Sign-on Guide for the .amsterdam DRS

For Registrar Users and Registrar Admin Users

Contact
T +31 26 352 5500
support@sidn.nl
www.sidn.nl

Office
Meander 501
6825 MD Arnhem
The Netherlands

Mailing address
Postbus 5022
6802 EA Arnhem
The Netherlands

Client
SIDN

Project number

Page
1/16

Project Manager
SIDN

Classification
Public

Status
Final

Date
29 August 2022

Author
SIDN

Contents

1 Quick guide for all users

To sign on to SIDN's systems, you need a username and password, which you can get from your organisation's Registrar Admin.

Two-factor authentication

Access to our systems is controlled using two-factor authentication (2FA). In other words, to sign on you need your username-password combination, plus a second authentication factor.
We currently support the following second-factor options:

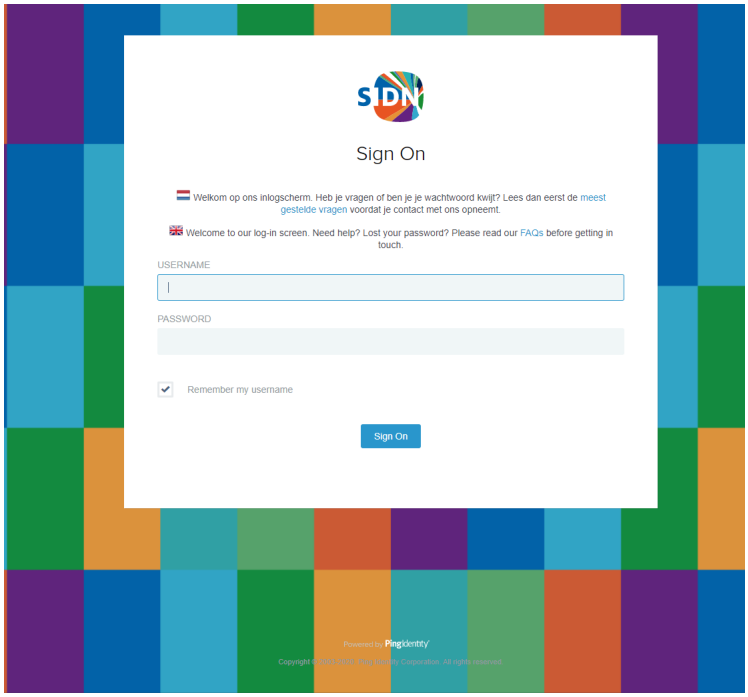
- The PingID app
- The Google Authenticator app
- SMS (mobile phone text message)

When you sign on to our systems for the first time, you are prompted to reset your password and set up 2FA. Once you've done that, you can proceed to use our systems.

1.1 Signing on for the first time

Here's how you sign on for the first time:

1. Open an internet browser and go to https://portal.sidn.nl.
2. Enter your username and password, then click 'Sign On'.



3. When you sign on for the first time, or if your password has been changed, you are immediately prompted to reset your password. See also 1.2 Resetting your password when you sign on for the first time.

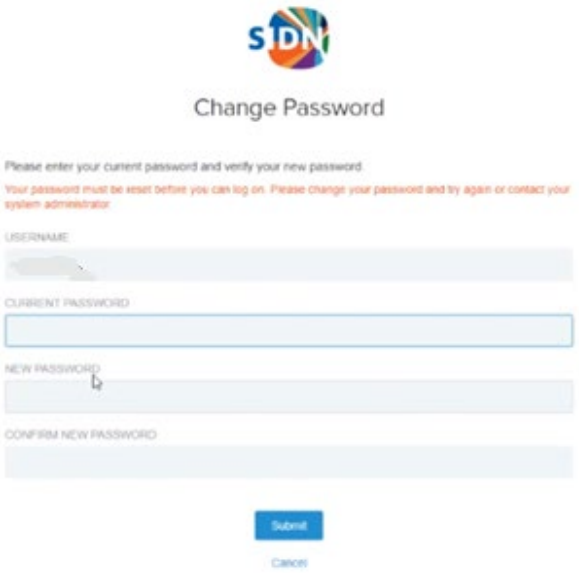
4. Next, you are asked to set up 2FA. You can choose from:
    - PingID
    - Google Authenticator
    - SMS

    See also 1.3 Setting up 2FA when you sign on for the first time.
5. Once you've successfully set up 2FA, the application page should open, showing the applications available for you to use.
   Are some applications missing? If so, please contact your organisation's Registrar Admin.
   Clicking an application tile gives you immediate access, without the need to sign on to the individual application.
6. Finished? Simply sign off from the portal. That will sign you out of all the individual applications at once. See also 1.5 Signing off.
7. After you have successfully signed on and off again once, all subsequent sign-ons will be on the basis of 2FA. In other words, you'll sign on to the portal using your username and password, plus a mobile phone-based second authentication factor. See also 1.4 Signing on.

