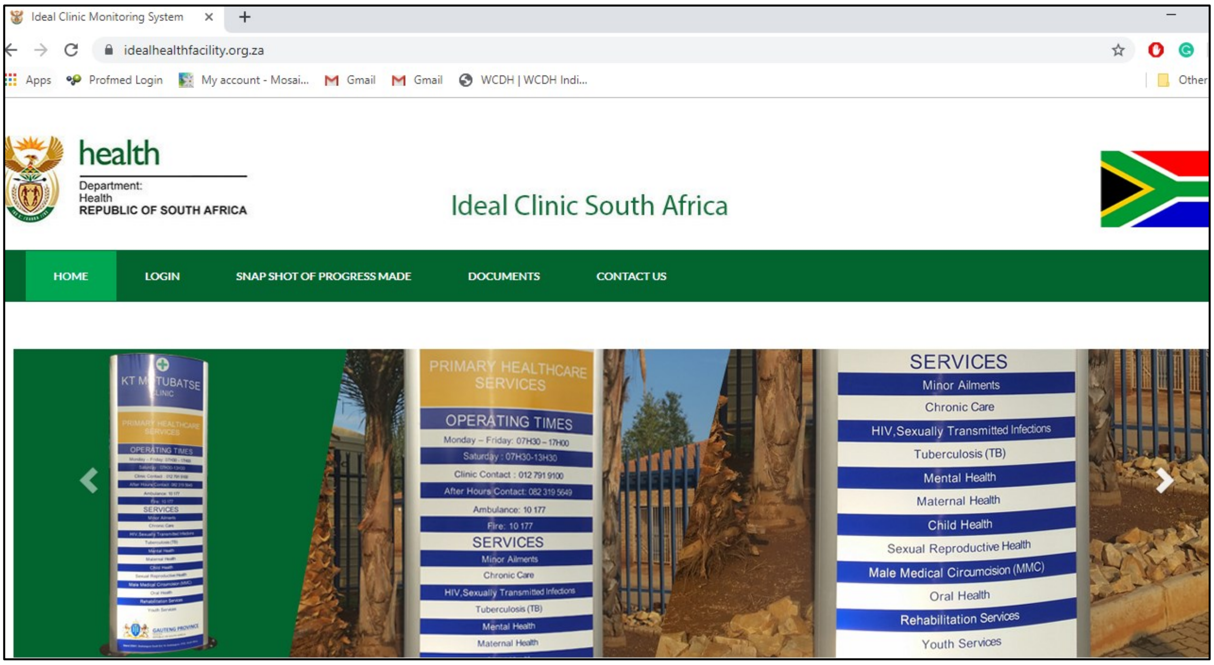
STANDARD OPERATING PROCEDURE TO MANAGE USER ACCOUNTS ON THE IDEAL HEALTH FACILITY INFORMATION SYSTEM



Date: July 2023

health
Department:
Health
REPUBLIC OF SOUTH AFRICA

2030 NDP

This standard operating procedure (SOP) sets out the procedure to manage existing user accounts and create new user accounts on the Ideal Health Facility web-based information system located at https://www.idealhealthfacility.org.za/ .

Revision of the SOP is done when:

- There is a change in the functionality of the user accounts.
- The user account registration form is updated.

Summary of SOP version controls:

- 1st Publication: 30 December 2019
- 2nd Publication: July 2022. Updated to address Auditor General's findings that the SOP did not address the review of user access rights and system administrator activities.
- 3rd Publication: October 2022. Reporting templates updated
- 4th Publication: July 2023. Password requirements/security and creation of district user accounts

Ms JR Hunter

Deputy Director General: Primary Health Carer

Date: 24/7/2023

Table of contents

List of figures

List of Annexures

A. Introduction

This standard operating procedure describes how user accounts should be managed, i.e. manage existing user accounts and create new user accounts, on the Ideal Health Facility information system. A new functionality has been added to allow user account managers to upload the completed user account form, see **Annexure A**. The blank registration form can be downloaded from the information system by selecting the *Account* option under the *Setup* tab on the top navigation bar. Select the button named *User Account Request*. You will be redirected to the screen named *Upload a new request for account*. Download the registration form by clicking on the *Download Form* button. See **Figure 1**. The file will be in PDF format. Save the blank form to your document folder so that you can send it to users to complete.

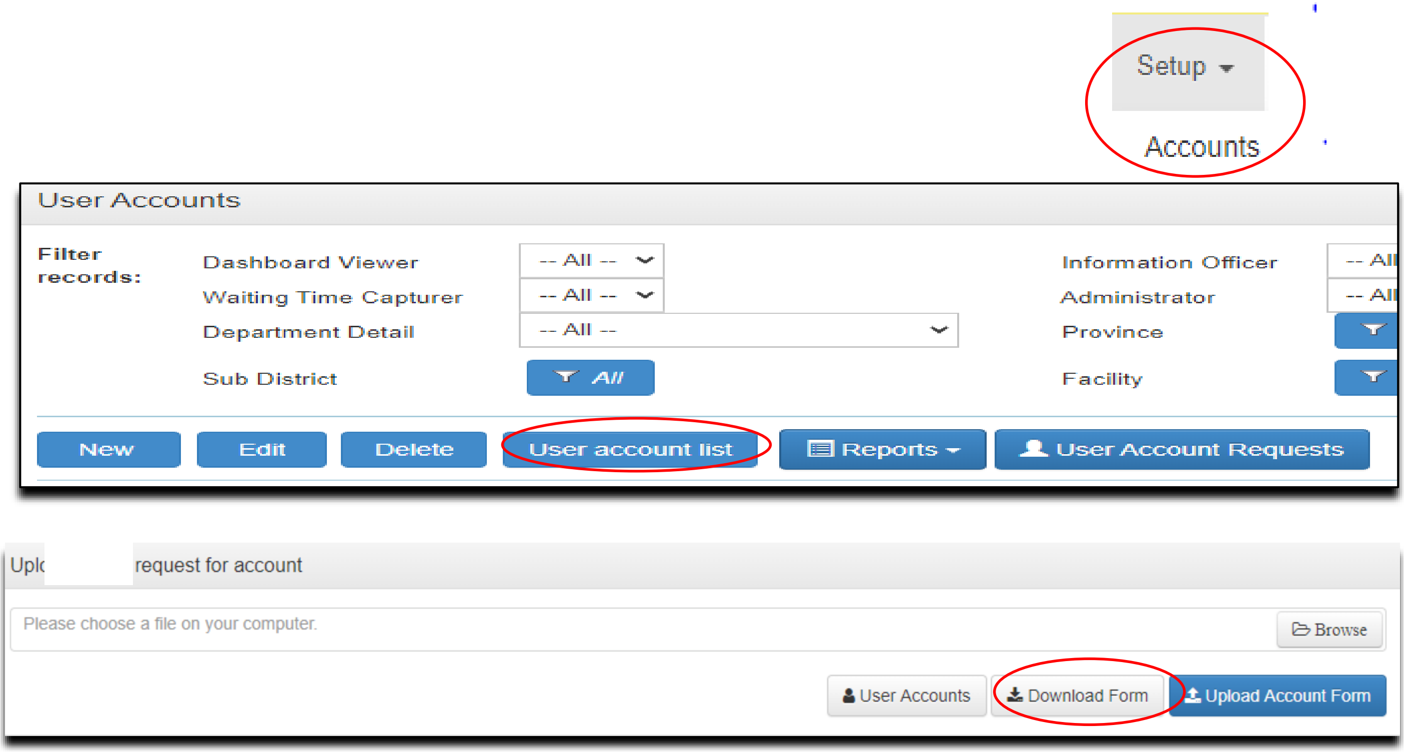


Figure 1: Download a blank request form

The user account form was introduced in 2020, therefore existing user accounts did not have a user account form. Therefore the end goal is to upload a completed user account form for all existing users! This will ensure compliance with the Auditor General requirements. Note that once the functionality to create user accounts has been delegated to a province, the province will be audited in terms of compliance with user account forms that has been uploaded and whether the content of the user account form correspond with the roles and permissions assigned on the information system.

A quick reference guide in the form of a process map is explained in section B. Detailed explanation of the process to follow to manage existing user accounts and create new user accounts is set out sections C and D.

Important terminology used:

- ✓ **Role** = this describes the function a user can perform on the system, e.g. view reports, capture data, create user accounts for specific module on the information system.
- ✓ **Permission** = is the organizational (Org) unit that is assigned to the Role that will allow the user access to a specific or multiple Org units.

B. Process mapping for managing existing user accounts and creating new user accounts

Note the following:

- The user must have the role for “Account Manager” to manage user accounts for the province/ district/sub-district.
- **A user account form must be uploaded for all new users as well as existing users whose user accounts require updating in term of roles/permissions.**

Add a new user account or change/update an existing user account

Go to https://www.idealhealthfacility.org.za and login

Go to the Main menu bar on top of the screen. Select Setup > Accounts.

Select the *User Account Request* button

Select the user account form you want to upload from your Document folder where you have saved the user account form, then select the *Upload Account Form* button.

The e-mail address of the user account form that was uploaded will appear in the list of user accounts. Select the icon under the *Action* section. You can first *Review* the request and then *Accept* the request or immediately *Accept* the request (it is recommended that the request is first reviewed). Select the *User Accounts* button to return to the user account main screen.

On the *Main user account* screen, look under the column marked *Username* for the e-mail address of the account form that you have uploaded, it should display at the top of the screen.

Add the Permissions for the Roles (highlighted in orange) under the column named Permissions. Double click on the Roles listed in the Permission column to add the permissions, the screen named ‘Account Permissions’ will open. **Note:** when you upload a *User account* form of an existing user to update roles/permissions, you must add the additional roles and permission on the Main user account screen. When you upload a *User account* form of an existing user who never had a previous form uploaded, you must add the permission for all the roles as all the existing permissions is removed as a security measure to ensure that correct permissions are assigned. See p7 to p11 for detailed explanation on adding permissions. To enable (activate) a disabled user account, search for the account and tick the ‘enabled’ tick box (p15). **Note:** All users with disabled accounts must submit a

Send account invitation to the user by selecting the *Reset Password* button.

