_at": "1649670621462",
  "client_id": "hhBA9OAulmThRpDD6KB30PuSMy9bPZ0J",
  "access_token": "MFZeqRG2ufutu08lFirTbsCtHcQ7",
  "application_name": "d7c18d91-62f7-4136-a4b3-ebda6e4c0721",
  "scope": "",
  "expires_in": "1799",
  "refresh_count": "0",
  "status": "approved"
}
```


Response Body (failure) in case of wrong key value


```
{
  "code": "NB_40100",
  "error": "InvalidAPIKey",
  "message": "Invalid API Key, please check your API Key."
}
```

16. API Documentation



5.2 ConsentRegister_V1 API

Provider	du
Consumer	Client

URL: **https://api.du.ae:9141/tanlaconsentmanagement/ConsentRegister_v1**

Method: POST

API Description: Invoke this API request to register a consent for a mobile subscriber.

Headers:

Header	Meaning	Sample	Mandatory	Comments
Authorization	Base 64 encoded client key & secret	Authorization: Bearer ACCESS_TOKEN}	Yes	Access token received from the previous API call

Parameters:

Parameter	Data Type	Description	Remarks
user	String(50)	API User ID & Password from Enterprise SMS Portal as UserID|Password Ex: user11|testpass123	(Mandatory)
msisdn	String(12)	Valid Mobile subscriber MSISDN with Country code "971"	(Mandatory) Ex: 971XXXXXXXXX
template_id	String(20)	An active Consent Template ID which is defined in Enterprise SMS Portal	(Mandatory)

16. API Documentation

cms_id	String(19)	19 digit Entity Id generated by Enterprise SMS Portal for each Enterprise Account	(Mandatory) Pattren:[0-9]
consent_time	String(10)	Consent registration date. Unix timestamp.	(Mandatory) Ex: 1603780067
channel	String(3)	Allowed values: web and app. Case insensitive. Ex: WEB/Web/weB also accepted)	(Mandatory)
channel_val	String(50)	URL Address /Social Platform Name or Application Name	(Mandatory) minimum 4 characters and maximum 50 characters with all ascii characters allowed
digital_id	String(500)	System generated ID/ Log or Email Address	(Mandatory) minimum 4 characters and maximum 500 characters with all ascii characters allowed

Request Body Formats

```
{
  "user":"tgnblbnpzkmxhallbvwilbascsndlepal8==a[$#2~(q:1)`",
  "msisdn":"97152220448209",
  "templateId": "1208164810161552691",
  "cmsId":"1201523290000000042",
  "consentTime":"3242",
  "channel":"APP",
  "channelVal":"2342",
  "digitalId":"87486"
}
```

Response:

The response will be in JSON format, it contains status, message and a unique request ID(max length 50).

Status 2000 indicated the request is accepted and request_id is the unique reference number for this transaction.

16. API Documentation

Response Body:

SUCCESS Response:


```
{
  "ConsentRegisterResponse": {
    "status": 2000,
    "message": "Request accepted",
    "request_id": "08aa4cbeb7774bd3a52a7e064f461c85"
  }
}
```


Failure Response:


```
{
"ConsentRegister_v1Response": {
"WS_HEADER_OUTPUT": {
"RESPONSE_CODE": "-700",
"RESPONSE_MSG": null,
"ERROR_CODE": "5011",
"ERROR_DESCRIPTION": "Invalid user value"
}
}
}
```


Failure Response in case of Token Expiration:


```
{
  "ResponseCode": "4001",
  "ResponseDescription": "Access Token Expired",
  "ErrorCode": "4001",
  "ErrorDescription": "Access Token Expired"
}
```

16. API Documentation

5.3 ConsentRevoke_V1 API

Provider	du
Consumer	PARTNER

URL: **https://api.du.ae:9141/tanlaconsentmanagement/ConsentRevoke_v1**

Method: POST

API Description: Invoke this API request to revoke a consent for a mobile subscriber.

Headers:

Header	Meaning	Sample	Mandatory	Comments
Authorization	Base 64 encoded client key & secret	Authorization: Bearer ACCESS_TOKEN}	Yes	Access token received from the previous API call

Parameters:

Parameter	Data Type	Description	Remarks
user	String(50)	API User ID & Password from Enterprise SMS Portal as UserID|Password Ex: user11|testpass123	(Mandatory)
msisdn	String(12)	Valid Mobile subscriber MSISDN with Country code "971"	(Mandatory) Ex: 971XXXXXXXXX
type	String(1)	S for SenderID, G for GroupID	(Mandatory) Pattren:S/G
type_value	String(11)	Active/Suspended SenderID (or) Active GroupID	(Mandatory) Ex: AD-XXXX (or)12
cms_id	String(19)	19 digit Entity Id generated by Enterprise SMS Portal for each Enterprise Account	(Mandatory) Pattren:[0-9]
revoke_time	String(10)	Consent revokation date. Unix timestamp.	(Mandatory) Ex: 1603780067

16. API Documentation

Request Body Formats