Various aspects of the process outlined above are considered more closely in the following subsections.

1.2 Resetting your password when you sign on for the first time

When you successfully sign on to the SIDN Portal for the first time, you are immediately prompted to reset the password initially assigned to you.

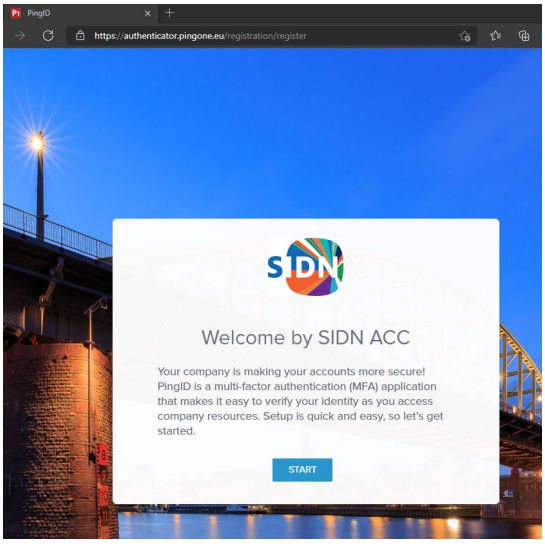


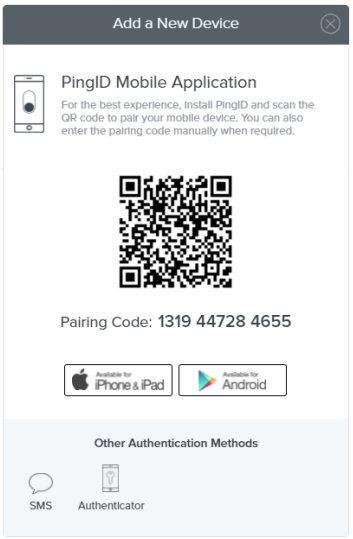
An immediate password reset ensures that no one except you knows your password. Follow the instructions on the screen.

1.3 Setting up 2FA when you sign on for the first time

Your organisation's Registrar Admin will give you a username and password so that you can start using our systems. You'll need to use that username and password to sign on to our portal for the first

time, as described in **1.1 Signing on for the first time**. Once you've successfully entered your username and password, you'll be prompted to set up 2FA. Click 'Start' to begin the set-up procedure for PingID, Google Authenticator or SMS.
The default option (offering the strongest security) is PingID (see **1.3.1 Using PingID for 2FA**). However, if you prefer, you can use Google Authenticator or SMS instead (see **1.3.2 Using Google Authenticator for 2FA** and **1.3.3 Using SMS for 2FA**, respectively). Simply select your preferred option on the following screen.

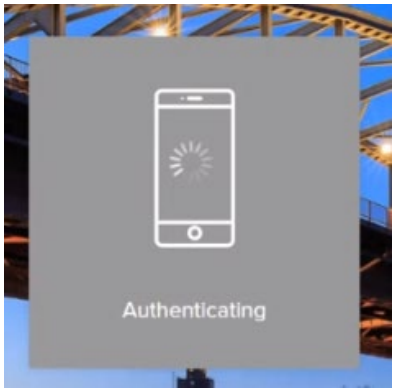


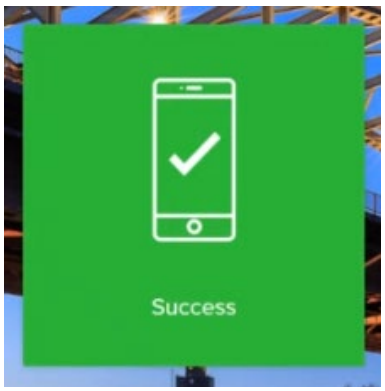


Set-up 1PingID (iPhone or Android)

1.3.1 Using PingID for 2FA

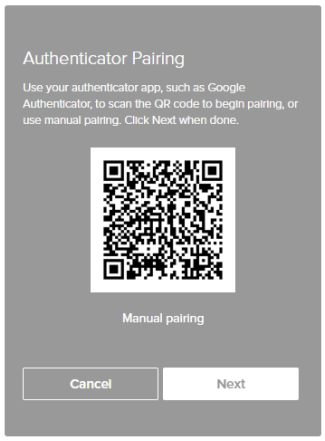
The default 2FA option is the PingID app, which we believe offers the strongest security. The app is available from the App Store and the Play Store. Instal and open the PingID app, then use it to scan the QR code shown on your computer screen.
The PingID app will then prompt you to approve a sign-on request. Depending on the capabilities of your smartphone, you'll be able to approve the sign-on by fingerprint scanning, facial recognition, swiping or clicking 'OK'. Once you've approved the sign-on, your 2FA is all set up.