C. Uploading user account forms for new user accounts or for updating existing user accounts

1. To create a new user account or update an existing user account, go to the Main menu bar on top of the screen. Select Setup > Accounts.
2. Select the *User Account Requests* button in the Command row of the Account Management screen. See **Figure 2.**

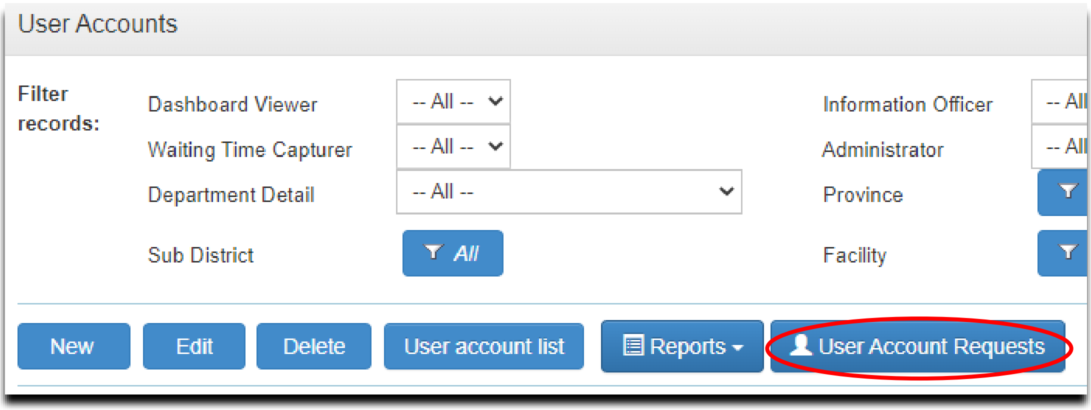


Figure 2: Use the User Account Requests button to create a new user account.

3. Upload the user account request form by selecting the *Browse button*. Find the signed account form in your document folder (where you have saved the user account form) and select it. See **Figure 3**.
4. Click on the *Upload Account Form* button. **Note:** The system will give an error message if all the required fields were not completed and the form will not be uploaded.
5. A new line will then appear in the listing on this screen. In **Figure 3** a request to add username "Sarah.mahlangu@gmail.com" has been added.

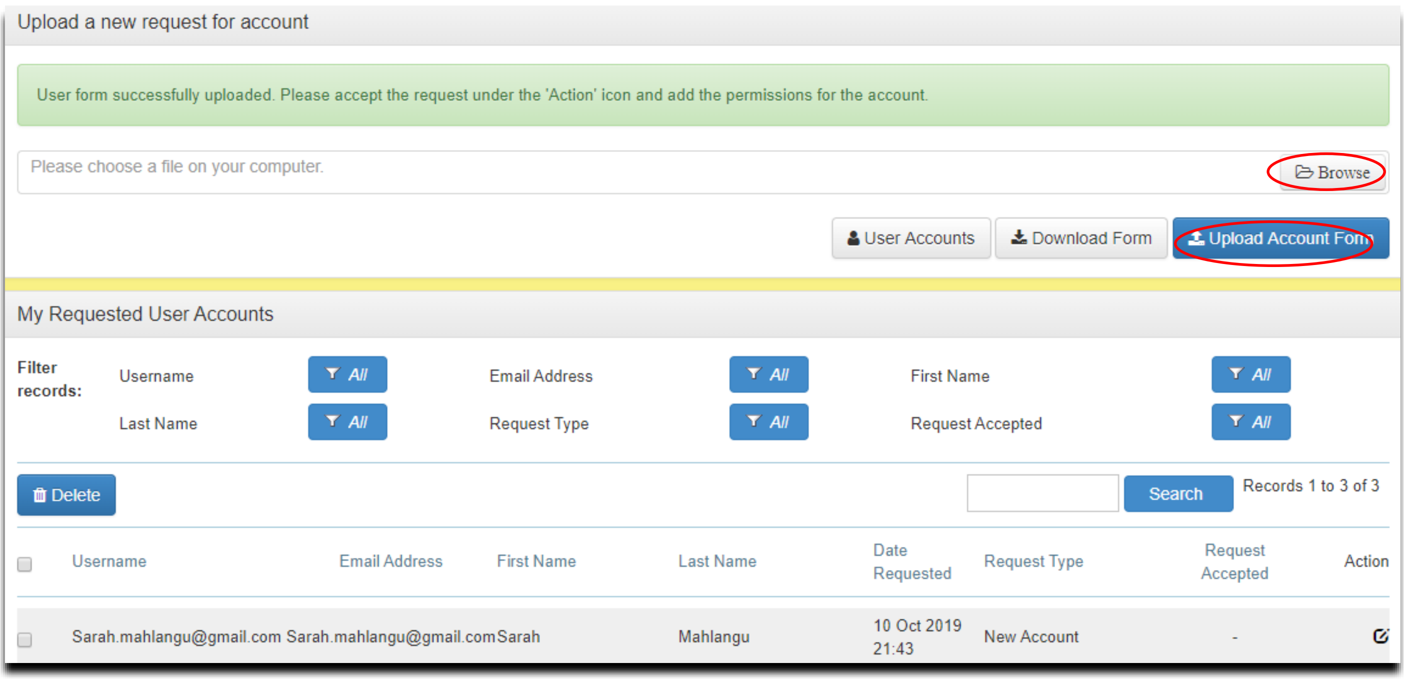


Figure 3: Creating a new or updating a user account

6. Once the form has been uploaded, it needs to be actioned. On the right side of each entry in the *Account Request Form* screen there is a small icon in the *Action* column. See **Figure 4**.

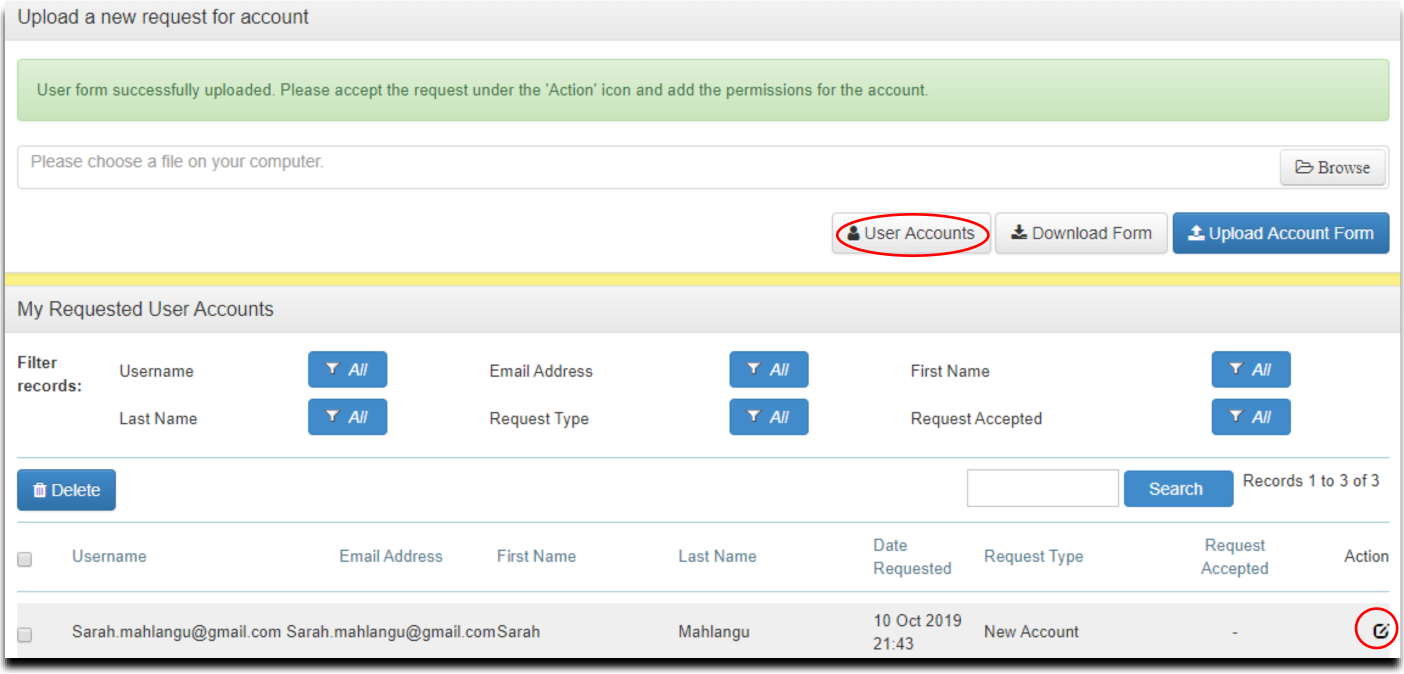


Figure 4: Use the icon in the Action column to action each request.

7. When you click on the Actions icon, you will have the functionality to (see **Figure 5**):
   ✓ View Request Action
   Before actioning the request, it is recommended that you review exactly what is being requested. **Note: The personal information on the form and the Roles will automatically uploaded** to the user account information. By selecting this option in **Figure 5**, you'll be able to see what has been requested and uploaded to the system.
   ✓ Accept Request Action
   This will create a new account or update an existing user account (without having viewed it) that will be listed in the *User Accounts* page. This is not recommended, always first View Request to ensure the correct information will be created on the user account.
   ✓ Decline Request Action
   This will only decline the request and there will be no action required thereafter. Once declined, the request cannot be accepted.
   ✓ Download Form
   Download the original document that has being uploaded.

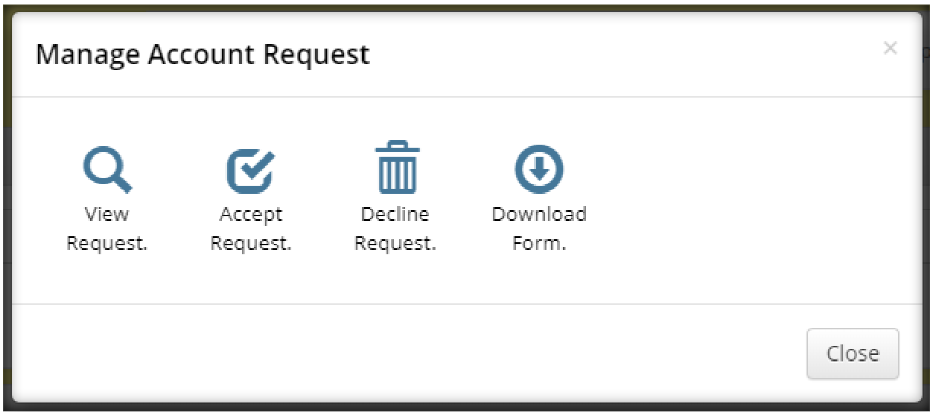


Figure 5: My Requested User Accounts Actions (New and existing user accounts)

8. Once the *Accept Request* option has been selected, the word *Yes* will appear under the column for *Request Accepted*. **Note:** Once you have Accepted the request, select the *User Account* button to return to the main user account screen. See **Figure 6**.