```
{
  "user": "tgnblbnpzkmxhallbvwilbascsndlepa|8==a[$#2~(q:1)`",
  "msisdn": "971522204482",
  "type": "S",
  "typeValue": "AD-preprd12",
  "cmsId": "1201523290000000042",
  "revokeTime": "1603780679"
}
```


Response:

The response will be in JSON format , it contains status, message and a unique request ID(max length 50).

Status 2000 indicated the request is accepted and request_id is the unique reference number for this transaction.

Response Body:

SUCCESS Response:


```
{
 "ConsentRevokeResponse": {
  "status": 2000,
  "message": "Request accepted",
  "request_id": "87f73a04e6b9410ebf9c07ec7b211ba5"
 }
}
```


Failure Response:


```
{
"ConsentRevoke_v1Response": {
"WS_HEADER_OUTPUT": {
"RESPONSE_CODE": "-700",
"RESPONSE_MSG": null,
"ERROR_CODE": "5012",
"ERROR_DESCRIPTION": "Invalid cms_id length"
}
}
}
```

16. API Documentation

Failure Response in case of Token Expiration:


```
{
  "ResponseCode": "4001",
  "ResponseDescription": "Access Token Expired",
  "ErrorCode": "4001",
  "ErrorDescription": "Access Token Expired"
}
```


5.4 Error Codes/Status

Error code(status)	**Description**
NB_40100	Invalid API Key
4000	Bad request
4040	No data available, Empty set
4001	Invalid token
5000	Technical error
5010	<parameter>parameter is missing Ex: 'user' parameter is missing 'msisdn' parameter is missing 'template_id' parameter is missing 'cms_id' parameter is missing 'consent_time' parameter is missing 'channel' parameter is missing 'channel_val' parameter is missing 'digital_id' parameter is missing 'type' parameter is missing 'type_value' parameter is missing 'revoke_time' parameter is missing

16. API Documentation

5011	Invalid <parameter> value Ex: Invalid 'user' value Invalid msisdn value Invalid 'template_id' value Invalid 'cms_id' value Invalid 'consent_time' value Invalid 'channel' value Invalid 'channel_val' value Invalid 'digital_id' value Invalid 'type' value Invalid 'type_value' value Invalid 'revoke_time' value
5012	Invalid <parameter> length Ex: Invalid 'user' length Invalid 'msisdn' length Invalid 'template_id' length Invalid 'cms_id' length Invalid 'consent_time' length Invalid 'channel' length Invalid 'channel_val' length Invalid 'digital_id' length Invalid 'type' length Invalid 'type_value' length Invalid 'revoke_time' length
5013	Account not found or not active
5014	Consent Template not found or not active
5015	SenderID not found
5016	GroupID not found or not active
5017	API User not found or not active
5018	SenderID is Disabled or Deleted
2000	Success

16. API Documentation

6. Email Notification