1.3.2 Using Google Authenticator for 2FA

If you prefer, you can set up 2FA using the **Google Authenticator** app. The app is available from the App Store and the Play Store. Setting up Google Authenticator access is possible only if you selected Google Authenticator earlier in the 2FA set-up process. See **1.3 Setting up 2FA when you sign on for the first time**.

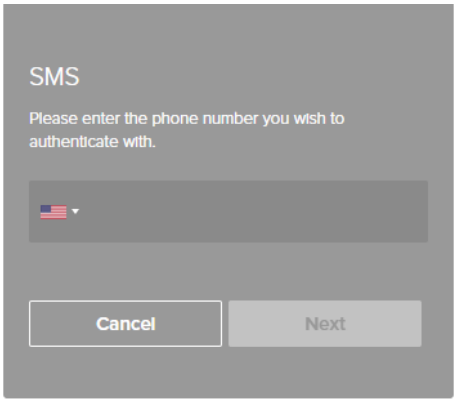


Set-up 2 Google Authenticator

Open the Google Authenticator app on your smartphone and use it to scan the QR code on your computer screen. The app will then show an entry labelled 'SIDN', containing a code. Go back to your computer and click 'Next'. You will then be prompted to authenticate yourself again by entering the code shown in the Google Authenticator. Once you've entered the correct code, your 2FA is all set up.

1.3.3 Using SMS for 2FA

The third, but least secure, 2FA option is to use codes sent to your mobile phone by SMS ('text message'). We advise using this option only if you don't have access to a smartphone that will support PingID or Google Authenticator.
To set up SMS-based 2FA, you first select the country where your mobile number is registered, then you enter your phone number (without the country code). Once the number has been validated, click 'Next'.



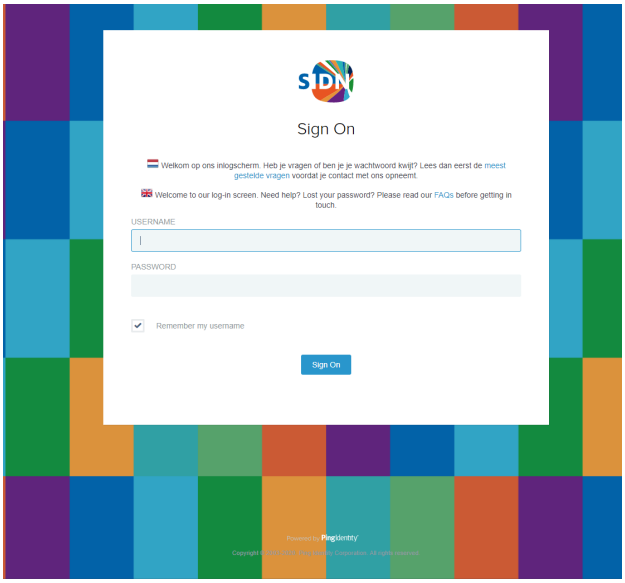
Set-up 3 SMS to a registered phone number

You will then be prompted to authenticate yourself again by entering the code sent to your mobile by SMS. Once you've entered the correct code, your 2FA is all set up.

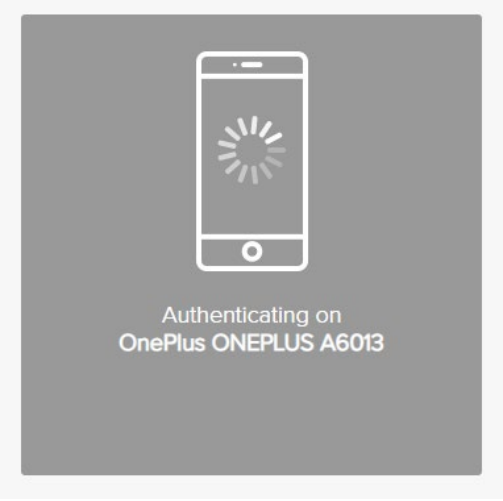
1.4 Signing on

To access the SIDN Portal, first enter the following URL into your browser: https://portal.sidn.nl.