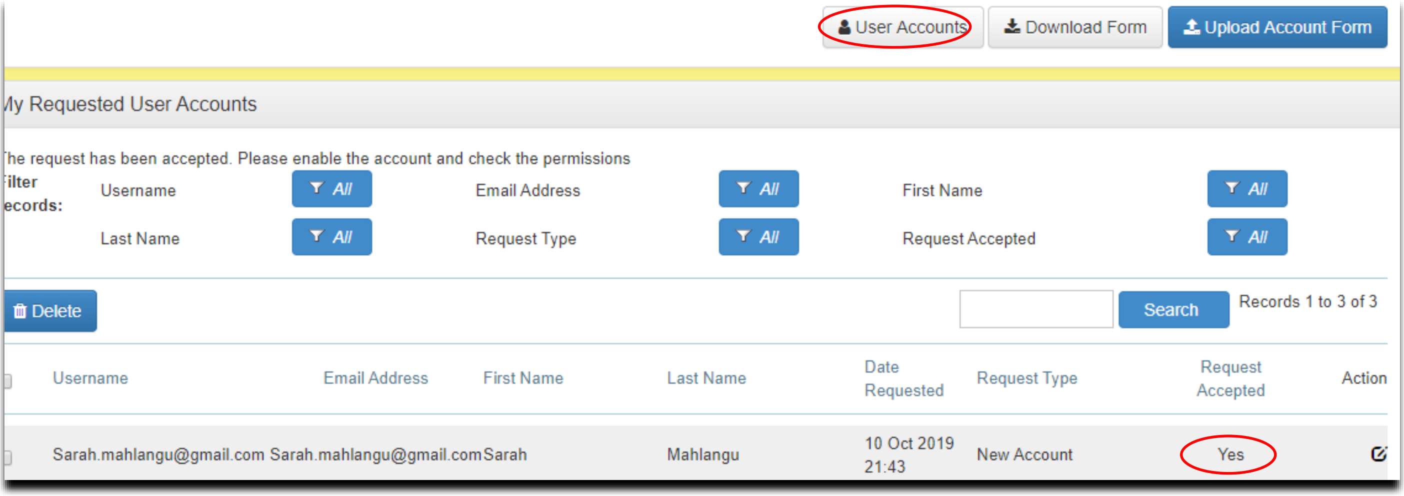


Figure 6: Action Request completed

9. If you want to delete a user account form that was uploaded so that the form no longer appears on the 'My Requested User Accounts' section, select the tick box next to the form that you want to delete, then select the 'Delete' button. See **Figure 7**.

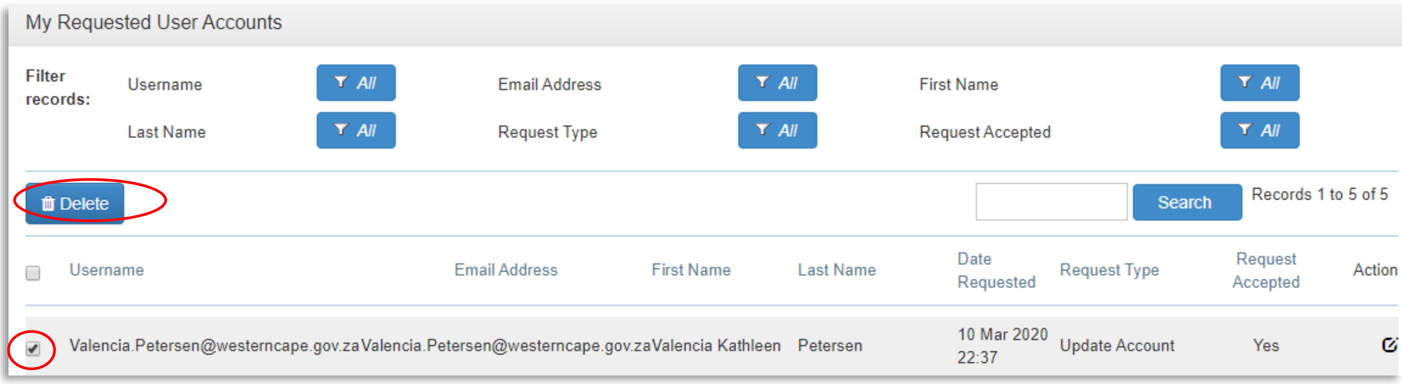


Figure 7: Delete and uploaded form

Note: When the user account is created the user's personal information on the user account form is automatically inserted on the information system and the roles selected on the user account form is also automatically ticked on the information system. The roles on the user account form must always correspond with the roles selected on the account. The account manager must however update the permissions manually by assigning a permission for every role that was selected (see **Section D**). Once the permissions were assigned, the login details must be sent (see **Section E**).

The e-mail address is used as the unique identifier for the user accounts, therefore once an account is created, the e-mail may not be changed/edited. If a user requests to use a different e-mail, the user must submit a new user account form. The user should also submit a second user account form to terminate the current user account (with the e-mail address that will no longer be used).

When Provincial/District account managers create user accounts for District user account managers, the section for 'Organisation' on the user account must be updated to reflect the district that the user is assigned to (to access the 'Organisation' section, double click on the account on the main user account screen where permissions are assigned, it's at the bottom of the screen). Therefore, once the form has been uploaded and accepted, correct the 'Organisation' section. If this is not corrected, the district account manager will not be able to view and access the user accounts for which forms were uploaded.

D. Assigning permissions

Roles have Permissions, i.e. is the organizational (Org) unit that is assigned that will allow the user access to a specific or multiple Org units. Permissions must be assigned to each Role after the user account form has been uploaded by selecting the Org unit for every Role. For example, if a user in the Western Cape is given a Role to view reports and their Permission is set to the Western Cape, they will be able to view all the reports for facilities in Western Cape.

1. Navigate to Setup > Accounts on the navigation bar at the top of the screen. See **Figure 8**.

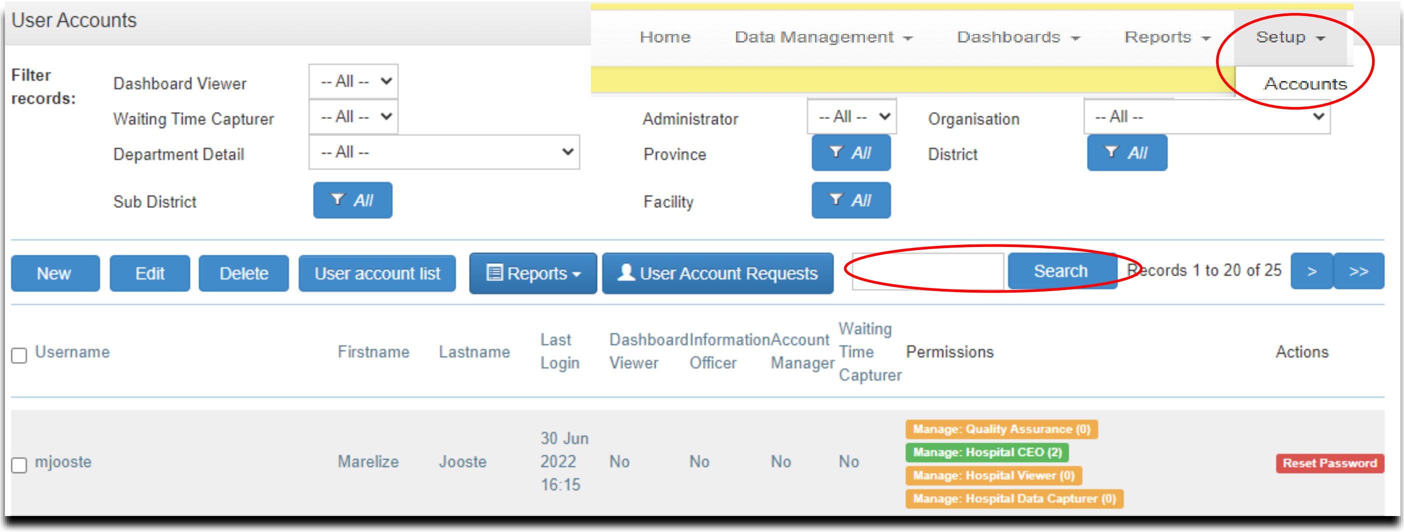


Figure 8 The User Accounts page.