At the end of each day a separate email will be sent to the API User email address for each API for Consent and Revoke API calls. Only one email will be sent per day containing success/failure response of all API calls made on the same day

Consent API Email Report:

Following information will be available against each consent upload API request:

MSISDN: The mobile number of the mobile subscriber

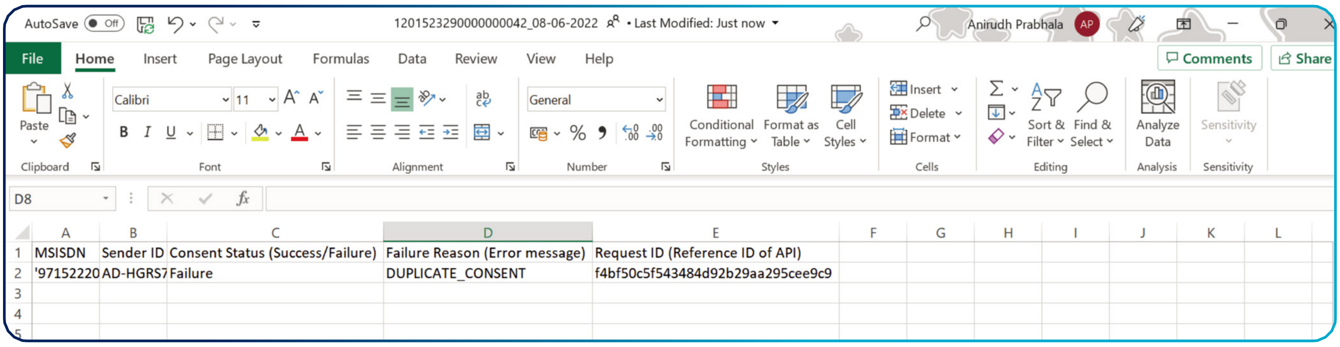
Sender ID: The Sender ID against which the consent is being added

Consent Status: "Success" in case consent was successfully upload in the system. "Failure" in case consent was unsuccessful to be uploaded.

Failure Reason: In case of "Failure" consent status, the failure reason

Reference ID: The "request_id" returned in the API response body of the Success Response

Below is the sample of the email report received on daily basis.



Below Error Code will be returned in the email in case of failure transactions:

ENTITY-IS-NOT-FOUND	INVALID_CHANNEL
ENTITY-IS-NOT-ACTIVE	INVALID_CHANNEL_VALUE
CONSENT_TEMPLATEID_NOT_FOUND	INVALID_DIGITAL_ID
NO_SENDERIDS_FOUND	INVALID_CONSENT
INVALID ROW	DUPLICATE_CONSENT
UNRECOGNISED NUMBER	SENDERID_NOT_ACTIVE
INVALID MSISDN	TECHNICAL_ERROR
INVALID_DATE_FORMAT	

16. API Documentation

Revoke API Email Report:

Following information will be available against each revoke consent API request:

MSISDN: The Sender ID against which the consent is being revoked

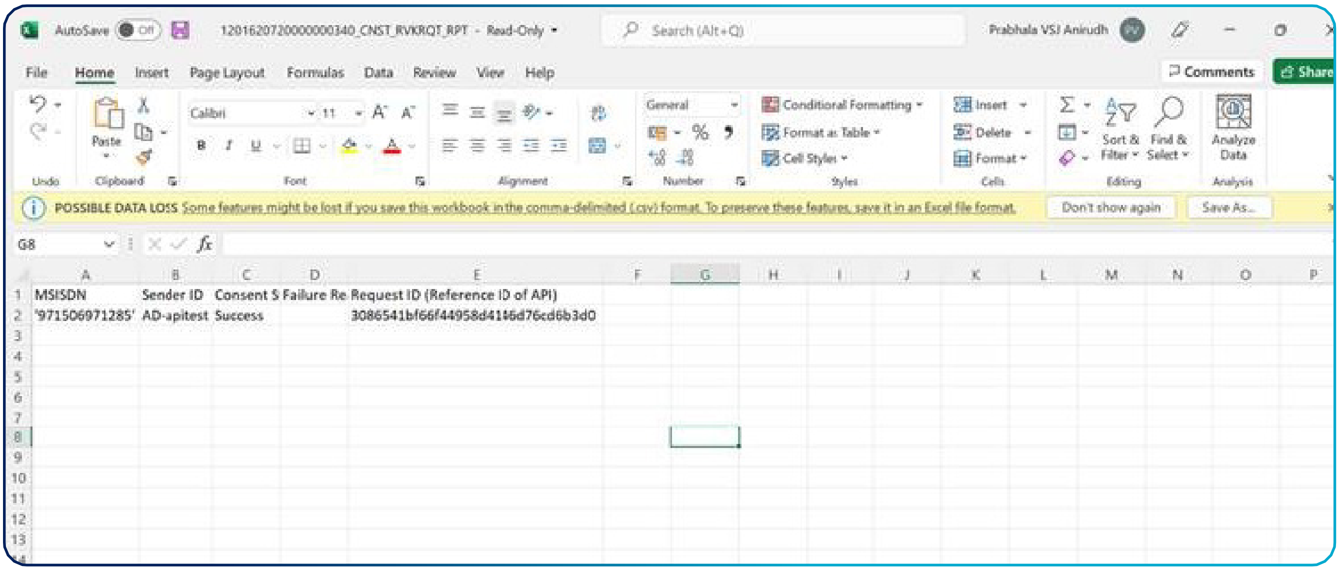
Sender ID: The Sender ID against which the consent is being revoked

Consent Status: "Success" in case consent was successfully revoked in the system. "Failure" in case consent was unsuccessful to be revoked.

Failure Reason: In case of "Failure" consent revoke, the failure reason

Reference ID: The "request_id" returned in the API response body of the Success Response

Below is the sample of the email report received on daily basis.



Below Error Code will be returned in the email in case of failure transactions:

ENTITY-IS-NOT-FOUND
ENTITY-IS-NOT-ACTIVE
NO_SENDERIDS_FOUND
INVALID MSISDN
SENDERID_NOT_ACTIVE
CONSENT_NOT_FOUND
CONSENT_NOT_ACTIVE
TECHNICAL_ERROR

16. API Documentation

7. API Operational Support

In case of any issue on use of API, the client can raise the issue over the following email address:

Support Email Addresses:
IT_APIGateway_ops **IT_APIGateway_ops@du.ae**
Muhammed Asim **Muhammed.Asim1@du.ae**

The Client must follow the below email template while raising the issue:

Email Subject: APIGW_ESP_Client-Name_Issue-Summary

Client Name:

Client Entity ID:

Issue summary:

Issue start time:

Issue detail:

API name:

Actual API response:

Actual API log:

Network connectivity Status (telnet status/logs):

Thank you

BUSINESS