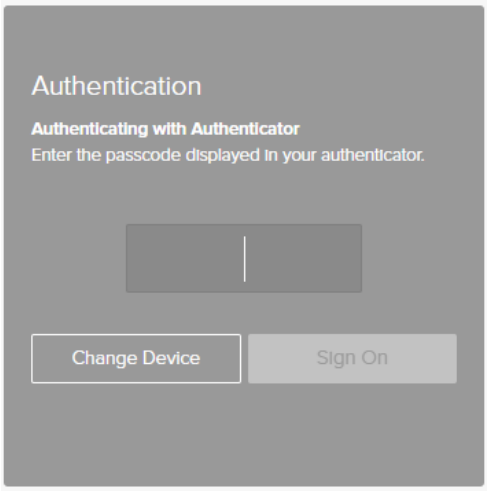
The following sign-on screen will then appear.



Enter your username and password. Depending on which 2FA option you previously set up, you may get a notification from the PingID app on your smartphone, or you may be asked to enter a code: either as shown in the Google Authenticator app or as sent to your mobile by SMS. One of the following screens will appear:

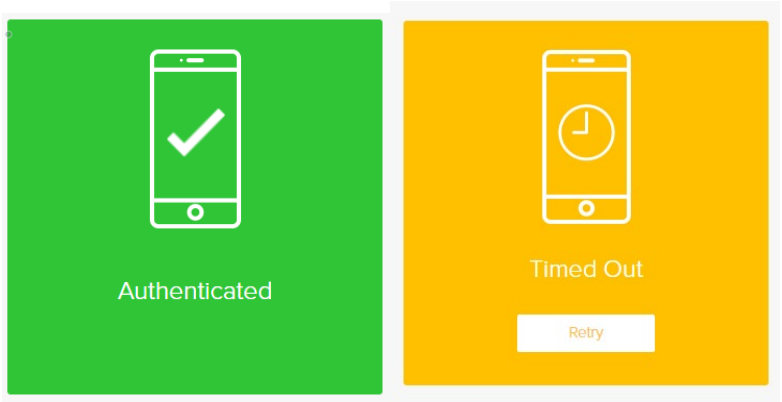


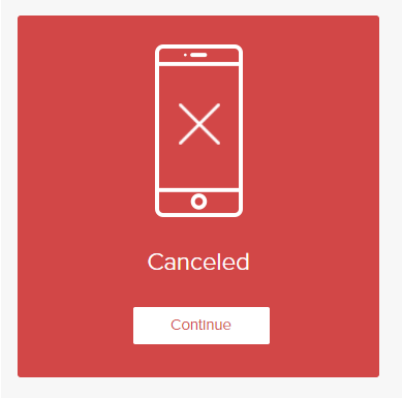
PingID



Google Authenticator

Open PingID or Google Authenticator on your smartphone and either confirm the sign-on using your fingerprint or enter the access code on the browser screen and click 'Sign On'. (The procedure depends on the brand and model of your smartphone.)



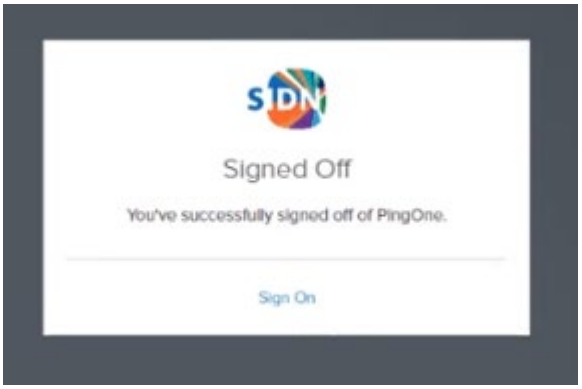


You have a window of a few minutes to respond. If you don't respond quickly enough, you'll need to start a fresh sign-on. Once the second authentication factor has been successfully processed, you'll be signed on to the central SIDN Portal. Your name should then be visible at the top of the screen, on the right. In the main part of the screen, you'll see tiles for the available applications. Exactly what you see will depend on your access rights, but the screen will look something like this:

1.5 Signing off

If you click the user icon next to your name, a menu drops down.

Select 'Sign Off' to sign yourself out of all the applications you have accessed from the central SIDN Portal ('single sign-off').



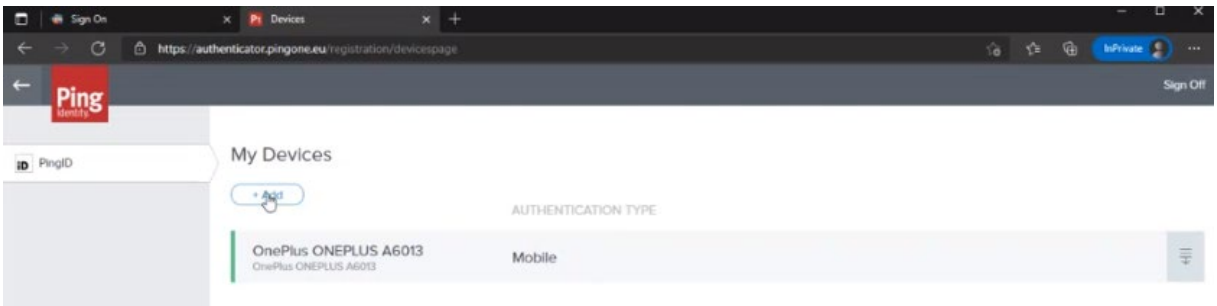
1.6 Changing the device you use for 2FA

The screen grabs in this subsection feature the start screen that a Registrar User sees when signed on. The exact appearance of the screen depends on the individual user's rights. Some users see more applications than others.