2. To search for a user account, you want to assign permissions for, type the name/surname or username you want to edit in the box provided under the search function. Select the *Search* button. See **Figure 8**.
3. A list of names/surnames that you have typed in will appear.
4. For each Role that the user has been assigned (reminder that the roles are prepopulated according to the selecting that was made on the user account form that was uploaded), click on the Role name in the Permissions column for the Role you want to add a Permission for. Roles that have not been assigned Permissions is coloured amber while Roles where Permissions were assigned is coloured green. See **Figure 9.**

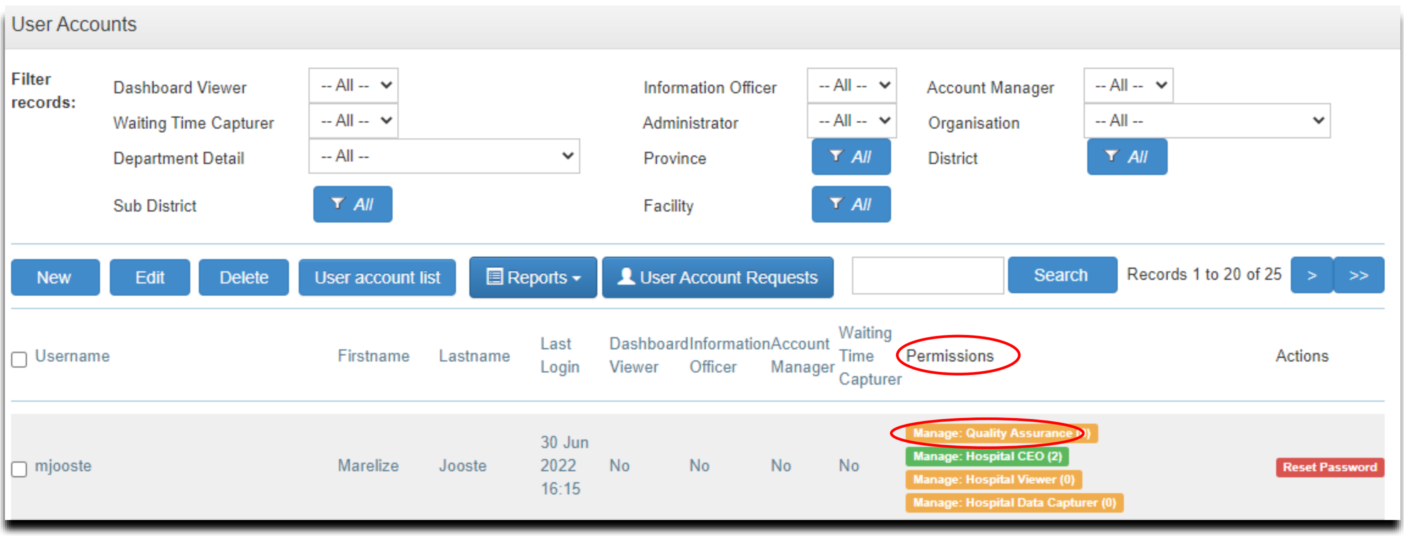


Figure 9: How to add Permission

5. The *Edit Account Permission screen* will open. In the Permissions screen, click on the *New* button. See **Figure 10**.

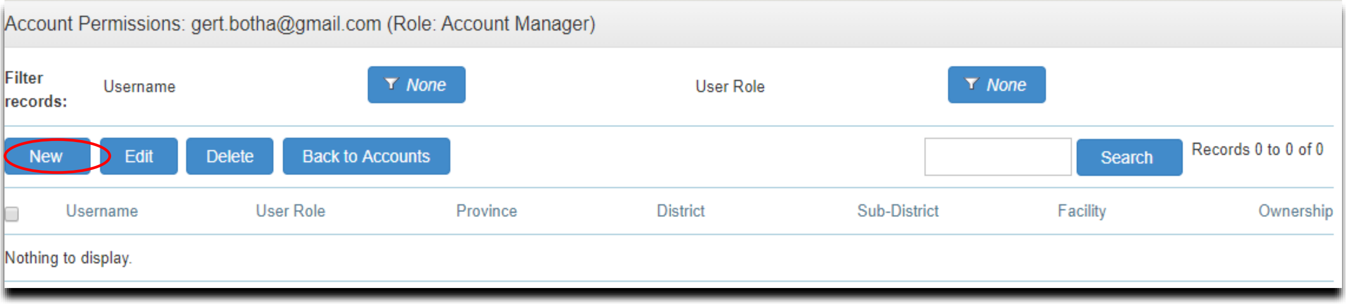


Figure 10: Add a new Permission

6. Assign the Permission to the user by entering (See **Figure 11**):
   i. Permission Level – Select the appropriate option
   ii. Structure – Search for the correct location by clicking on the magnifying glass. A pop-up screen will appear. Type the name of the facility/district/sub-district you want to add as a Permission in the *Search* box and select the *Search* button. Clinic the radio button next to the facility/district/sub-district you want to select and click in the *Select* button.
   iii. Ownership Type (only applicable to provinces that still has provincially and municipality owned facilities). By selecting for example, Gov, the user will only have access to facilities owned by the Provincial Department of Health.
   iv. Click *Save* in order to save the Permission.

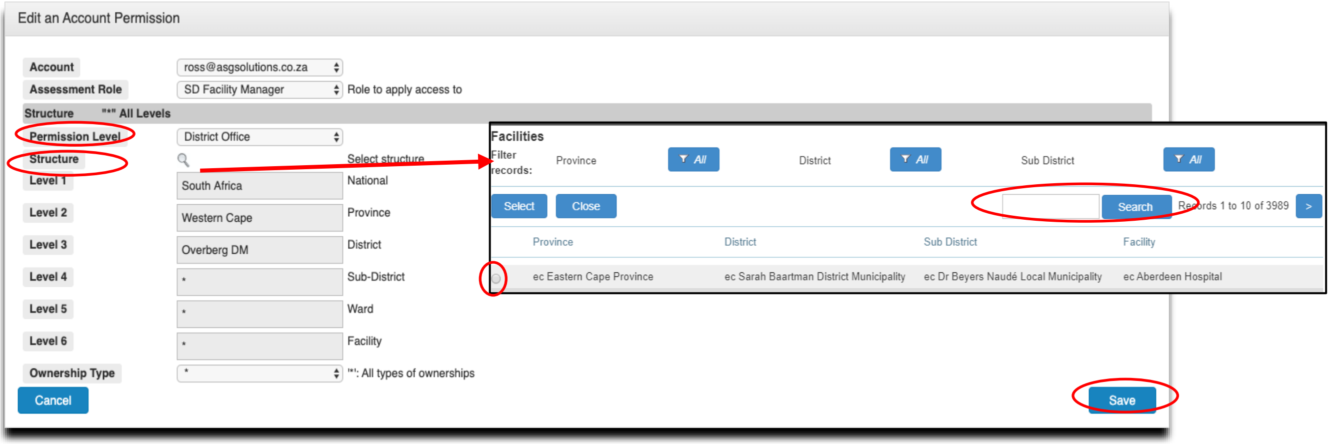


Figure 11: Assigning Permissions

Note the following when managing Permissions:

- You can add more than one Permission per Role, e.g. if a user requires access to three different health facilities. To add additional Permissions, just select the New button again, see **Figure 10**, and follow the steps to add another Permission.
- For PSI, CCS and Hospital Roles, the Permissions can be copied to other Roles if the user has more that one Role for that specific module. This is a short cut to avoid going through the entire process as outlined in **Figure 11**. For example, if a user has a Role for Hospital viewing reports and to capture. You can assign a Permission to the Role for Hospital Viewer. Once the Permission has been assigned a section will open below the Permission that will allow you to copy the Permission to the Role of Hospital Capture. To do this select the *Copy Permission* button. A pop-up message will appear requesting you to confirm the action. Select the *OK* button. The Permission assigned to the *Hospital Viewing* Role which is Aberdeen Hosp in the example in **Figure 12** will be copied to the Role for *Hospital Capture*.

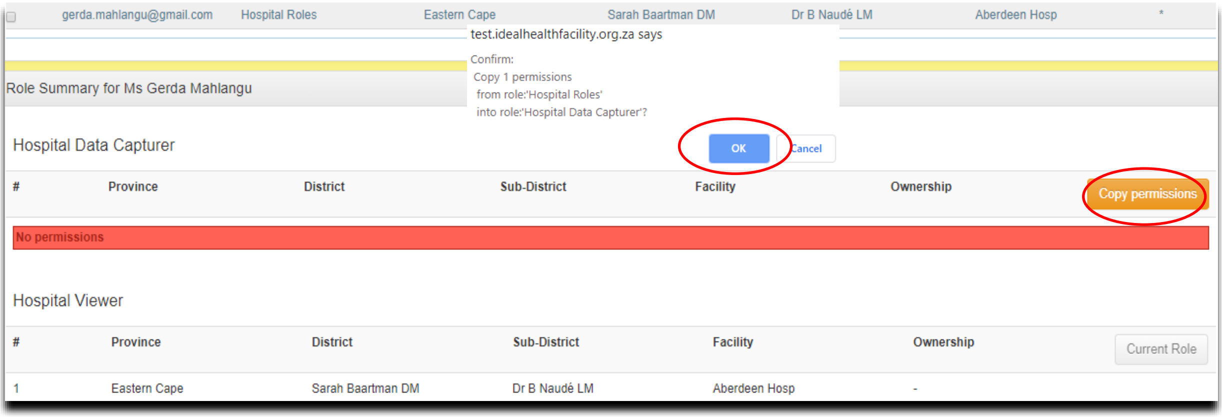


Figure 12: How to copy Permissions

A message will appear *1 Permission copied over into the Role: Hospital Data Capturer.* The *Hospital Data Capture* Role will now have the same Permission as the *View* Role. See **Figure 9**.

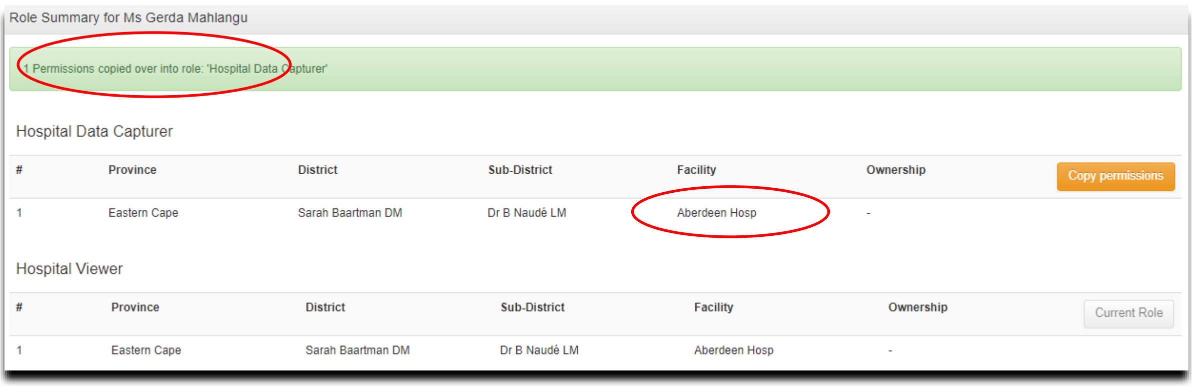


Figure 13: Copy Permission completed

- The Role to View Clinic reports – no Permission needs to be assigned as the system automatically assign viewing Permissions for the country.
- The Role for Facility Profiles and Waiting time - no Permissions need to be assigned as the Roles will automatically be assigned with the Permissions assigned to the Facility SD capture Role.

7. Repeat the process for each Role. **Every Role must have a Permission assigned to it**. The number of Permissions assigned for each Role is indicated in brackets next to the Role, see **Figure 9**. Roles that do not have a Permission assigned to it will not be available to the user to use.

Very important: All permissions assigned must correspond with the permissions as indicated on the user accounts form for the specific user. If it does not correspond, it will result in an audit query.

E. Send the account invitation with login details or reset a password

1. Once the permissions have been assigned, for new user accounts, **an account invitation must be sent**. The same processes apply if you want to reset a password of a user who has forgotten/lost their password. **Note**: When a password is reset, a new user account form must be completed and uploaded under the 'User Account Request section' and permissions must be assigned.
2. On the user account that you want to send an account invitation to, click on the red *Reset Password* button under the column named Actions.
3. The system will give a pop-up message to confirm that you want to send the password with login details. Select "OK". A message *Password Reset Successfully* will appear. See **Figure 14**.

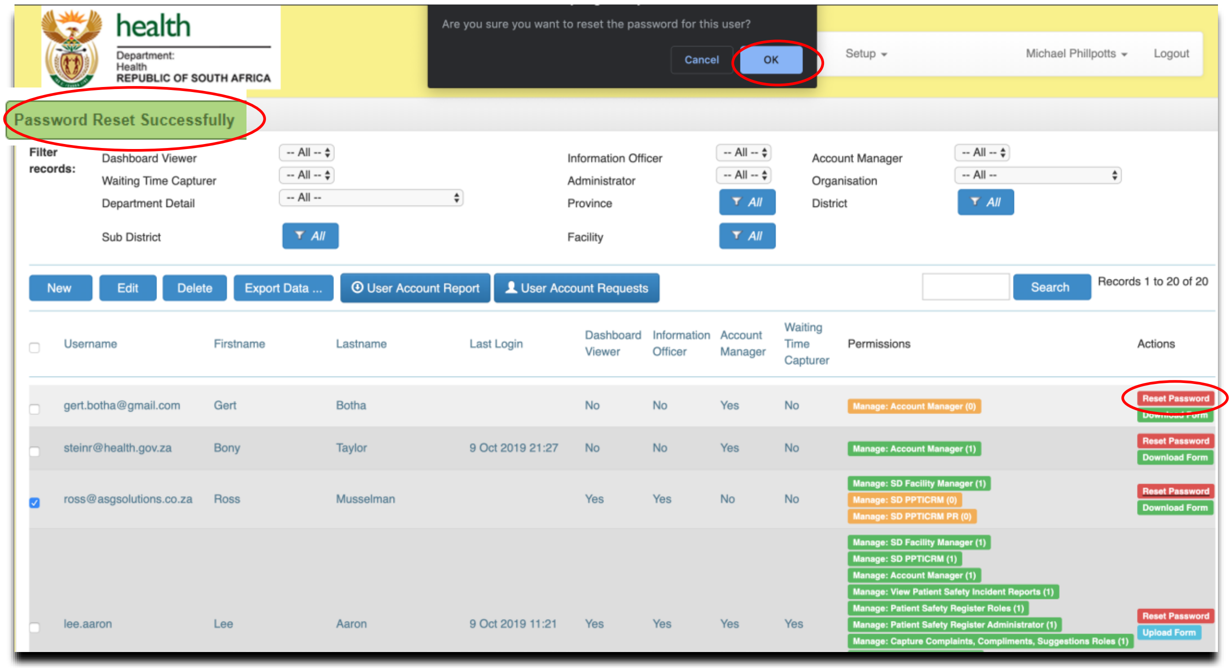


Figure 14: Reset password

4. An email will be sent to the user. The e-mail will contain their login credentials (account username and temporary password) and a link to the site. When they login, they will be prompted to reset their password. Note that user accounts that have not been accessed for three consecutive months are disabled. See section G to enable disabled user accounts. **Note:** A new user account form must then be completed and uploaded under the 'User Account Request section' and permissions must be assigned. The password configuration is as follow:

Password configuration	**Parameter**
Length and characters for password	8 characters, of which one is an uppercase letter, one lower case and one numerical number or special character
Password age	3 months
Password history	May not use previous 12 passwords
Lockout threshold	6

Users of the system may not share the passwords for their user accounts and the 'save password' option in web-browsers should not be activated when logging in. A security notice in this regard is also displayed on the login page of the website. Provincial Departments of Health must reiterate this when staff are trained in general security for information systems, and it should also be stated in the Provincial IT Security Policy/ Procedures and user account SOPs.

5. The Account Manager must inform the user via e-mail that his/her account has been created/updated and that login details were sent.

F. Retrieving user account forms (current and historic) for auditing purposes

1. The latest uploaded user account form can be downloaded from the main user account screen.
2. To download the existing registration form, click the *Download Form* button. See **Figure 15**.

Figure 15: Download the latest user account form

3. A PDF document will be downloaded to your preferred directory.
4. To retrieve historic (previous user account forms that were uploaded go the 'User Account Section. See **Figure 16**.

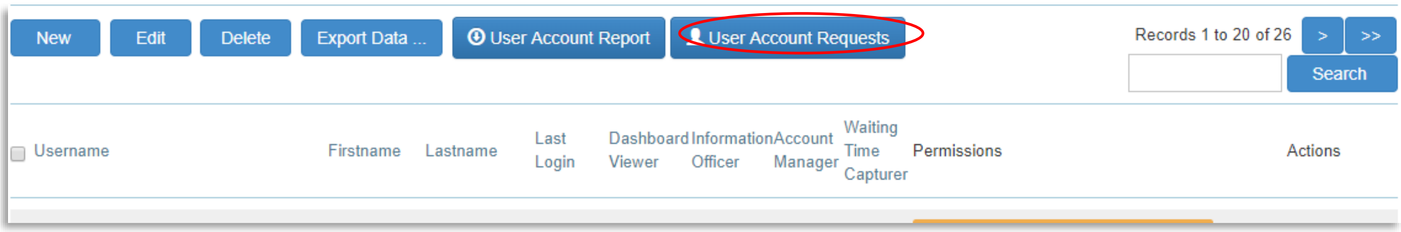


Figure 16: Navigation to 'User Account Requests'

5. To search for user account forms for a specific user, type the surname of the user in the text box next to the button named *Search*. Select the *Search* button. A list of all the user account forms for the specific user will appear. The time and date the form was uploaded will display. To download a form, select the icon with a pencil in. See **Figure 17**.

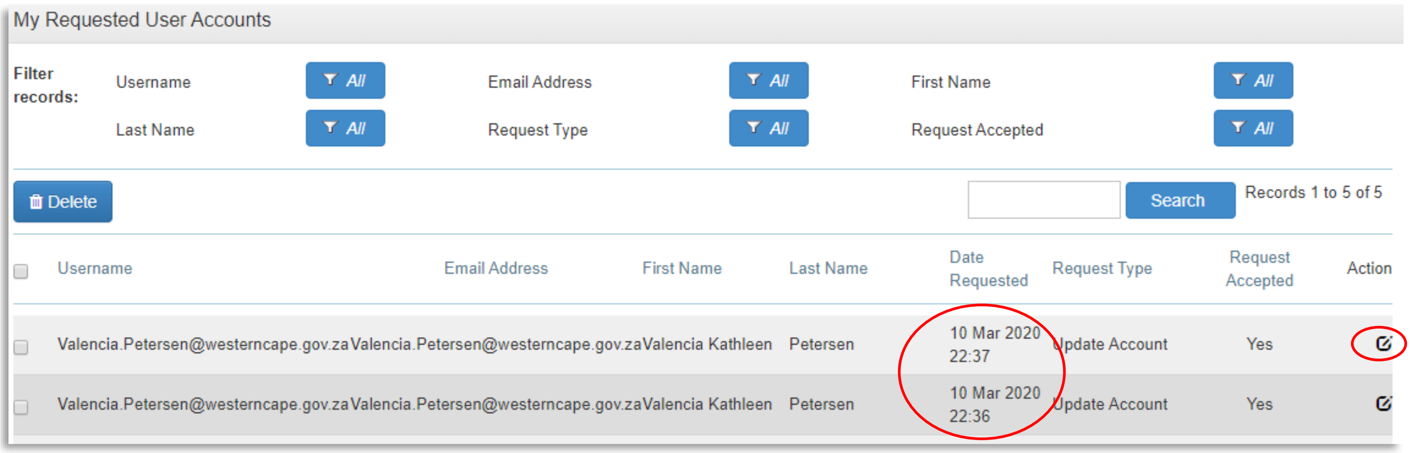


Figure 17: Download previously uploaded forms

6. A pop-up screen will appear. Select the icon for 'Download Form'. See **Figure 18**. The form will download in PDF format.

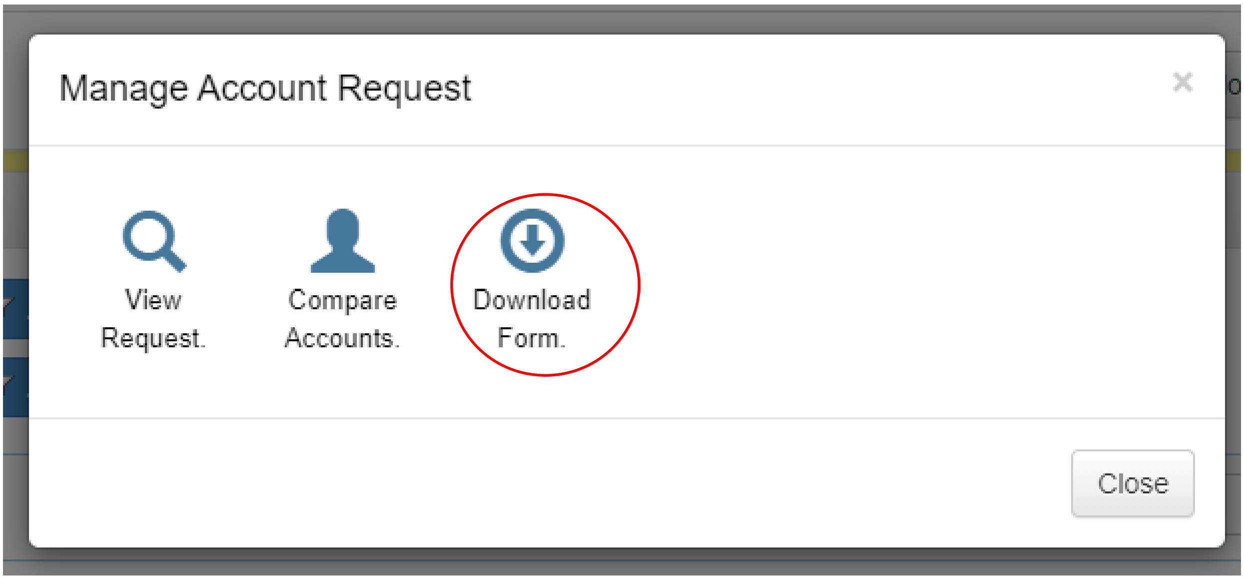


Figure 18: Icon to download previously uploaded forms

G. Enable a disabled user account

1. To enable (activate) a user account that have not been accessed for three consecutive months, go to the main user account screen. **Note**: A new user account form must then be completed and uploaded under the 'User Account Request section' and permissions must be assigned.
2. Type the name of the user account you want to enable in the search text box. Select the tick box next the user account you want to edit, then select the *Edit* button and do the changes (or just click on the user account name). See **Figure 19**.