If you click the icon next to your name, a menu drops down, with three options:

- Devices
- Help
- Sign Off

If you select 'Devices', the 'My Devices' page opens, showing the device currently set up for 2FA.



You switch devices as follows:

1. Click 'Add'.
2. Delink your old device.
3. Link your new device.
4. Sign out of the SIDN Portal.
5. Sign back on and follow the instructions in 1.3 Setting up 2FA when you sign on for the first time.
6. You can then go back to 'Devices' and delete your old device.

At present, up to two devices can be listed on the My Devices page, one of which is defined as your primary device. To make sure you don't lose access, we recommend setting up two devices, in case one gets lost or broken.

Note:
In order to set up a new 2FA device, you need access to your existing device because you can't sign on without it. If you don't have your old device any more, please contact SIDN's Support Department by mailing support@sidn.nl.

2 Quick guide for Registrar Admin Users

The central SIDN Portal supports several user types, each with its own rights, corresponding to various management levels. For Registrar Admin Users, two types are important: the Registrar Admin User themselves and the Registrar Users within the relevant Registrar (organisation).

Registrars (organisations) and Registrar Admin Users are created on the system on SIDN's behalf by SIDN Admin Users (the third type of user), who also assign rights to the Registrar Admin Users.

2.1 Registrar Admin Users

A Registrar Admin User currently sees the following start screen. Exactly what you see will depend on your access rights, but the screen will look something like this:

A Registrar Admin User can manage only the Registrar Users within their own Registrar (organisation).
At the moment, a Registrar Admin User has access to the following two applications:

- RegistrarSite: the operational SIDN application that you click on for access.
- SIDN usermanagement, for managing the following within your own Registrar (organisation):
    - Registrar Users
    - Group Memberships (assignment of application groups)

A Registrar Admin User can perform management tasks for their own Registrar (organisation), such as creating Registrar Users and defining Group Memberships (assigning application groups) for Registrar Users.

2.2 Registrar Users

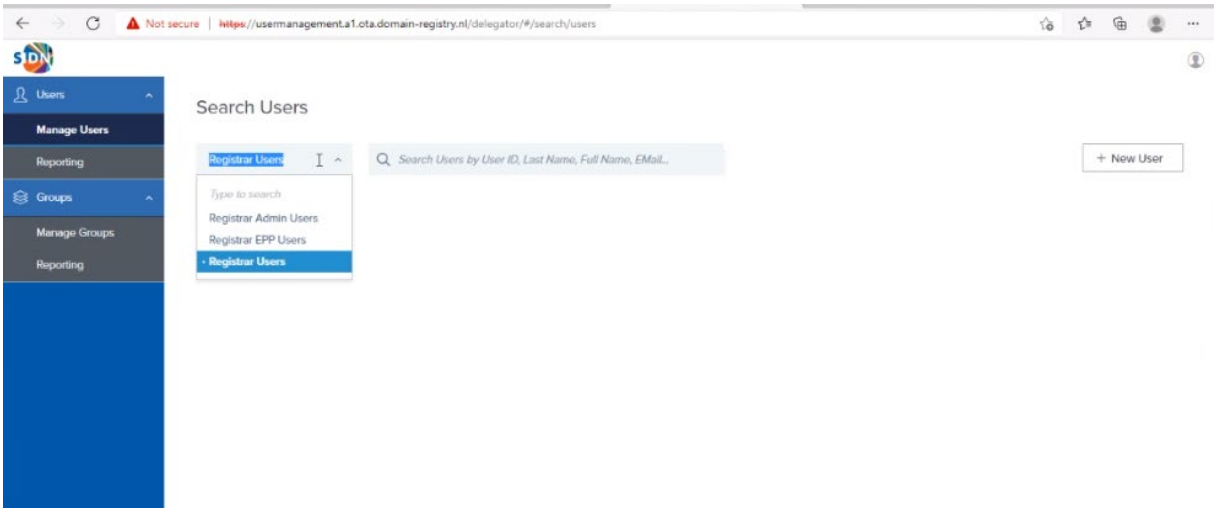
A Registrar User's start screen currently features only one application: RegistrarSite. Exactly what you see will depend on your access rights, but the screen will look something like this:

Registrar Users are configured by the relevant Registrar's (organisation's) Registrar Admin User.