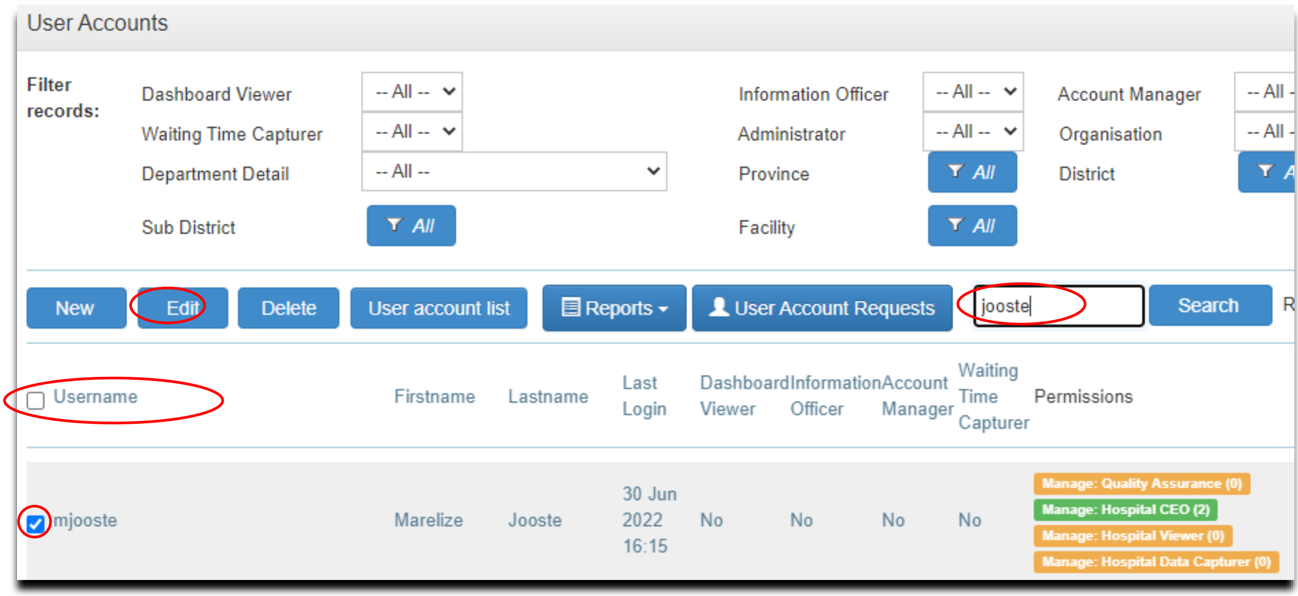


Figure 19: How to edit existing user accounts

3. The *Edit user account* screen will open. See **Figure 20**. You can enable a disabled user account by ticking the box next to *Enable*. Select the *Save* button.
4. An account invitation must now be sent, see **Section E**.

5. Note: the password that is sent only lasts 14 days, therefore it is important that they login to their account within 14 days after the new login details were sent.

Figure 20: Enable a disabled user account

H. Termination and deleting of user accounts

1. All staff that has left the service or staff that no longer require access to the information system, must complete a user account form and select the option for 'Termination' and enter the date of termination of the user account. Once a user account form is uploaded for staff that has terminated their service, the system uses the date of termination filled in on the form to insert the date of termination on the 'User Account List', see **Section I**. Note that the account must then also be disabled by unticking the box for 'Enabled', see **Section G, Figure 20**.

2. To delete a user account, select the tick box next the user account you want to delete. Select the *Delete* button. A pop-up message will appear to request to confirm the action. Select *OK.* A message will appear *1 record deleted*. See **Figure 21**.
Note that only user account that were incorrectly created should be deleted. The e-mail address of accounts that are deleted is stored at the back end of the information system, therefore the system will not allow you to use that e-mail again. Therefore make very sure before you delete an account. User account of staff that has left the service must be disabled and not deleted to ensure that there is an audit trail.

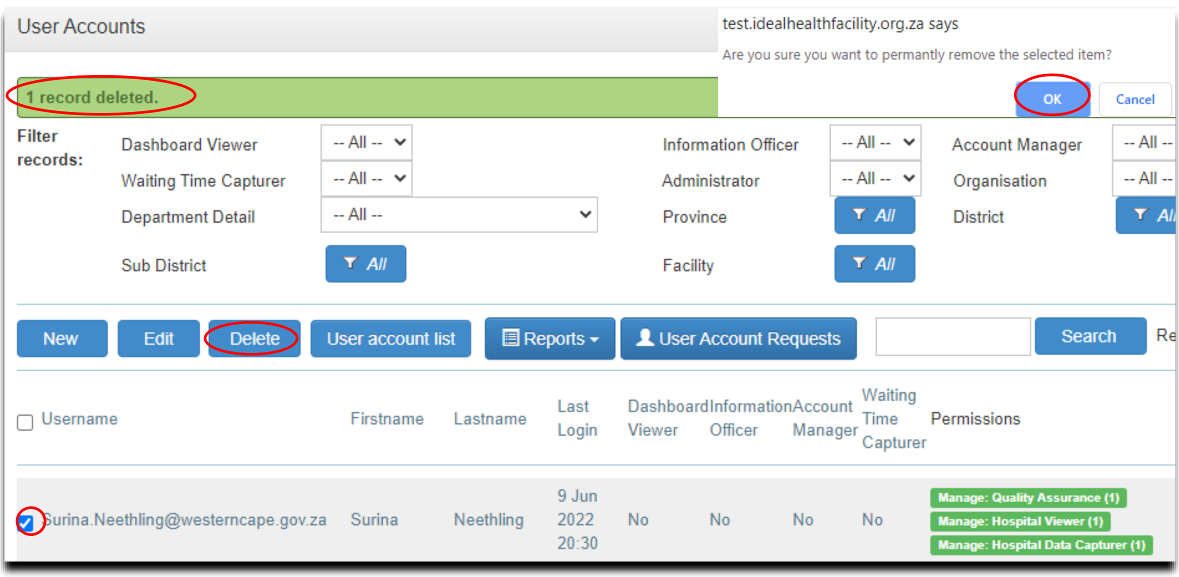


Figure 21: Delete a user account form the system

I. Generate a user account list and review user account access rights

1. All user accounts must be reviewed annually to ensure that user accounts that are enabled (active) have the correct user role and permissions and that the staff member must have access to those roles and permissions. The Province/District/Sub-District may schedule the reviews throughout the year to ensure that all districts are reviewed by the end of the financial year. The Provincial SOP should outline the schedule when each district will be reviewed.
2. To generate a list of all the user accounts, go to 'Setup', 'Account' and select the 'User Account List' button from the 'User Account' screen. See **Figure 22**.

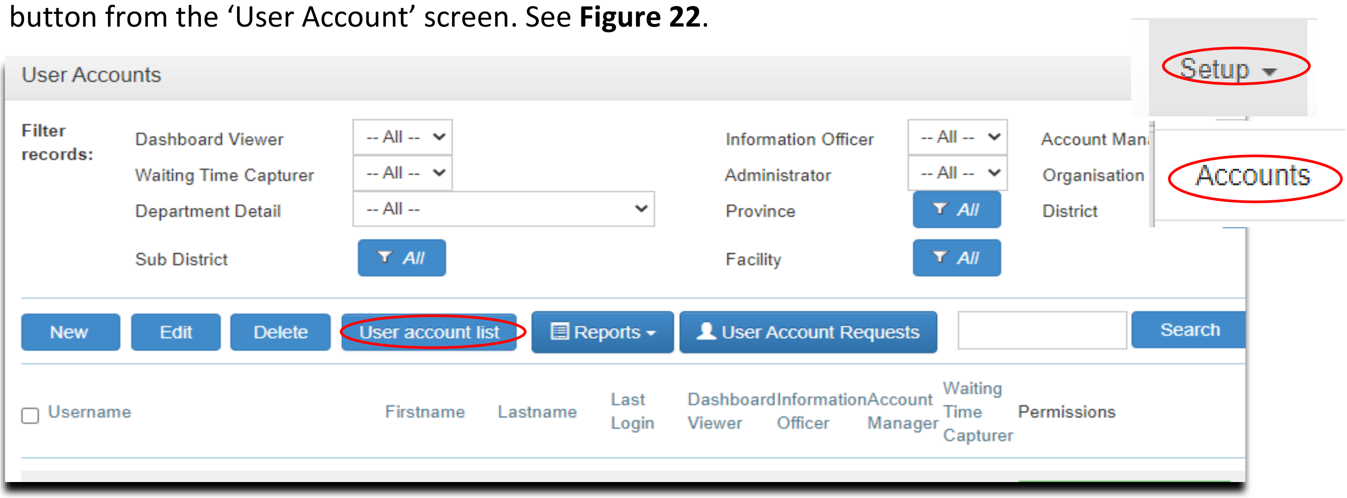


Figure 22: Export user account list

3. Note that the report has filters that you can be used to generate reports per district/sub-district/facility. Also note that only staff with an "Account Manager' role can generate the list and you will only be able to generate list for the province for which your account is registered. Select the *Generate Report* button. A report will appear in the *Schedule Report* section and a message will appear *Your request has started and is busy being proceeded….* Wait a few minutes while the system is busy generating the report and then select the *Refresh* button. Once the report has been downloaded a *Download* option will appear. Click on it to download the report. See **Figure 23**.