2.3 Registrar User management tasks performed by Registrar Admin Users

2.3.1 Managing Registrar Users

Start the SIDN usermanagement application from the start screen. On start-up, the application will show the following main menu.

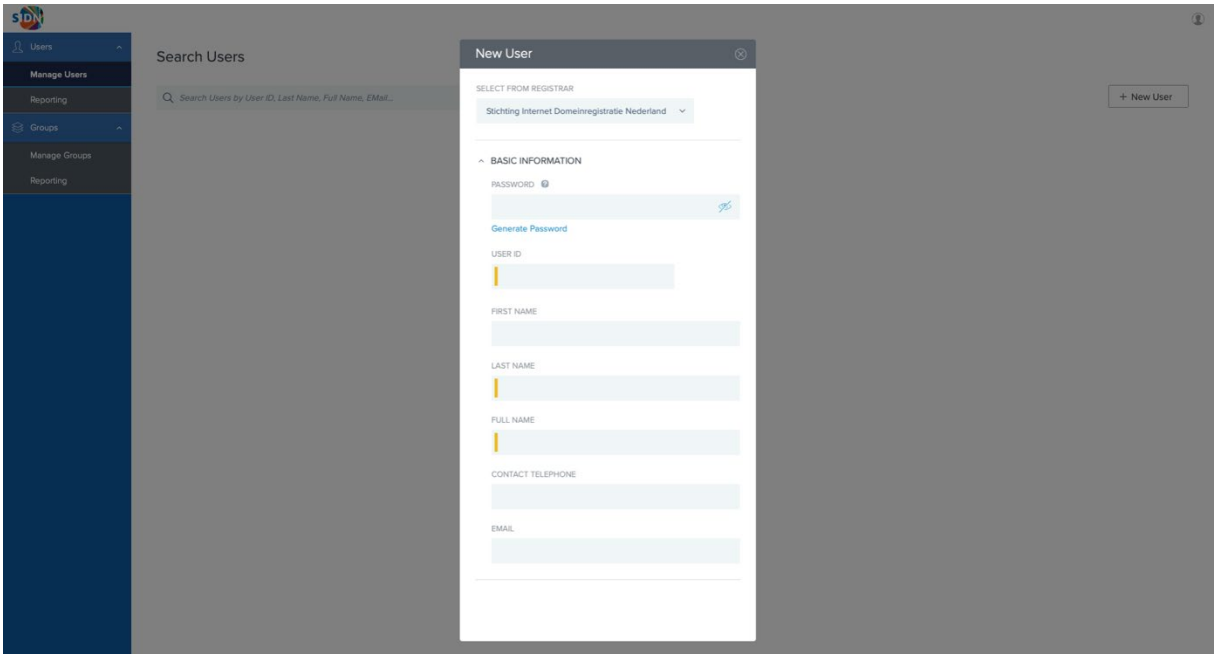


This is the starting point for the management tasks that a Registrar Admin User can perform, including the following Registrar User management tasks:

- Creating new Registrar Users
- Activating/deactivating Registrar Users
- Resetting Registrar Users' passwords
- Defining Registrar Users' Group Memberships

2.3.2 Creating a Registrar User

Only a Registrar Admin can create a new Registrar User. The new user creation process is a generic process, as described below.
The fields that have a yellow bar on the left are mandatory.