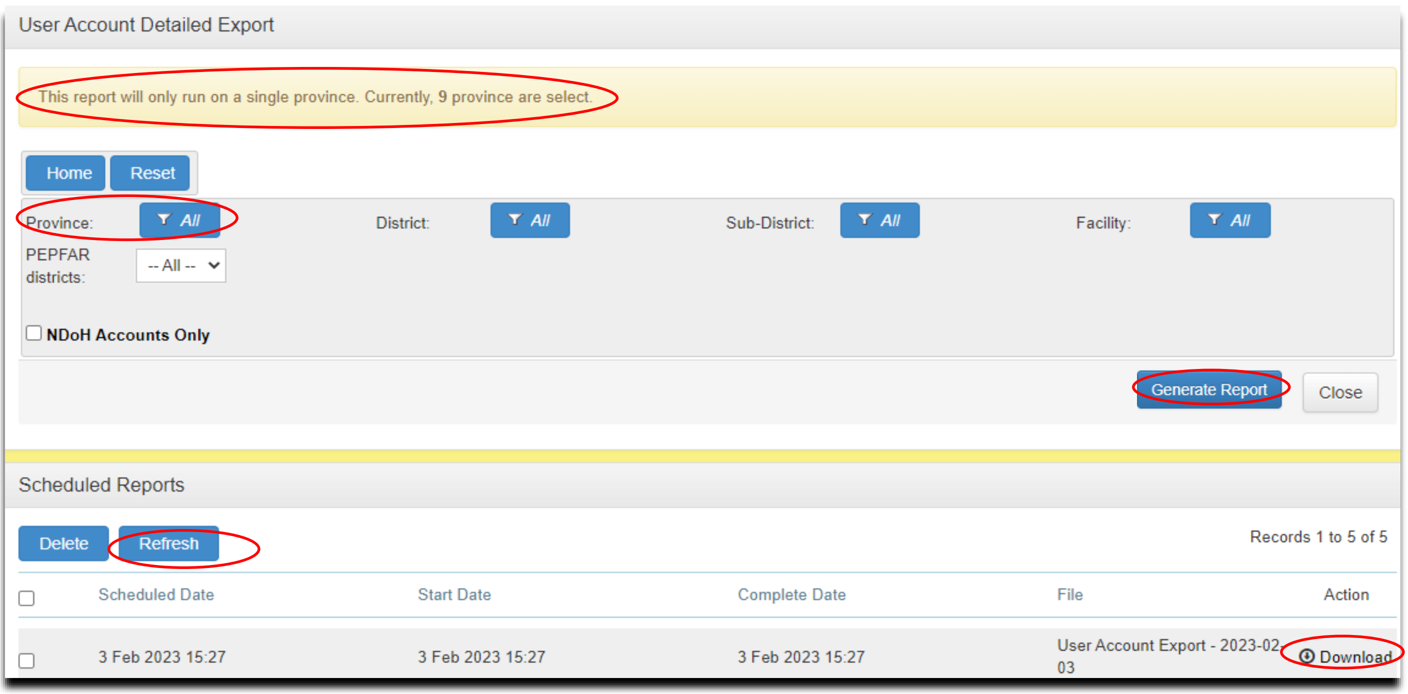


Figure 23: Generate user account list

4. The report contains a list of all the user accounts that are enabled (active) and disabled (not active) and detailed information about when the account was created/terminated, last login date, password age, and whether a user account form was uploaded. See **Figure 24**. Note that the report has an entry for every role and permission (org unit) for every user account, therefore an account for a user with multiple roles and permissions will appear more than once on the report.
5. To conduct an annual review of user accounts, remove from the list all the accounts that are disabled (mark with a 'No' in column H (Enabled) of the report (you can apply a filter on the column or sort the column and delete the disabled accounts). See **Figure 24.** Save the report (detailed user account list) as it must be attached to the 'User account review form, see **Annexure B,** that must be reviewed by the supervisors at facility/district level to review. Note that the form and the process described is an example that can be used. Provinces/districts may develop their own forms/processes that suites their context as long as the review is done (process to be described in provincial SOPs), signed off and documented evidence is filed.

health
Department: Health
REPUBLIC OF SOUTH AFRICA

Account Detailed Export

Date of Export 2023-02-03 15:26:42

Username	Firstname	Lastname	Email Address	ID Number	Employee Number	Enabled	Must Reset Password	Initial Date of Creation	Termination Date	Last Login Date	Password Last Reset Date	Current Password Age in Days	User Account Form Uploaded
TestAccount	Test	Account	ronel.steinhobel@			Yes	No	2019-11-18 17:17:31		2022-06-02			No
TestAccount	Test	Account	ronel.steinhobel@			Yes	No	2019-11-18 17:17:31		2022-06-02			No
TestAccount	Test	Account	ronel.steinhobel@			Yes	No	2019-11-18 17:17:31		2022-06-02			No
TestAccount	Test	Account	ronel.steinhobel@			Yes	No	2019-11-18 17:17:31		2022-06-02			No
TestAccount	Test	Account	ronel.steinhobel@			Yes	No	2019-11-18 17:17:31		2022-06-02			No
TestAccount	Test	Account	ronel.steinhobel@			Yes	No	2019-11-18 17:17:31		2022-06-02			No
TestAccount	Test	Account	ronel.steinhobel@			Yes	No	2019-11-18 17:17:31		2022-06-02			No
TestAccount	Test	Account	ronel.steinhobel@			Yes	No	2019-11-18 17:17:31		2022-06-02			No

Figure 24: User Account List Report

6. The 'User account review form', see **Annexure B**, serves as the sign off form for every district/sub-district/facility (this will depend on the process the province decides will work best). The 'User account review form' must be accompanied by:
   - A detailed list of all the user accounts, see section 5 above that explains how to generate a detailed user account list and remove the disabled account form the list, and,
   - the 'List of User Accounts to be reviewed form', see **Annexure C**. To compile the 'List of User Account to be reviewed', make a copy of the report that was generated in section 5 (detailed User Account List). Remove the user account names that appears more than once (as explained in section 4 the number of times an account appears depend on the number of roles/permissions assigned). Copy the 'User account name, Name, Surname, District, Sub-district, Facility name, and Account form uploaded' sections and paste it in the table in the 'List of User Accounts to be reviewed form' (**Annexure C)**.

7. Submit the 'Ideal Health Facility User Account Review Form' (**Annexure B**) with the accompanying 'List of User Account to be reviewed' (**Annexure C**) and the detailed user account list to every district/sub-district/facility with a request to complete it and return it to the System Administrator (Account Manager). Upon receipt of the form, review and do all the corrections as indicated in the column for comments on the 'List of User Account to be reviewed'. Once completed, sign off the 'Ideal Health Facility User Account Review Form' and submit a copy of the signed off form to the district/ sub-district/facility. Keep the signed off form in a file for auditing purposes.

J. Generate user account audit log for review of system administrator (account managers) account activities

1. A quarterly report must be generated for all user account activities that will serves as:
    a. a record for auditing purposes that details all account activities
    b. a record should there be any queries regarding user account activities

2. To generate a list of all user account activities, i.e. accounts created, roles and permissions added/changed, and password reset done, select the 'Audit log Report' button. See **Figure 25**.

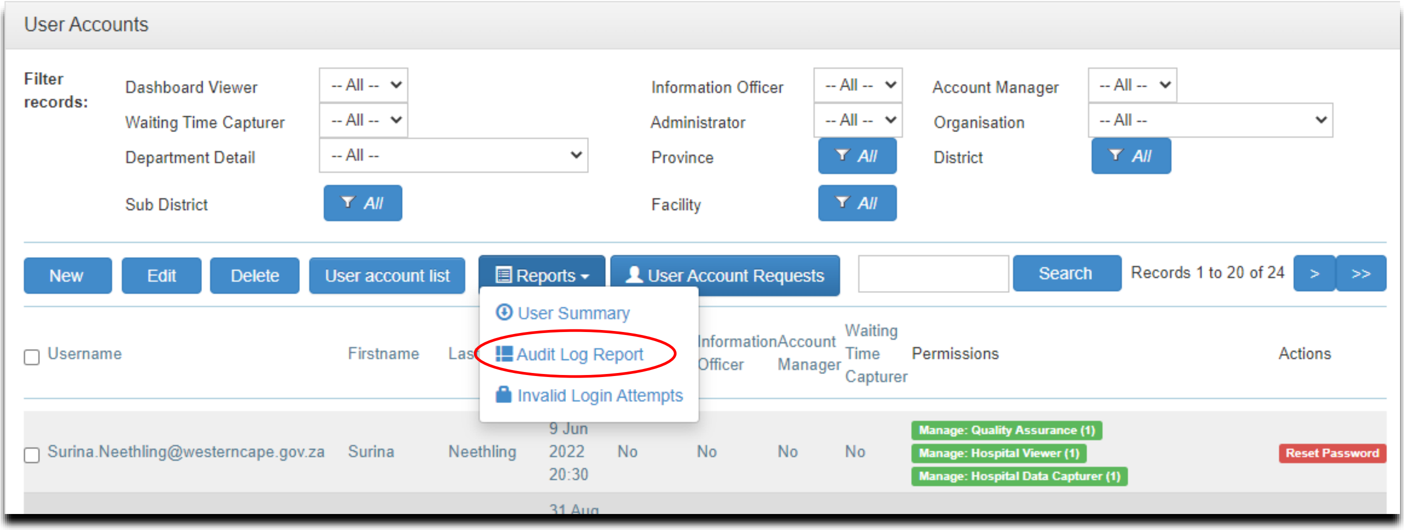


Figure 25: User account audit log

3. Select the 'Date Range' for the report by selecting the start date and end date. Select the 'Generate Report' button. **See Figure 26**. The report will be scheduled to generate.

Figure 26: Generate User Account audit log report

4. The report, see **Figure 27**, should be generated at the beginning of the next month following the end of a quarter and kept as a record of all user account activities executed for the quarter. The report must be

printed, signed off and filed. See **Annexure D** for an example of a sign off form that can be edited to suite the provincial context.

health

Account Audit Log Report

Date of Export: 2023-02-03 15:29

Province	District	Sub-District	Facility	Username	Name	Surname	ID Number	Employee Number	By Who	By Who Username	Action Type	Date	Fields Changed
wc Western Cape	wc City of Cape Tow	wc City of Cape Town	wc Groote Schuur	mjooste	Marelize	Jooste			Michael Phillpot	admin	Update	2022-06-27 14:39:11.00	pprticr, pprticr_pr, pprticr_pru, organisa
wc Western Cape	wc City of Cape Tow	wc City of Cape Town	wc Groote Schuur	mjooste	Marelize	Jooste			Michael Phillpot	admin	Create	2022-06-27 14:31:33.00	role_api_qip, expunged, file_id, place
wc Western Cape	wc City of Cape Tow	wc City of Cape Town	wc Groote Schuur	TestAccount	Test	Account			Michael Phillpot	admin	Update	2022-06-02 16:53:47.00	password, date_updated
wc Western Cape	wc City of Cape Tow	wc City of Cape Town	wc Groote Schuur	TestAccount	Test	Account			Michael Phillpot	admin	Update	2022-06-02 16:52:32.00	role_hospital_viewer, role_data_captu
wc Western Cape	wc City of Cape Tow	wc City of Cape Town	wc Groote Schuur	Valencia.Peters	Valencia K	Petersen	850620006408	54247594	Ronel Steinhobe	rsteinhobel	Delete	2022-05-19 07:37:39.00	type, username, password, lastlogin, e
wc Western Cape	wc City of Cape Tow	wc City of Cape Town	wc Groote Schuur	Valencia.Peters	Valencia K	Petersen	850620006408	54247594	Ronel Steinhobe	rsteinhobel	Update	2022-05-19 07:37:39.00	enabled, date_updated, last_updated

Figure 27: Audit log report

K. Generate a summary of number user accounts per Province/District

1. To generate a list that sets out the number of enabled user accounts per Province/District, select the button named 'User Summary'. See **Figure 28**.

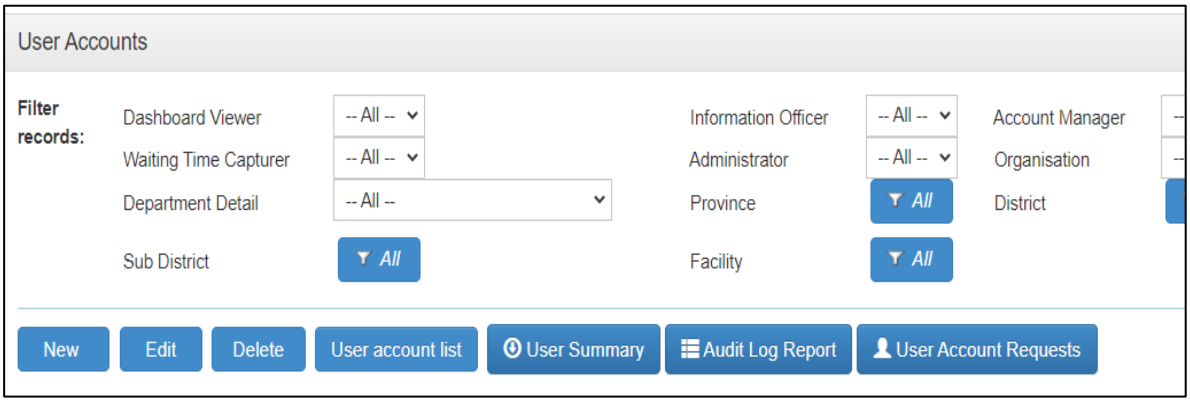


Figure 28: Generate summary of number of enabled user accounts

2. The report will generate at the bottom of the page, see **Figure 29**.

health

Department:
Health
REPUBLIC OF SOUTH AFRICA

Ideal Clinic Monitoring

Number of enabled user accounts

Province	District	# Accounts
ec Eastern Cape Province		560
	Provincial Office	98
	ec Alfred Nzo District Municipality	116
	ec Amathole District Municipality	90
	ec Buffalo City Metropolitan Municipality	46
	ec Chris Hani District Municipality	71
	ec Joe Gqabi District Municipality	19
	ec Nelson Mandela Bay Municipality	23
	ec Oliver Tambo District Municipality	52
	ec Sarah Baartman District Municipality	45
fs Free State Province		358

Figure 29: Report for number of enabled accounts

Annexure A: User account request form

health
Department:
Health
REPUBLIC OF SOUTH AFRICA

Ideal Health Facility - User Registration Form

All existing users of the web Ideal Health Facility Information System (WIHFIS) that have not previously completed this form must complete it. Thereafter existing users that want to change/edit their previously assigned permissions, must also complete this registration form, only indicating changes/additions. Kindly complete the required user information and upload the form onto the WIHFIS system. ONLY after signoff and approval, will the user be created or edited.

* fields are Compulsory Information that must be completed.

TYPE OF REQUEST (Tick where applicable)		
• New users must tick the 'New User' box. • Existing users must tick the 'Existing User' box AND specify what type of change to the user account is required e.g. Orgunit, user role, permission set, password reset. • If Termination box is ticked, provide the termination date. *	New User	☐
	Existing User	☐
	Password reset/account reactivation	☐
	Change/addition of user role	☐
	Change of Organisational Units Access	☐
	Termination	☐
	Termination Date:	

Personal Details	
First Name (in full) *	
Surname (in full) *	
Email Address *	
Position (eg. Data Capturer, Information Officer, deputy director, CEO etc.) *	
Place of employment *	
ID Number *	
PERSAL/Employee Number *	
Work/Cell Phone Number (eg.082 123 1234)	

User Roles and Permissions			
Module	**Role**	Specify the Orgunit Parent by entering **the NAME of the** province/district/sub-district/ facility **the user requires access** to for this role. The user will have access to this org unit and all its children. If a role is left blank, it will not be added to the account	**Date Requested**
Ideal Clinic	View reports		
	Capture Facility SD		
	Capture PPTICRM SD		
	Capture PR SD		
	Capture PRU SD		
	Capture waiting time		
	Capture facility profile		
Ideal Hospital	View reports		
	Data capturer		
	Authorise QA		
	Authorise CEO		
Patient Safety Incidents (PSI)	View reports		
	Capture PSI		
	Data controller		
	Notifications contact manager		
Complaints, compliments and suggestions (CCS)	View reports		
	Capture		
	Data controller		
General	Account Manager		

Authorisation			
User's authorisation			
Date of user's signature *		User's signature *	
Manager's authorisation			
Manager's name *		Manager's surname *	
Manager's position *		Manager's contact number	
Date of manager's signature *		Manager's signature *	

* is required fields

GUIDANCE TO COMPLETE THE USER REGISTRATION FORM:

1. Complete all the fields marked with an asterisk.
2. Description of the function of the Roles for user accounts:
   - **a. All roles:**
     - i. Role for Viewing will allow the user to generate reports.
     - ii. Role for Capturing will allow the user to capture data.
   - **b. PSI and CCS:**
     - i. Role for Data Controller for PSI and CCS will allow the user to open closed PSIs/CCSs and to deleted closed/open PSI/CCSs.
     - ii. Notification contact manager will allow the user to add an option for a user to receive notifications via e-mail once a SAC1 PSI has been recorded on the WIHFIS. Note: the user for which a notification role has been added must have an existing PSI user account.
   - **c. Ideal Hospital:**
     - i. Role for Authorise QA will allow the user to authorise data captured by the data capturer and the user can also capture data.
     - ii. Role to Authorise CEO will allow the user to approve captured data for Ideal Hospital. NB: a user with this role will not be able to capture data.
     - iii. All three roles cannot be assigned to one user, these are the following combinations that can be assigned:
       - ✓ Data capturer
       - ✓ Data capturer and Authorise QA
       - ✓ Authorise CEO
   - d. **General: Account Manager will allow the user to assign a role to a user to allow them to create user accounts for other users to access the WIHFIS.**
3. For the field named *Specify the Orgunit Parent*, note the following:
   - a. If the user requires access for **all the facilities within the province**, note down only the name of the province only.
   - b. If the user requires access for **all the facilities within a district/sub-district**, note down only the name of the district/sub-district that the user requires access for.

     Note: For PSI and CCS, if a district/sub-district is selected, the user will have access to all the clinics, CHCs and district hospitals within that district/sub-district. If the user requires access for Regional, Provincial and Central hospitals within the specified district, the names of those hospitals must be noted down as separate facility names.
   - c. If the user requires access **for more than one facility**, write down the names of all the facilities that the user requires access for.
4. For the field named *Date Requested*: write down the date for which the role/permission is requested.

   Note: if the user has been assigned roles/permissions, the dates of the previous permissions roles requested must alsobe noted down.

Annexure B: User account review form

Ideal Health Facility User Account Review Form

Province: _______________

District/Sub-district/facility: _______________________

Financial year: ______________

Instruction for district/sub-district/facility to complete the form:

- Please review the attached detailed user account list that details the roles and permissions for every user that has an account that is enabled.
- Verify that the account information is correct for every user by signing in the designated column on the ''List of user account to be reviewed form'. If the account is not correct, sign and indicate the action to be taken for the account in the column provided for comments.

Please return the completed form to (e-mail address) _____________________by (Date)______________

Section to be completed by System Administrator (Account Manager) and Supervisor of System Administrator (Account Manager):

I (User account manager/Administrator) ______________________ have reviewed the form and made corrections on the Ideal Health Facility web-based information system where indicate/if indicated.

Signature: _______________________

Date: _____________

Verified by Supervisor of System Administrator (Account Manager):

Name and surname: ________________________

Signature: _____________________

Date: _____________________

Annexure C: List of user accounts to be reviewed form

User account name	Name	Surname	District	Sub-district	Facility Name	Account form uploaded	Sign off by Supervisor (Facility manager/ District manager)	Comments

Annexure D: Cover sign off page for user account activity log

User Account Activity Log Form for Ideal Health Facility Information System

User account activity log for Quarter _______________ 20______

Generated on ___________________

Generated by System Administrator/Account Manager:

Name______________ Surname_________________

Designation_____________

Signature___________________

Date: _____________________

Verified by Supervisor of System Administrator (Account Manager):

Name and surname: ________________________

Signature: _____________________

Date: _____________________