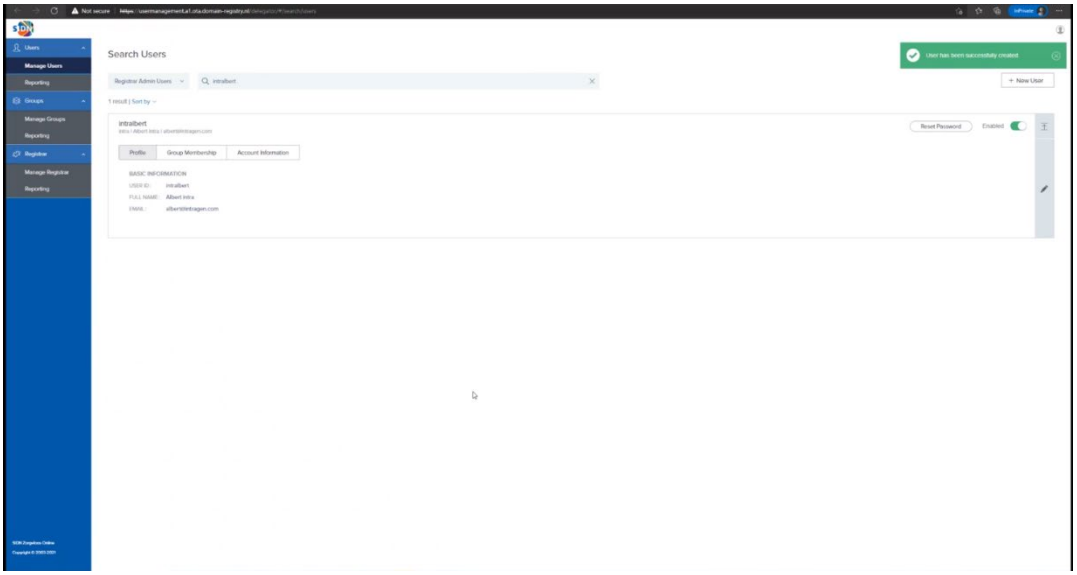


1. Select 'Manage User' and then, under 'Search Users', select 'Registrar Users' from the dropdown menu and click the 'New User' button that appears.
2. **PASSWORD**
   In this field, you can enter an initial password for the user or generate one by clicking 'Generate Password'. Save the password, preferably in a password manager. The password entered or generated here is a single-use password that you need to give to the new user, along with their username. When they use this password to sign on for the first time, the system will require them to choose a new password.
3. If you enter an initial password yourself, it has to meet the relevant criteria. We recommend using the 'Generate Password' option to make sure the initial password doesn't fail the criteria. The criteria that a password has to meet are as follows:
   - The password has to conform to at least three of the following character sets:
     - 0123456789
     - ZYXWVUTSRQPONMLKJIHGFEDCBA
     - abcdefghijklmnopqrstuvwxyz
     - ~!@#$%^&*()-_=+[]{}|;:,.<>/?
   - The password must not include the user's username or personal name.
   - The password must not be a commonly used password.
   - The password must be at least sixteen characters long.
   - No character may be used more than twice in succession. For example, 'SIDDN' is permissible, but 'SIDDDN' is not.
   - At least one day must have passed since any previous password reset.
   - A password must be reset at least once a year.
   - A new password must not be the same as any of the user's last ten passwords.
4. **USER ID**
   Enter a username for the new user. Only the following characters are permitted: A..Z, a..z

and 0..9. (An e-mail address cannot therefore be used as a username.) A change request is currently pending to permit use of the '@' and a '.' characters.

5. Make sure that the username (User ID) you enter is not already in use. If you enter an existing username, the system currently returns a confusing error message.
6. **FIRST NAME**
   The user's first name.
7. **LAST NAME**
   The user's surname.
8. **CONTACT TELEPHONE** (optional)
   Enter the user's phone number if you wish.
9. **E-MAIL** (mandatory)
   Enter the user's e-mail address. Make sure that any address you enter is not already linked to another user. If you enter an existing e-mail address, the system currently returns a confusing error message. The address you provide is also used for account recovery, if the need ever arises.

Once you have completed all the appropriate fields, a 'Save' button appears at the bottom of the screen. Once you have successfully created a new user, the following screen appears.

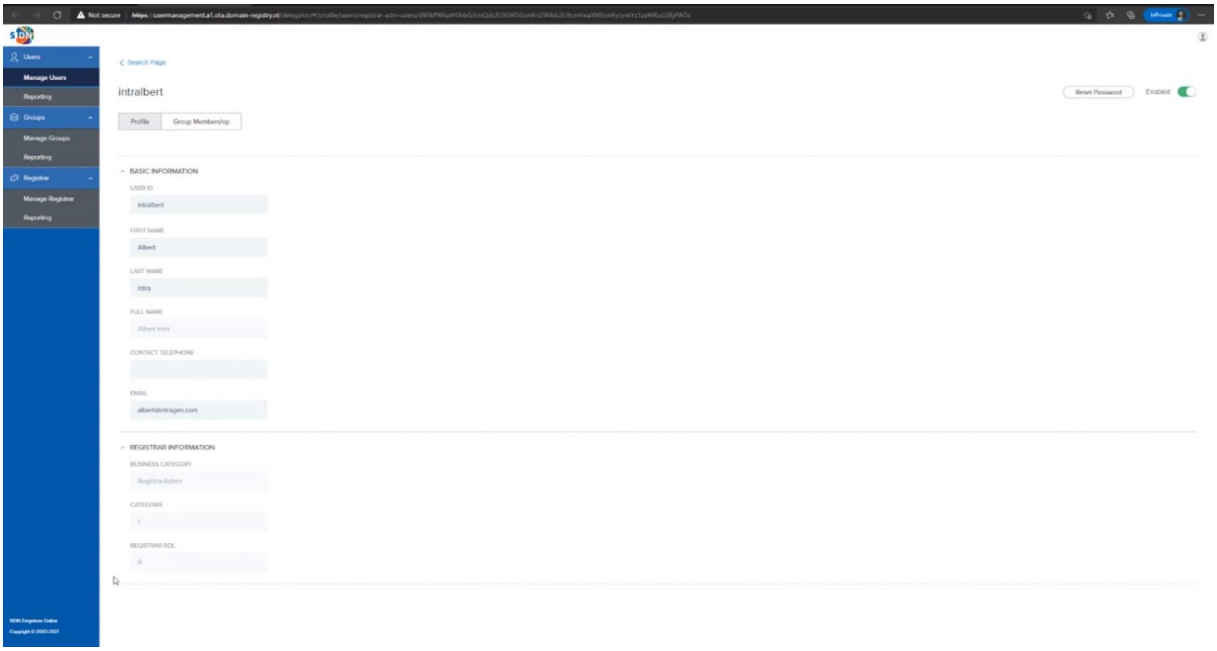


On the right-hand side of the screen, you can see that the user is 'Enabled'. You can disable the user by using the toggle switch.
On the same screen, you can also reset the user's password using the 'Reset Password' button.

- By default, the 'Profile' tab is visible, showing details of the (new) user.
- By switching to the 'Group Membership' tab, you can view the Group Memberships assigned to the user. When a new user is created, they initially have no Group Memberships.
- On the 'Account Information' tab, you can view information such as:
  - The user's most recent sign-on
  - Whether the user still needs to change their initial password (sign-on)
  - The user expiry date (one year by default)

2.3.3 Editing User Profile information

Click the pencil icon on the right-hand side of the screen to edit a user's profile.



From the Profile menu, you can edit certain information about the user. Editing rights depend on the type of user involved and are indicated under Business Category. A Registrar Admin User can edit only Registrar Users. That is indicated under Business Category.

All fields under Basic Information except for Full Name and User ID (dimmed) can be edited. If the e-mail address is edited, the new address must be unique, as when creating a new user.

Once changes have been made, a 'Save' button and a 'Reset' button appear at the bottom of the screen.

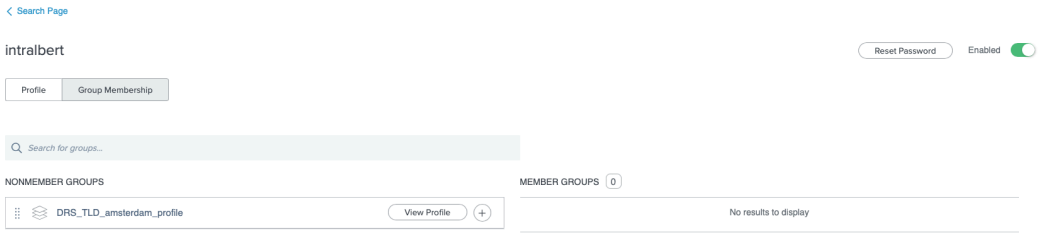
2.3.4 Assigning Group Memberships to a Registrar User

Select the 'Group Membership' tab.

You will see a list of the Group Memberships (e.g. RegistrarSite) that can be assigned to the Registrar User in question within the relevant Registrar (organisation).
On the dropdown menu, the Group Memberships assignable to Registrar Users are organised under two general headings:

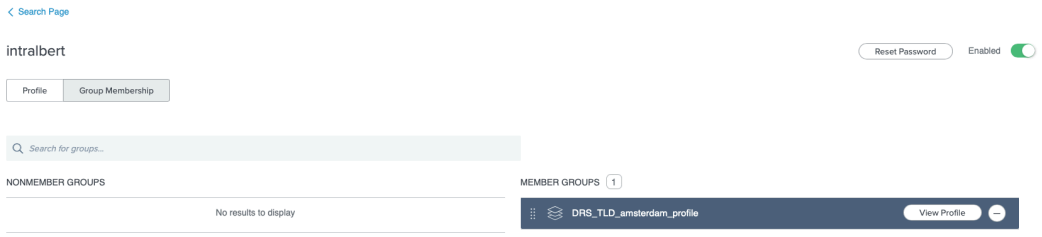
1. Application Admin Groups (currently containing a single group)
2. Employee Admin Groups (currently empty)

The Group Memberships assignable to Registrar Users within the Registrar (organisation) are listed. The Registrar Admin User can assign any of the listed groups to the relevant Registrar User.
However, the list of Employee Admin Groups is currently blank.



After selecting the Group Membership tab, all the assignable Application Admin Groups are listed. A group is assigned to a user by clicking the plus (+) by the relevant group, as illustrated below.

The assignment of a group to a user is undone by clicking the minus sign (-) next to the relevant group.



The diagram below illustrates how a Registrar Admin User creates a new user: