

MDES | Multi Data Exchange Solution

General user guide – reporting entity

MDES v3.3

December 2022 | Version 1.4

PUBLIC



BearingPoint®

Table of Contents

General Introduction	3
Introduction to the user guide	4
Contents of this user guide	4
Document structure and general layout	4
Application tasks	5
Abbreviations	6
Disclaimer	6
Section I General Overview	7
1 General Features & Navigation	8
1.1 Menu structure	8
1.2 Common User Interface Icons	9
1.3 MDES Portal Status	12
1.4 Instructional videos	13
2 Important process flows	14
2.1 Creating a new user account for a reporting entity	14
2.2 Managing partner jurisdictions	16
3 Security: Two-Factor Authentication	18
3.1 Enable Two-Factor Authentication	18
3.2 Disable Two-Factor Authentication	23
3.3 Reconfiguring Two-Factor Authentication	25
Section II Reporting entities	26
4 Registration process	27
4.1 [Task] Request a new account	27
4.2 [Task] Forgot password	33
5 Homepage Reporting Entity	35
5.1 Menu tab: Reporting Entity	36



General Introduction

BearingPoint®

Introduction to the user guide

Contents of this user guide

The MDES portal application facilitates the automatic exchange of information (AEOI) commitments and obligations between reporting entities, competent authorities, and partner jurisdictions.

This document is the general user guide for the MDES portal.

The purpose of this document is to provide information on the general section and/or functionalities of the MDES portal. Since the portal has a modular structure, the explanation for specific modules and/or functionalities have been developed in separate user guides.

For privacy reasons some (parts of) images have been blurred.

NOTE: depending on the application roles of the actual users, some tasks, screens, or functionalities may not be shown to a user once logged in.

Document structure and general layout

The MDES portal has two main user groups: the reporting entities (RE) and the competent authority (CA). This user guide is for the RE user group.

This user guide is divided into sections:

- **Section I:** [General Overview](#)
- **Section II:** [Reporting entities](#)

Each part outlines the relevant user pages, tasks, and breaks them down into the individual steps, describing the interaction with the system. In addition, the user tasks are illustrated with screenshots.

As mentioned in the introduction, this is the general user guide for the MDES portal. There are separate user guides for each additional module of the MDES: CRS / FATCA, CbC, EOIR, MoU.

Application tasks

Tasks have been made visible by adding [task] before each task of the MDES portal. The tasks described within this document are listed in below table.

Task	Group	Paragraph
Enable Two-Factor Authentication	All users	3.1
Disable Two-Factor Authentication	All users	3.2
Reconfigure Two-Factor Authentication	All users	3.3
Request an account	Reporting Entity	4.1
User account re-request for current user	Reporting Entity	4.1.1
Forgot password	Reporting Entity	4.2
Activate account with code	Reporting Entity	4.2
Request amendment exchange type(s)	Reporting Entity	5.1.1.1
Edit user profile	Reporting Entity	5.1.1.2
Create reporting entity user	Reporting Entity	5.1.1.3
Make reporting entity user the administrator	Reporting Entity	5.1.1.4

Abbreviations

CA	Competent Authority
CbC	Country by Country
CRS	Common Reporting Standard
CSV	Comma-Separated Values
CTS	Common Transmission System (Portal from OECD)
FATCA	Foreign Account Tax Compliance Act
FI	Financial Institution
FC	FATCA/CRS
IDES	International Data Exchange System
MDES	Multi Data Exchange Solution (Portal from BearingPoint)
MNE	Multinational Enterprise
OECD	Organization for Economic Co-operation and Development
RE	Reporting Entity
XML	Extensible Markup Language

Disclaimer

Information in this user guide may contain technical inaccuracies or typographical errors. The MDES portal is continually being improved and functionality might change without notice. Please contact BearingPoint Caribbean if any changes need to be made to this document.



Section I General Overview

BearingPoint®

1 General Features & Navigation

1.1 Menu structure

The home page is an intuitive homepage that shows a quick overview on important information, to-dos for the logged in reporting entity user. The application has a standard layout for navigating through the various functionalities. The tabs and screens that the system displays depends on the user’s role and user’s rights.

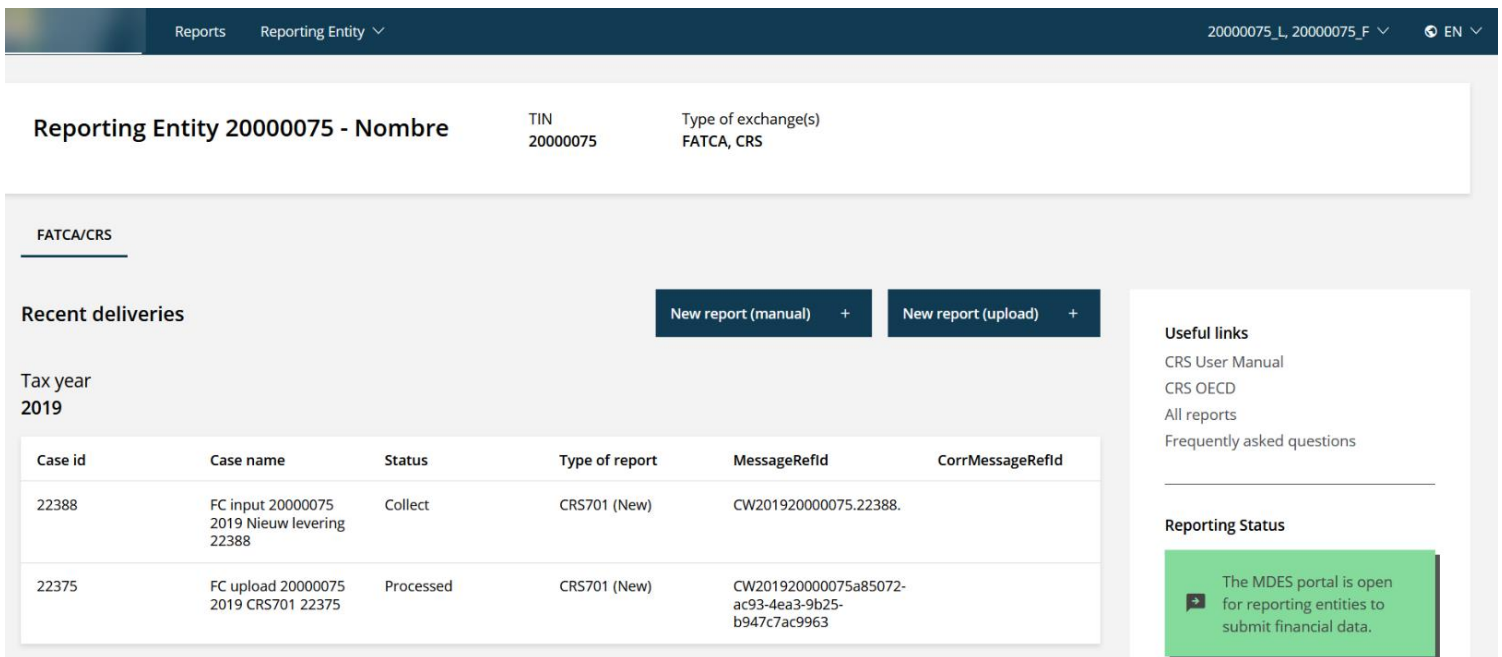
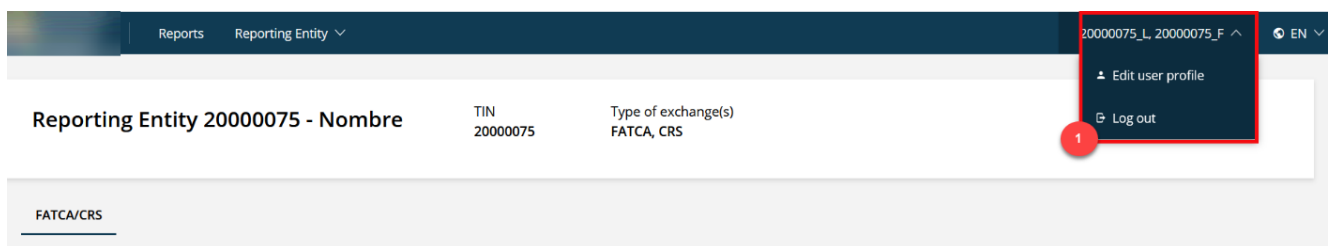


Figure 1-1 Landing page: My account overview for a reporting entity user

When logged into the system, the filter options (side bar), main menu items (top bar) and the register individual tasks (blue buttons) are visible on the screen.

1.1.1 Horizontal menu bar (tabs)

The horizontal menu bar is accessible on all screens. Via this menu you can navigate to the various parts of the application.



After logging in, the user's name will be displayed in the upper right corner. You can also log out here. By moving the cursor to the name, the menu expands (1). Click “Log out” to log out. In this panel you can also modify the language.

1.2 Common User Interface Icons

The system icons and buttons used are uniform and are shown and explained in this paragraph.

1.2.1 Date fields

The calendar can be used for all date fields and the calendar can be recognized by the calendar icon. By clicking on the icon, the calendar appears.

In case after reading a file, the date 01-01-1899 appears, it means that the entered date was not correctly entered / specified.

1.2.2 Mandatory fields

When a field is mandatory, it is displayed with an asterisk (*).

First name contact person *



Figure 1-2 Example mandatory field

1.2.3 Messages

There are several messages that may appear in the application. In some cases, it is not possible to continue when a message is displayed. Other messages serve as additional information and do not block the user from continuing.

Submit the information below

Responsible for exchange of information

2 The person responsible for data delivery for a FATCA liable institute should be the same person as the responsible officer entered in the FATCA registration

1

First name contact person *
● Field is mandatory

Last name contact person *
● Field is mandatory

E-mail address *
● Field is mandatory

Repeat e-mail address *

Figure 1-3 Example messages

The blocking messages are displayed near the line and field related to the message. When this type of message appears, it is not possible to continue until the message has been resolved.

There are also informative messages. This blue message (2) is just an explanation of what to fill in in the appropriate form (help text). The help text appears regardless of the input.

1.2.4 Choice options

Within the application the following choice options are available:

- **Choose a value.** Here you can make a choice by clicking the right arrow:



Figure 1-4 Example value option

- **Radio Buttons.** Up to 1 choice can be made.



Figure 1-5 Example radio button

- **Check boxes.** In this case, it is possible to choose either none or one (or more) options:

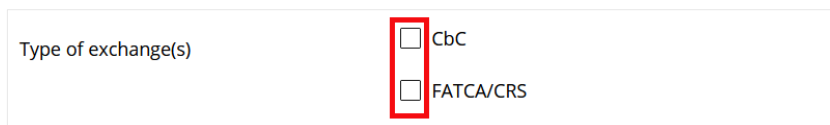


Figure 1-6 Example check box

1.2.5 Assistant texts

The application uses assistant texts. The assistant texts are displayed after hovering over a question mark icon.

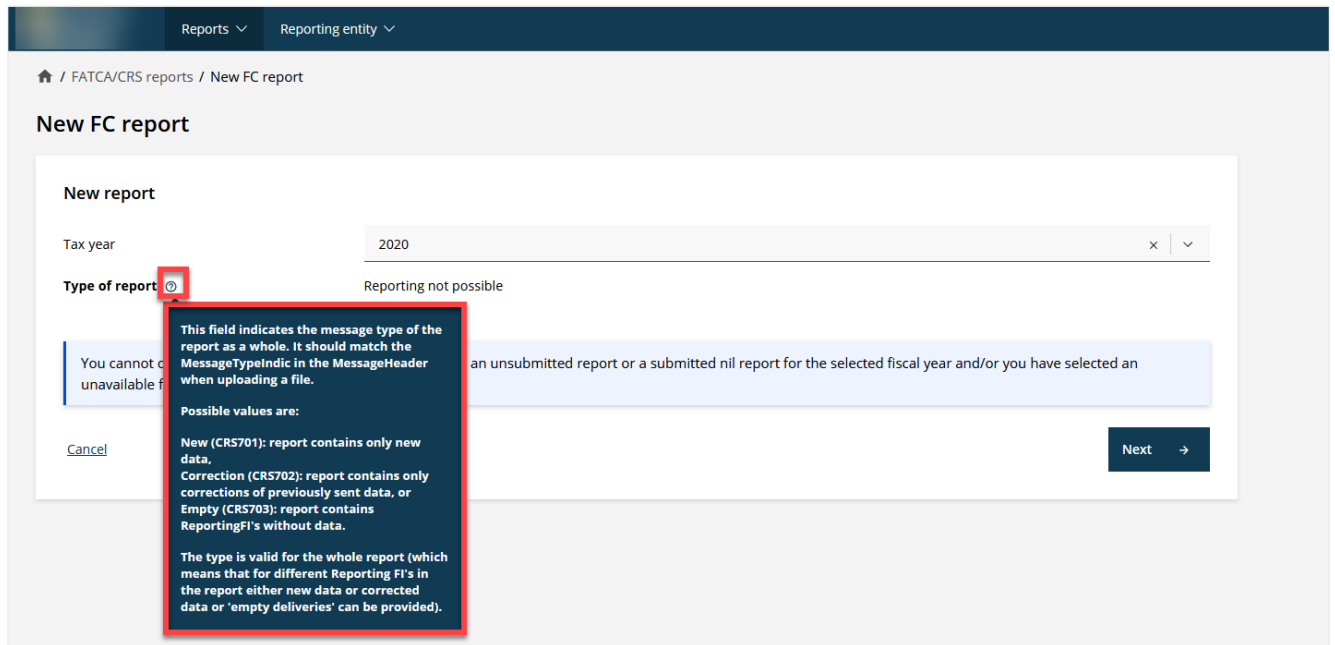


Figure 1-7 Example assistant texts

1.3 MDES Portal Status

A competent authority can manage the reporting process by opening (and closing) the portal for reporting during the year.

To facilitate this, the MDES portal has 3 statuses that can be changed at any time by the competent authority. These are:

1. Release for reporting
2. Release for relations management and testing
3. Not released

Table 1 MDES portal status

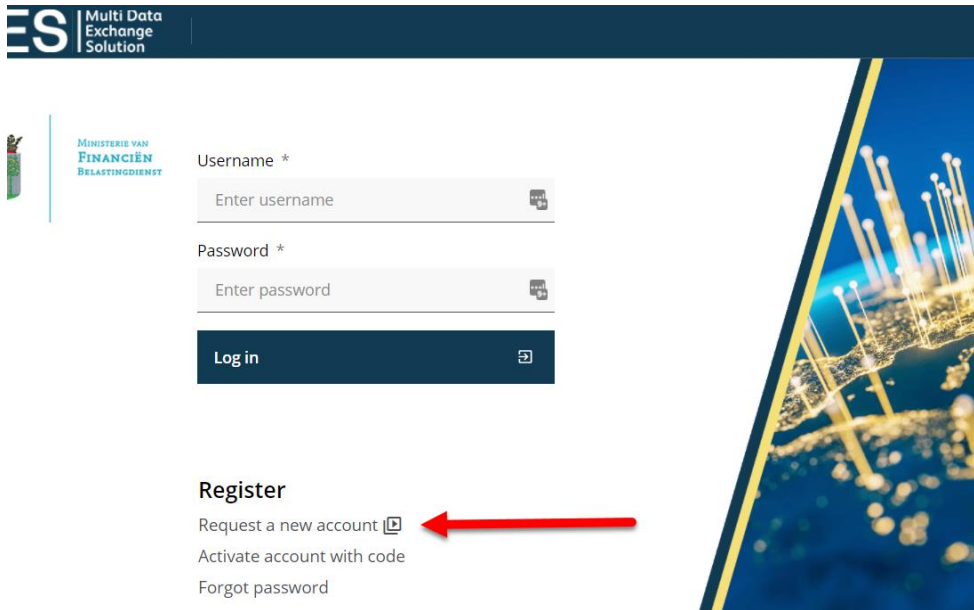
Portal status	Description
Release for reporting	<p>The MDES portal is open for the reporting entities to report/submit (financial) data by uploading an XML file or manually entering the data.</p> <p>During this status, the task to <u>validate</u> an XML file will <u>not</u> be available for the reporting entity.</p> <p>Depending on the installed MDES module, EOI relation management is only available to the competent authority.</p>
Release for relations management and testing	<p>Depending on the installed MDES module, EOI relation management is only available to the reporting entity.</p> <p>The reporting entities can validate XML files. The validation checks are performed on the XML files to verify that there are no file or record errors.</p> <p>During this status, the task to report/submit reports will <u>not</u> be available for the reporting entity.</p>
Not released	<p>It will not be possible for reporting entities to validate or submit any reports. Only changes to the profile or user account are possible.</p> <p>On January 1st of each year the MDES portal changes to this status.</p>

The system can send out e-mail notifications to update the reporting entities on the change in status.

1.4 Instructional videos

To further guide users and provide users with additional information about functionality and features, there are instructional videos available throughout the application.

To navigate to an instructional video, the user can click on the “play” icon (🎬) as shown below:



2 Important process flows

2.1 Creating a new user account for a reporting entity

2.1.1 Description

A reporting entity (RE) that does not have an account for the MDES portal can request a new account from the main MDES portal page.

Process:

1. The RE starts by clicking on the “Request a new account” task and follows the process as shown in Figure 2-1 Process flow.
2. Once the account is created an e-mail will be sent by the system. This is to validate the account request.
3. The RE must validate the account request within 24 hours (!).
4. After the account request has been validated, the RE needs to submit personal and company details and upload documents to complete the account registration for MDES.
5. After the complete account request is submitted the competent authority (CA) will assess the information provided.
6. The account request can be Approved or Declined. The RE will receive an e-mail after the assessment.
7. If the account request is approved, the RE will have access to all applicable AEOI functionalities of the MDES portal.

2.1.2 Process flow: Creating a new user account for a reporting entity

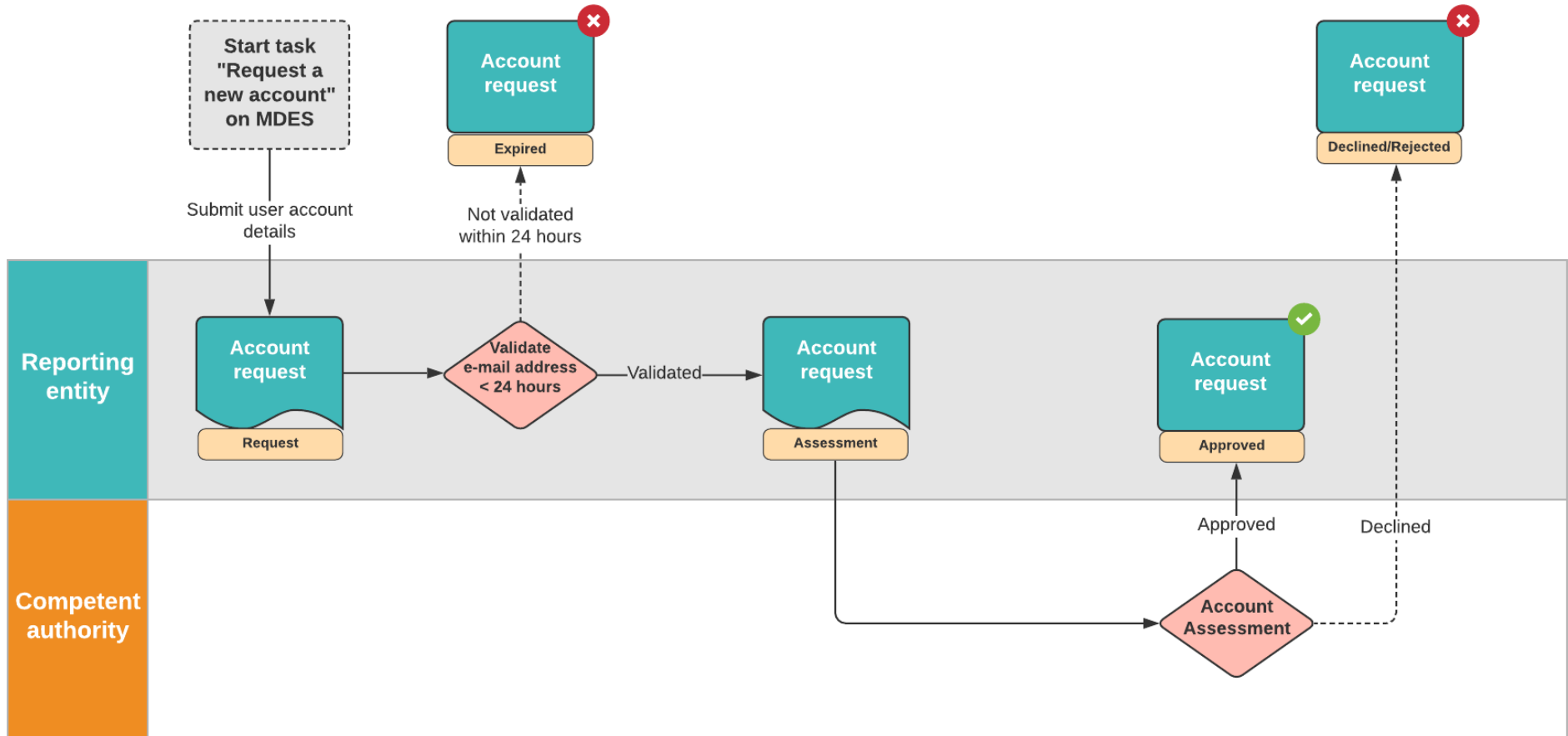


Figure 2-1 Process flow creating an RE account

3 Security: Two-Factor Authentication

From MDES release 3.1, it is possible to add an extra layer of security protection for the user by enabling Two-Factor Authentication. The below chapters provide guidance in how to setup, use and manage the Two-Factor Authentication functionality in MDES.

3.1 Enable Two-Factor Authentication

Important: Any user of the MDES portal can activate Two-Factor Authentication. Before enabling the Two-Factor Authentication functionality, please download any TOTP Two-Factor mobile application, such as the **Google Authenticator** or **Microsoft Authenticator** app.

Configure the app on your mobile phone before proceeding. Then, follow these steps:

1. Navigate to your profile page.
2. Click on the task **Enable Two-Factor Authentication**.
3. Enter your user password and click Next.
4. Using your mobile authenticator app, scan the QR-code. If OK, click Next.
5. If OK, enter the TOTP code in MDES that is shown on your mobile authenticator app. Click Next.
6. A screen is shown indicating that a back-up document will be generated, which can be downloaded from the user profile page. These back-up codes are available in case the mobile authenticator app is not available.
7. Download the back-up code document and store locally. **Note: this document is only available for 15 minutes.**
8. Note that Two-Factor Authentication is now Enabled.

Below screenshots illustrate the above-mentioned steps to enable Two-Factor Authentication.

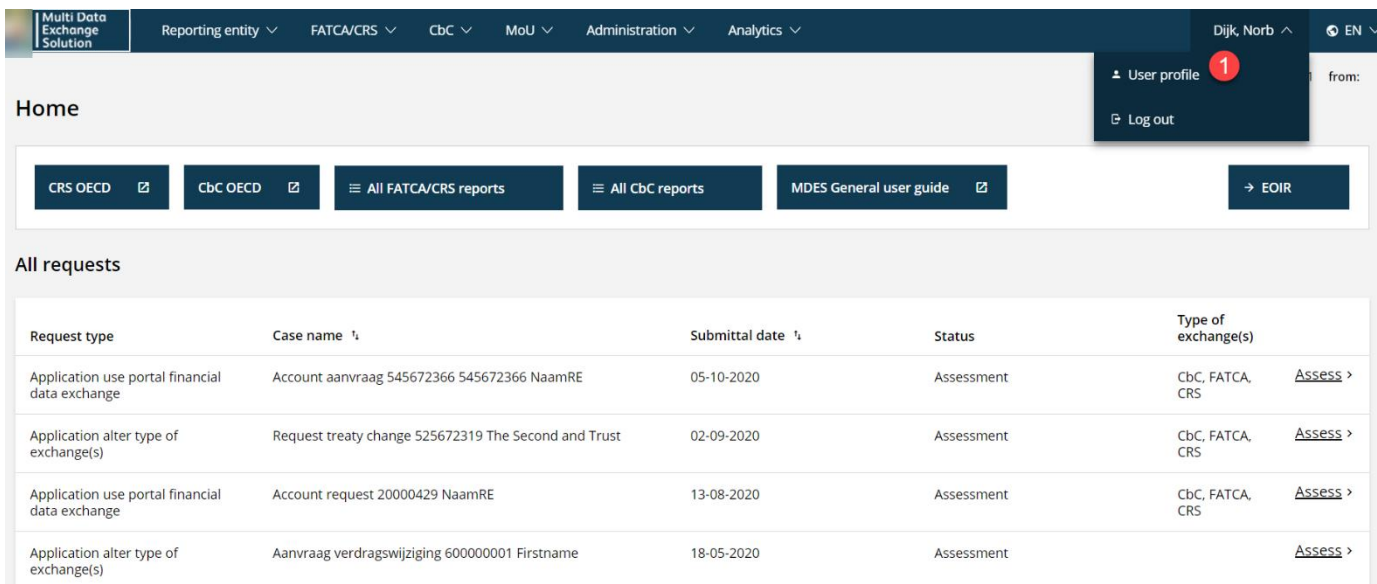


Figure 3-1 Navigate to the user profile

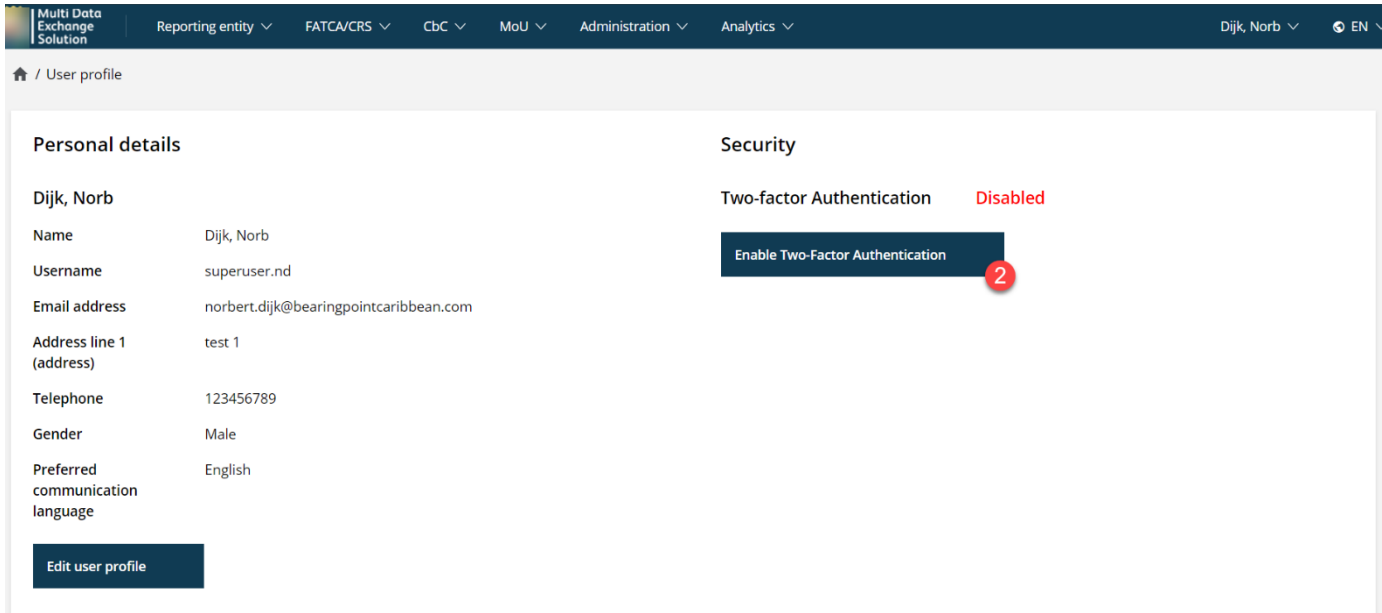


Figure 3-2 Click task to start process

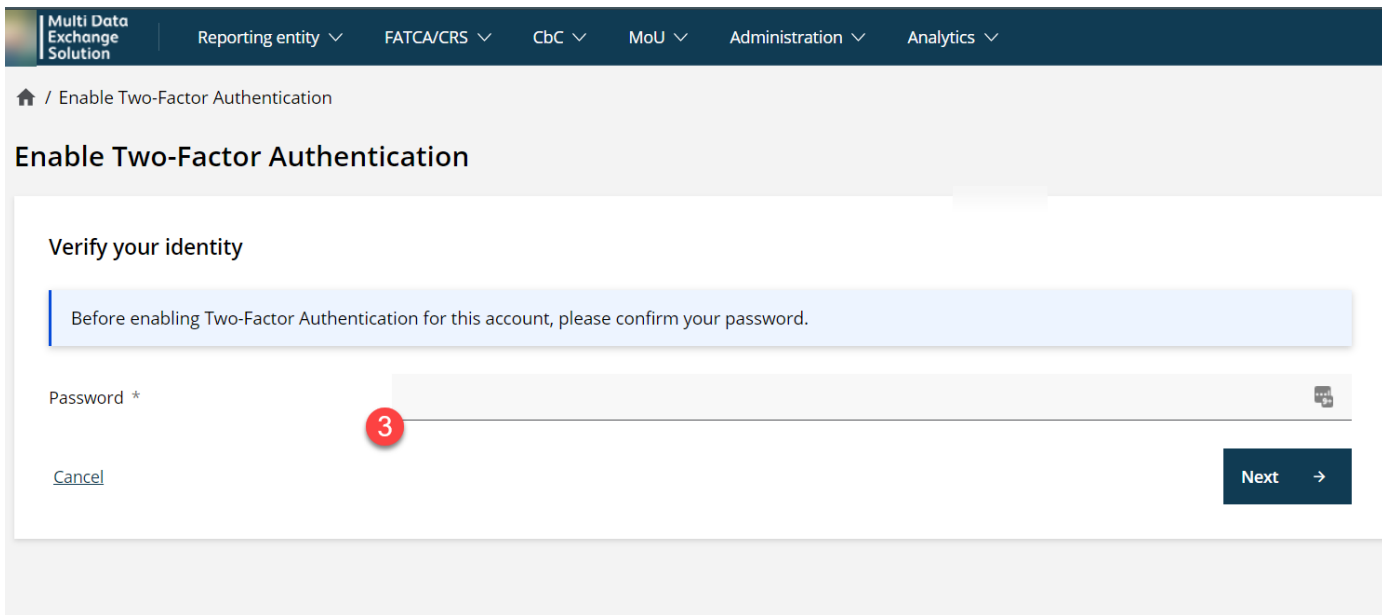


Figure 3-3 Enter password

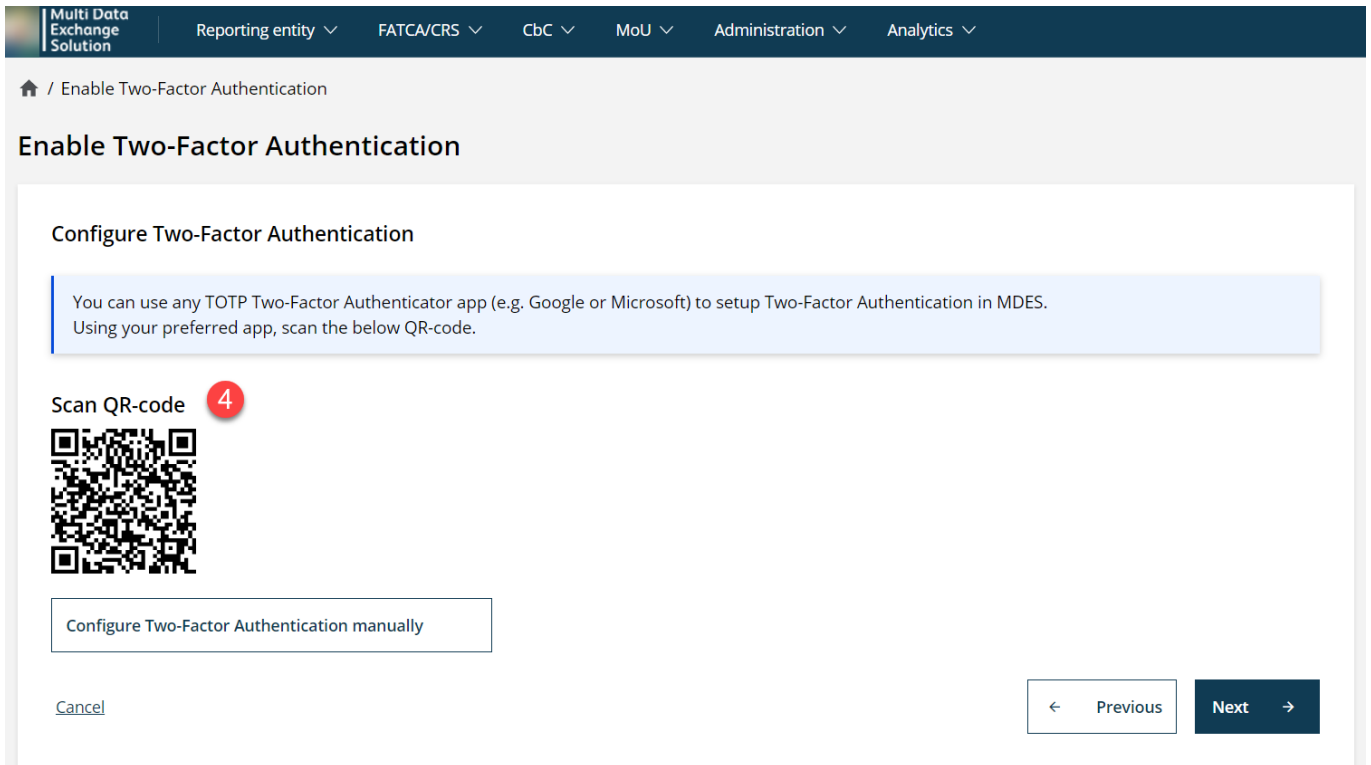


Figure 3-4 Scan QR-code

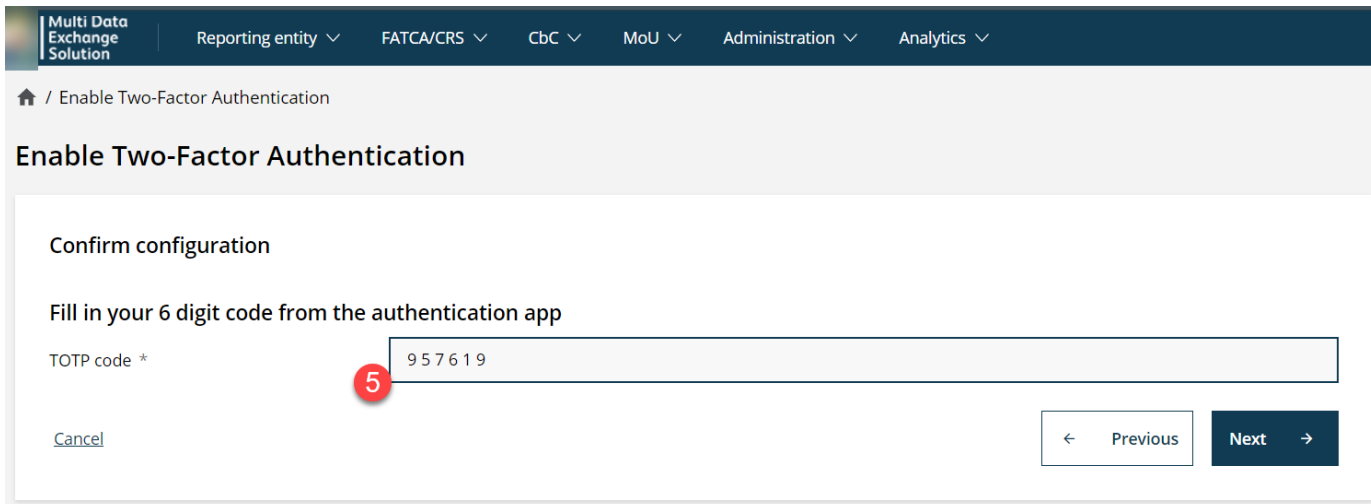


Figure 3-5 Fill in TOTP code

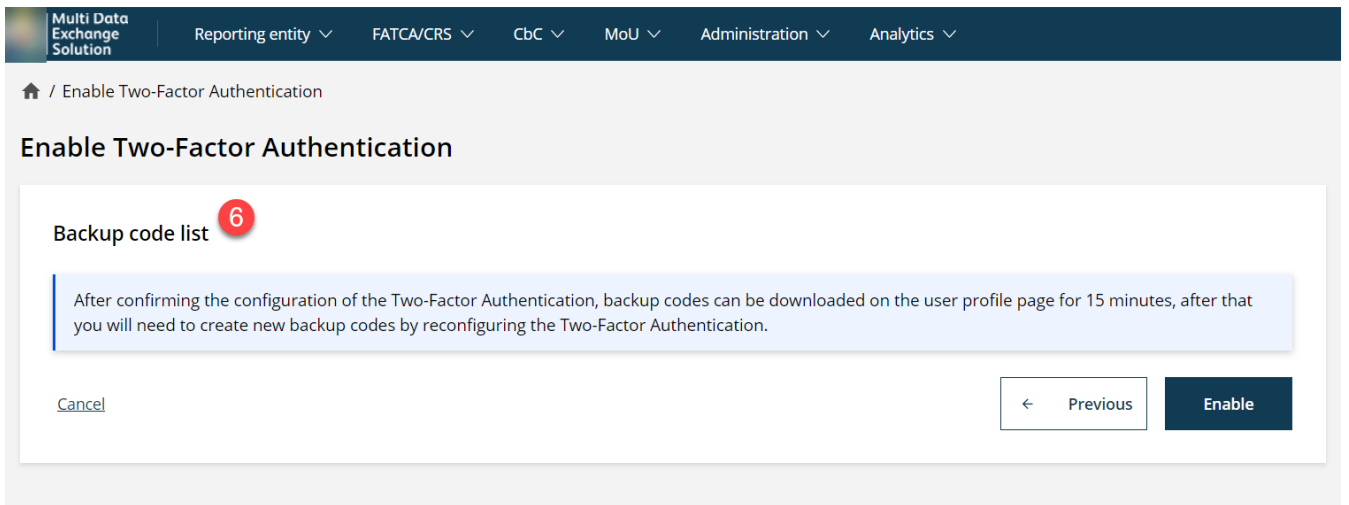


Figure 3-6 Note that the back-up code list is downloadable for 15 minutes

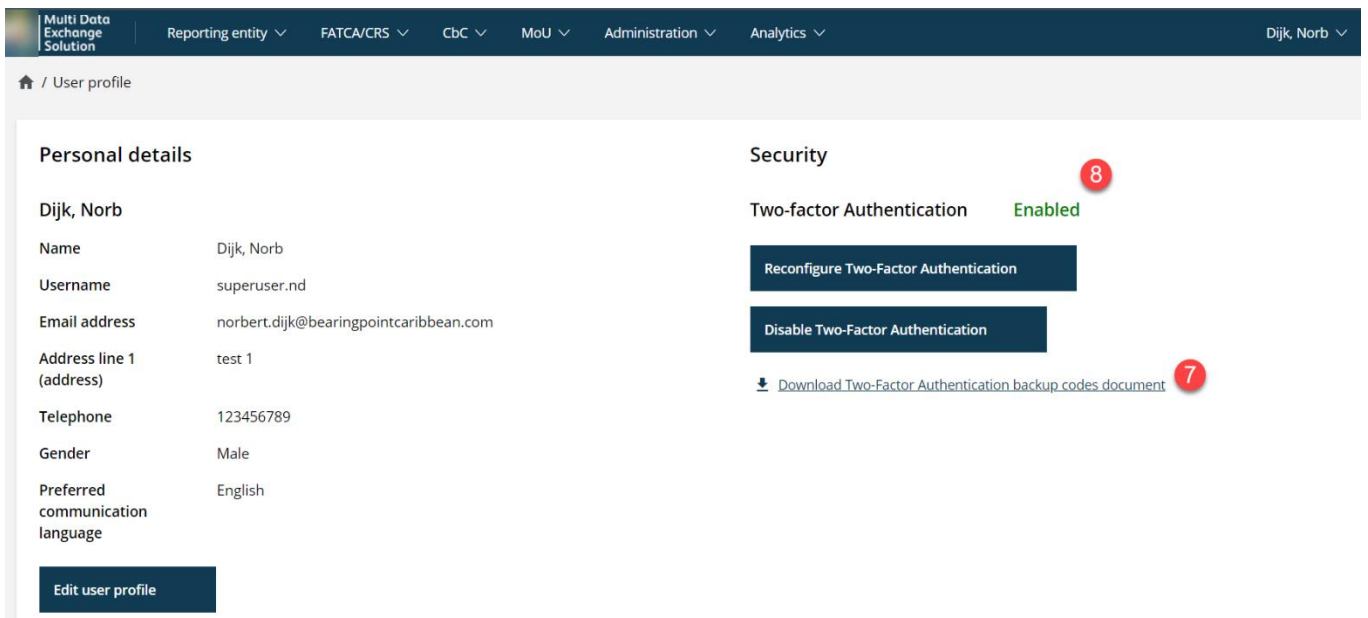


Figure 3-7 User profile screen and Two-Factor Authentication enabled

Note: the back-up code document is only available for 15 minutes.

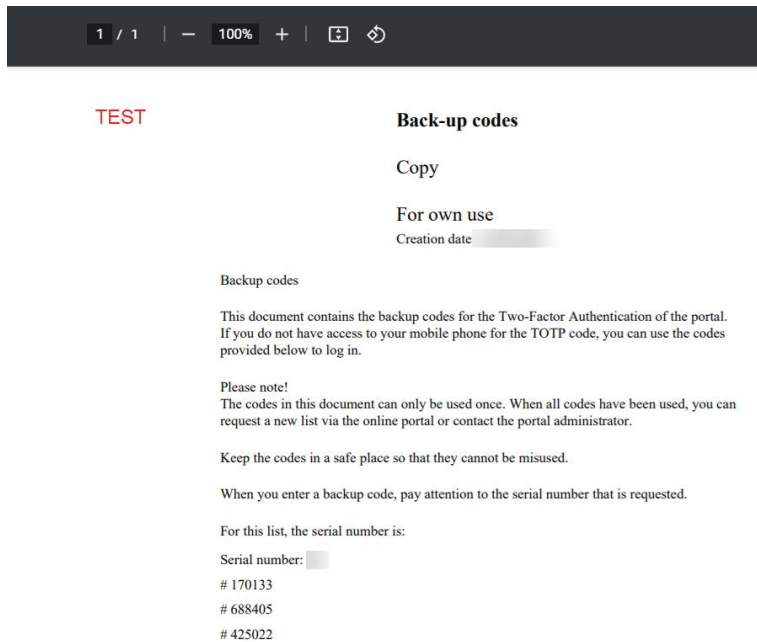


Figure 3-8 Example of back-up codes document

It is possible to configure Two-Factor Authentication without using a QR-code. First follow the above steps, however, instead of scanning the QR-code, you can enter a code manually into the authenticator app. **You will need your e-mail address associated to the MDES account.**

Below screenshots illustrate the above-mentioned steps to enable Two-Factor Authentication using a code.

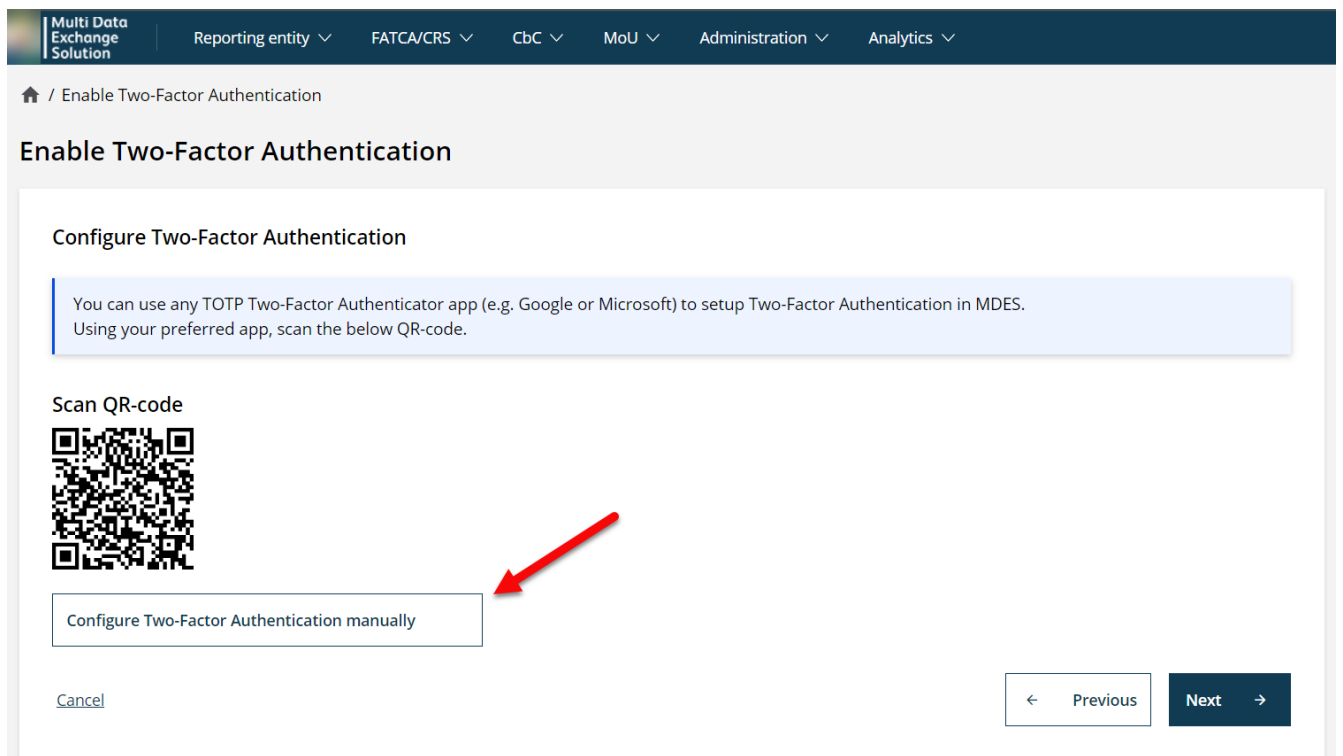


Figure 3-9 Click on this task to configure Two-Factor Authentication manually

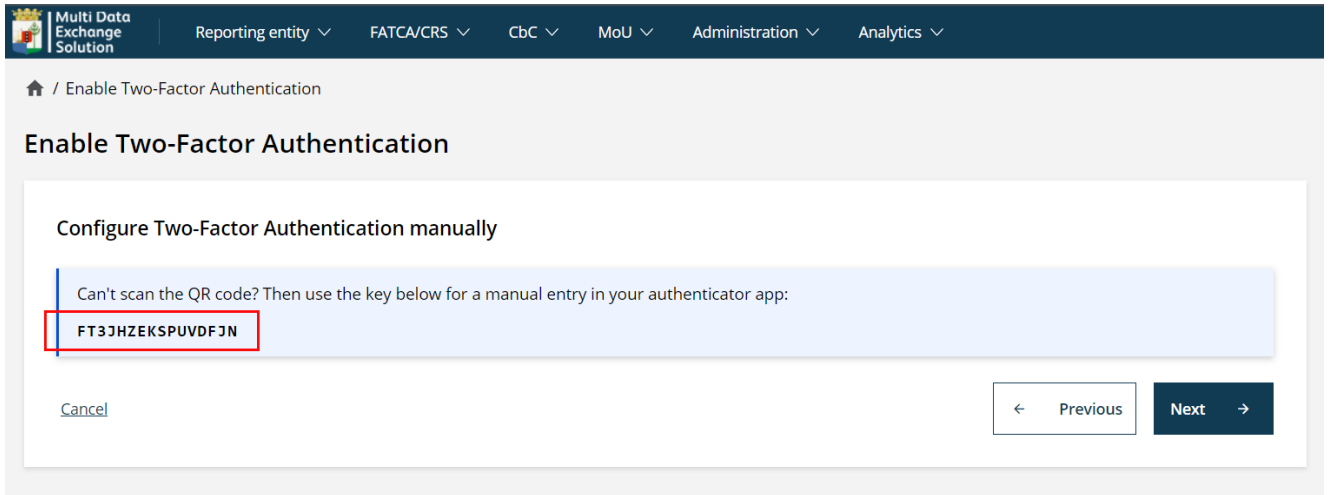


Figure 3-10 After submitting the key in the authenticator app, click Next to complete the setup

3.2 Disable Two-Factor Authentication

To disable Two-Factor Authentication, follow the below steps:

1. Navigate to your profile page.
2. Click on the task **Disable Two-Factor Authentication**.
3. Enter your user password.
4. Enter the TOTP code from the mobile authenticator app and click Next.
5. Click “Disable” on the final screen to confirm disabling the Two-Factor Authentication functionality.
6. Note that Two-Factor Authentication is now Disabled.

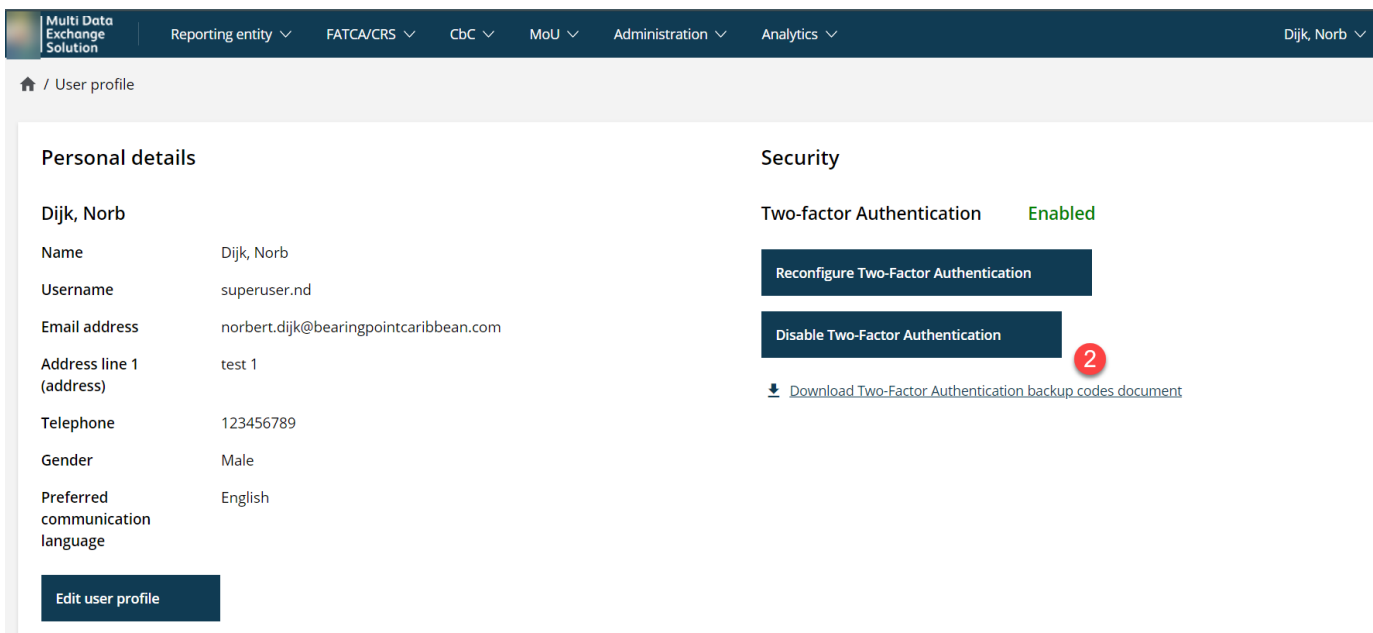


Figure 3-11 Click on the task "Disable Two-Factor Authentication"

Multi Data Exchange Solution | Reporting entity | FATCA/CRS | CbC | MoU | Administration | Analytics

Home / Disable Two-Factor Authentication

Disable Two-Factor Authentication

Verify your identity

Fill in your password

To disable Two-Factor Authentication, please fill in your password and code provided by the authenticator app.

Password * **3**

Fill in your 6 digit code from the authentication app

TOTP code * **4**

[Cancel](#) **Next** →

Figure 3-12 Enter password and TOTP code

Multi Data Exchange Solution | Reporting entity | FATCA/CRS | CbC | MoU | Administration | Analytics

Home / Disable Two-Factor Authentication

Disable Two-Factor Authentication

Are you sure you want to disable Two-Factor Authentication?

[Cancel](#) **5** **Disable**

Figure 3-13 Click Disable to complete process

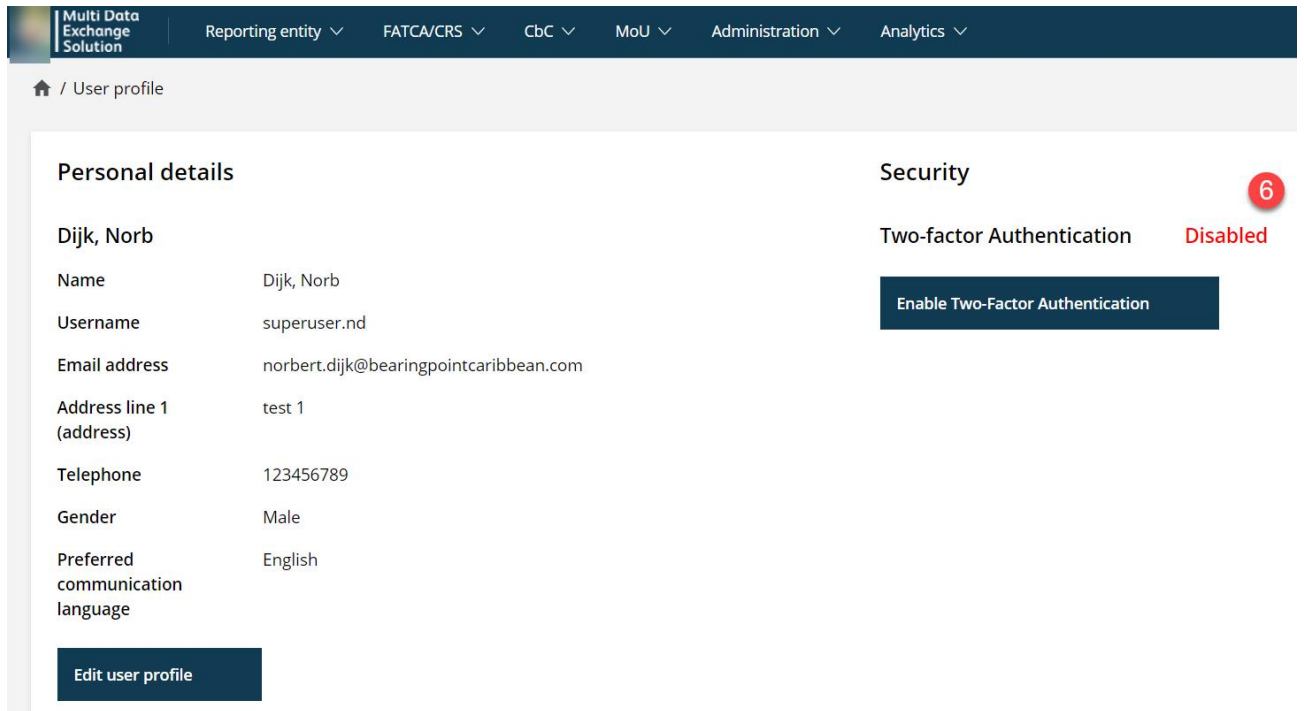


Figure 3-14 Two-Factor Authentication is now disabled

3.3 Reconfiguring Two-Factor Authentication

It is possible to manage the Two-Factor Authentication, for instance to reset/renew the TOTP code functionality on your app or to create a new list of back-up codes.

Open the TOTP app and follow the next steps:

1. Navigate to your user profile page.
2. Click on the task **Reconfigure Two-Factor Authentication**.
3. Enter your user password and click Next.
4. Enter your TOTP code and click Next.
5. Using your mobile authenticator app, scan the QR-code.
You might have to delete or overwrite the previous Two-Factor Authentication configuration in your app. If OK, click Next.
6. Fill in the TOTP code that is shown on your mobile authenticator app. Click Next.
7. A screen is shown indicating that a back-up document will be generated, which can be downloaded from the user profile page.
8. Download the back-up code document and store locally.
Note: this document is only available for 15 minutes.
9. Note that Two-Factor Authentication is Enabled.



Section II
Reporting entities

BearingPoint®

4 Registration process

Summary

For a reporting entity to be able to submit (financial) data, they should have authorized access to the application.

In general terms, the creation of accounts for the reporting entities is a four-step process as depicted below:

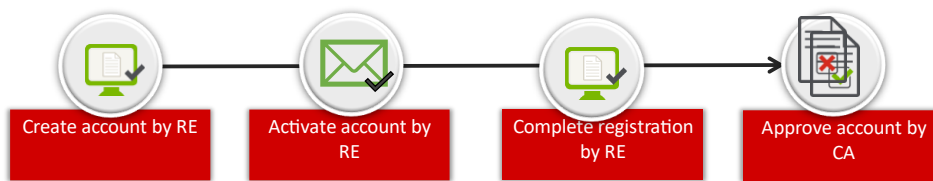


Figure 4-1 Four step account creation process

The first step is to request an account. The reporting entity will receive an e-mail to validate the account request and e-mail.

Note: the account activation by the reporting Entity must be done within 24 hours.

After the account has been validated and completed by the reporting entity, the competent authority can assess the account request and if approved, the account has been authorized and the registration process is complete.

4.1 [Task] Request a new account

The request button is on the landing page of the application.

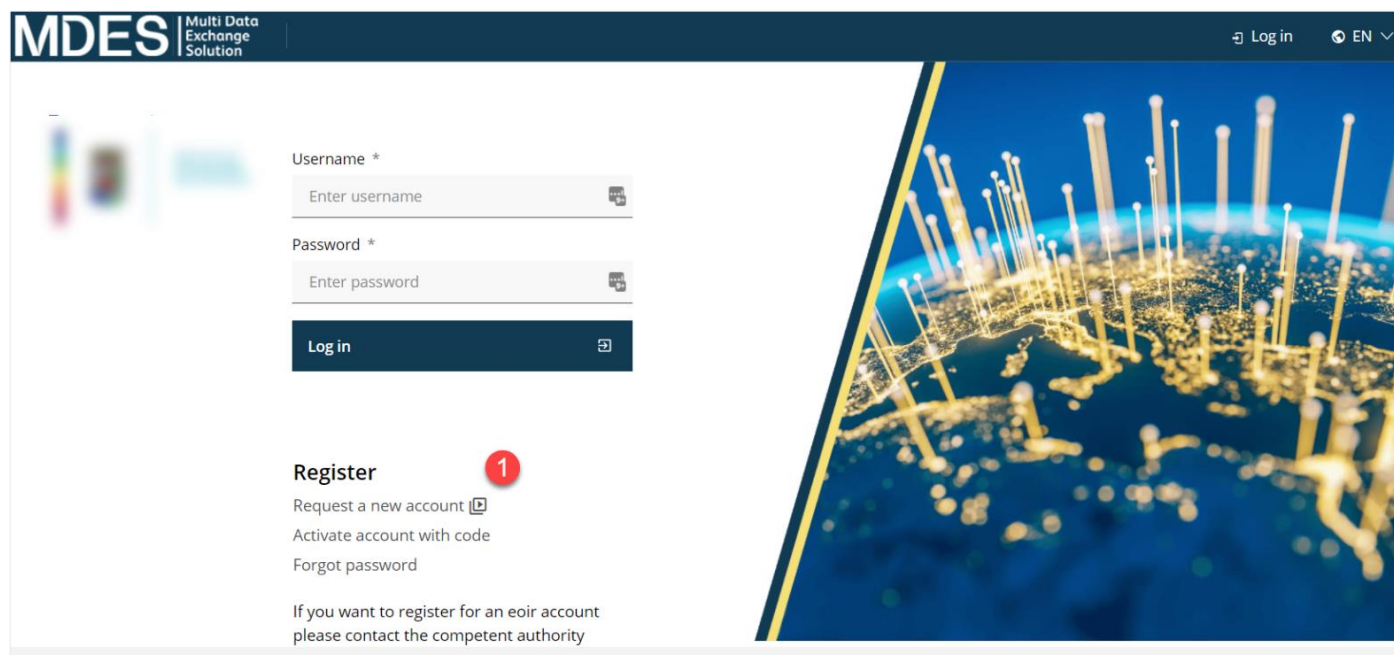



Figure 4-2 Request an account link

To register for an account, Click on the **Request a new account (1)** link.

Note the  icon. This means that there is an instructional video available relating to this task to the user.

The user will be presented with the enrollment page as shown in the image below.

MDES Multi Data Exchange Solution

Log in EN

Request a new account

Request a new account

Submit the information below

Login credentials

After creating a user account, you are still required to submit personal and company details and upload documents to complete the account registration for MDES. After you have submitted these details, the competent authority will assess your information. You will be notified by e-mail on the outcome of this assessment.

Username *

E-mail address *

Repeat e-mail address *

Password * ?

Confirm password *

Preferred communication language: Choose an option

[Cancel](#) **Finish** →

Figure 4-3 Registration form

To complete the request for a new account, the relevant fields should be entered. All fields with an asterisk are mandatory. If these fields are not entered, the user will receive a notification to complete the mandatory fields before being able to continue to the next screen.

After all information is entered and the next button is clicked, the user will get a confirmation that an e-mail has been sent and that the account should be activated within 24 hours.

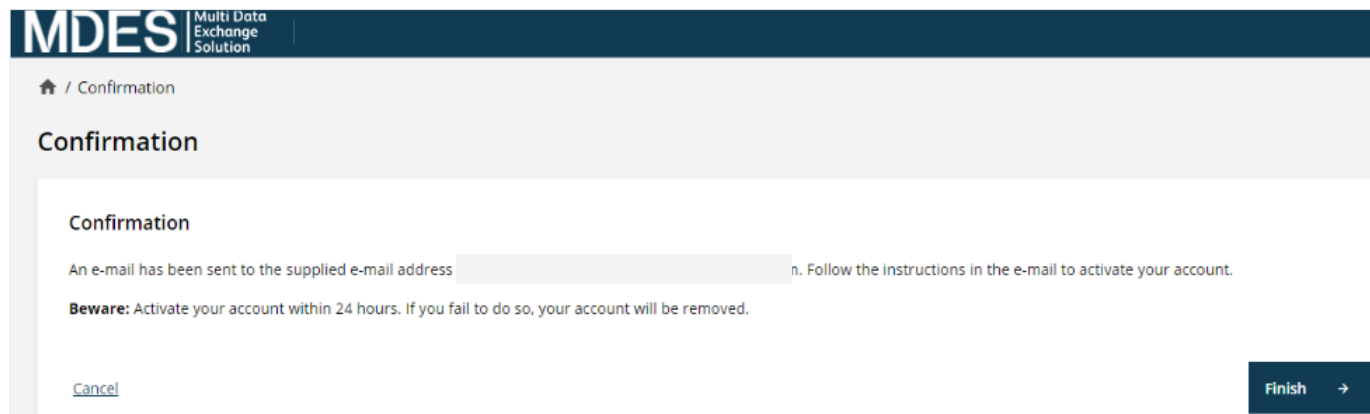


Figure 4-4 Account activation confirmation

After creating a user account, you are still required to submit personal and company details and upload the documents to complete the registration process.

Multi Data Exchange Solution | Reporting entity | charellaC | EN

Home / Request a new account | Last login: 2022-12-06 14:55:56 from: 192.168.11.131

Request a new account

Submit the information below

Responsible for exchange of information

The person responsible for data delivery for a FATCA liable institute should be the same person as the **responsible officer** entered in the FATCA registration

First name contact person *

Last name contact person *

Telephone number *

Identity document * ? Browse

Reporting entity

TIN *

Type of exchange(s) CbC FATCA/CRS

Formal/Legal name *

Tradename

Copy of company registration document * ? Browse

← Previous Next →

Figure 4-5 Account registration form

The user can login after the account has been successfully activated, but the user has limited access to MDES functionalities.

To use the portal, the request should be authorized by the competent authority. After the request has been approved, the user has full access to the portal.

In case the competent authority declined the request and requested additional information the requester will receive an email. The requester can login to re-submit the account request (see paragraph 4.1.1).

4.1.1 [Task] User account re-request for current user

In case the competent authority declined the request, the task **User account re-request for current user** will be visible. Once the user is logged into the MDES portal the user is redirected to the Home page. The task **User account re-request for current user (1)** is now available. With this task the requester can re-submit the account request.

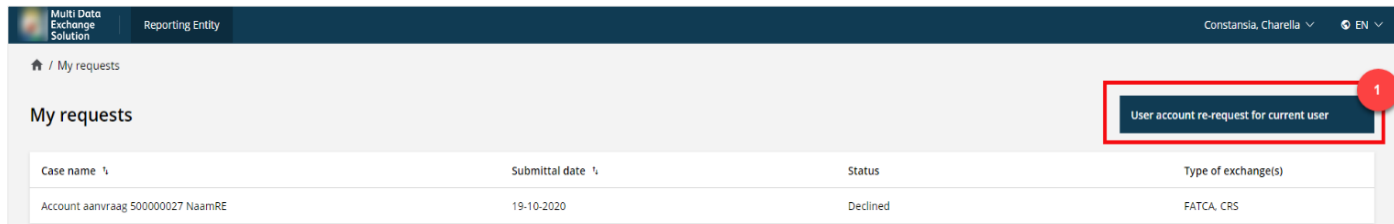


Figure 4-6 Resubmit account request

4.2 [Task] Forgot password

If you have forgotten your password, it can be retrieved. This is done by clicking “**Forgot password**” on the homepage.

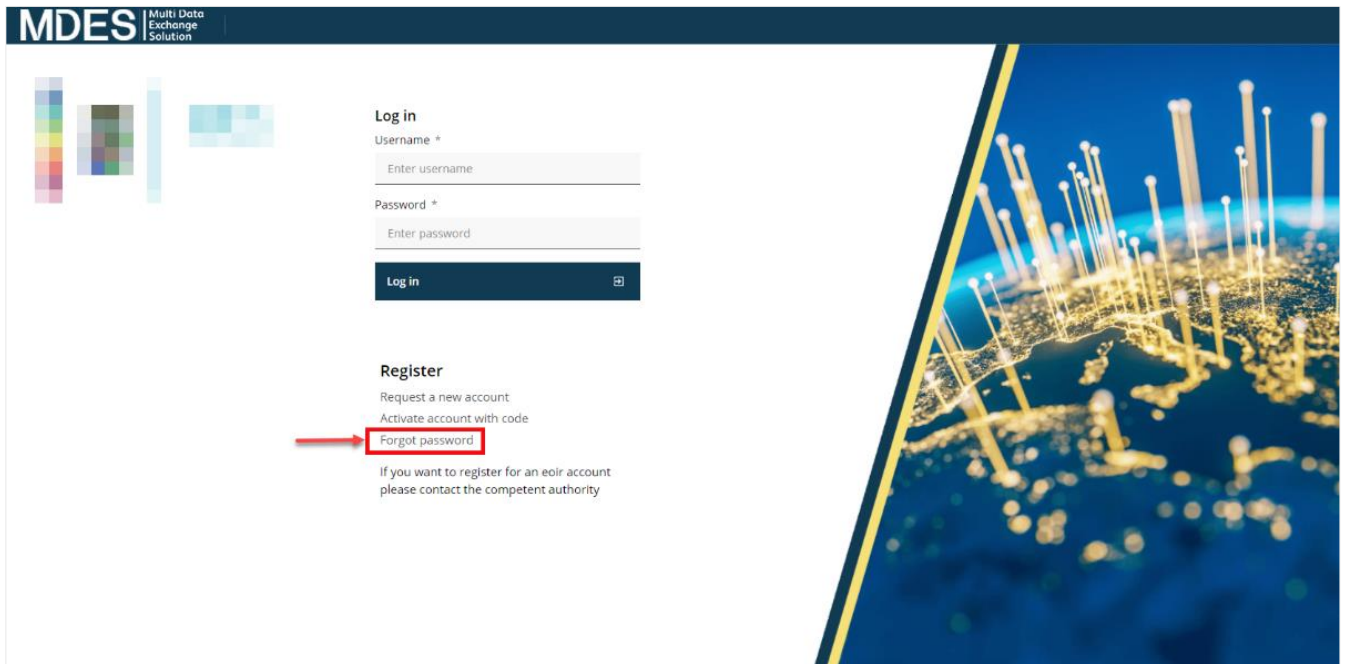


Figure 4-7 Home screen

The user is redirected to a “forgot password” form.

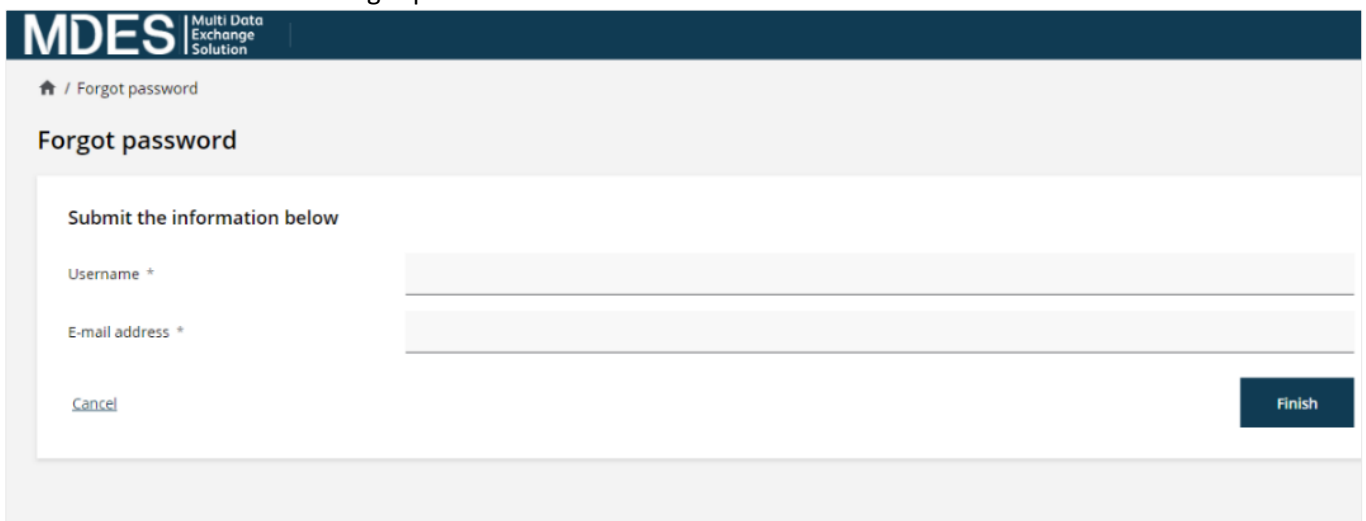


Figure 4-8 Forgot password form

After completing the form with correct data, you will receive an email with a new activation code within a few minutes.

After you receive a password reset activation code, you can navigate directly to the screen to change your password by clicking the attached link. This screen can also be accessed by clicking **“Activate account with code”** on the homepage.

The password must be at least 8 characters long and contain at least one uppercase letter, one lowercase letter, one special character (~, @, #, \$, %, ^, & *) and one digit (0-9).

After confirming your request, your old password is replaced by the new password. You can now log in to the portal with your username and new password.

5 Homepage Reporting Entity

Once the reporting entity user is logged into the MDES portal the user is redirected to the reporting entity dashboard.

When logging into the system, the main menu items in the top bar (1) (top bar), available tasks (2) and sidebar (3) are visible on the screen.

The user can see the status of the portal in sidebar (4).

Multi Data Exchange Solution | Reports | Reporting entity | Smith, John | EN

Last login: from:

Reporting Entity 999001 - Island Corportate Services

TIN: 999001 | Type of exchange(s): CbC, FATCA, CRS | Status: Stable

FATCA/CRS | CbC

Recent deliveries

Case id	Tax year	Case name	Status	Type of report	MessageRefId	CorrMessageRefId
23988	2019	FC input 999001 2019 Nieuw levering 23988	Collect	CRS701 (New)	CW2019999001.23988.	
22762	2017	FC input 999001 2017 Nieuw levering 22762	Processed	CRS701 (New)	CW2017999001.22762.	
22572	2019	FC input 999001 2019 Nieuw levering 22572	Processed	CRS701 (New)	CW2019999001.22572.	
22434	2018	FC input 999001 2018 Nieuw levering 22434	Collect	CRS701 (New)	CW2018999001.22434.	

New report (manual) + | New report (upload) +

Useful links

- MDES - General user guide
- MDES - FATCA CRS user guide
- MDES - FC XML Schema user guide
- IRS - Information about FATCA
- OECD - Information about CRS
- Frequently asked questions

Reporting Status

The MDES portal is open for reporting entities to submit financial data.

Figure 5-1 RE Homepage

5.1 Menu tab: Reporting Entity

Summary

By default, the information of the Reporting Entity will be displayed. This is the same information as available under the “My account” sub menu.

5.1.1 My account

This paragraph describes the information displayed when viewing an account.

The screenshot displays the 'Reporting Entity 20000076 - Nombre' page. At the top, there is a navigation bar with 'Reports' and 'Reporting Entity' tabs. The breadcrumb trail shows the path: Home / Reporting Entity 20000076 - Nombre / Reporting entity information. The main content area is divided into three sections:

- Section 1 (Header):** A table with the following data:

State	TIN	Type of exchange(s)	Status
Active	20000076	CbC	Stable
- Section 2 (Detail):** A sidebar menu on the left lists 'Reporting entity information', 'Contact person details', 'EOI relations', 'Registered users', and 'Documents'. The main content area shows 'Reporting entity information' with the following details:

Formal/Legal name	Nombre
Tradename	Nombre comercial
Street	Street
House number	6
Address suffix	
Place	City
Reporting period end day	31
Reporting period end month	12
- Section 3 (Task):** A button labeled 'Request amendment exchange type(s)' is located in the top right corner.

Figure 5-2 My account overview

The header section (1) displays the account information from the reporting entity. The information available in the case header are:

- State
- TIN
- Type of exchange(s)
- Status

The detail section (2) displays addition information about the reporting entity. The following information is available:

- Reporting entity information
- Contact person details
- EOI relations
- Registered users
- Documents

The task available for the user will also be displayed (3). The following tasks are available:

- Request amendment exchange type(s)

5.1.1.1 [Task] Request amendment exchange type(s)

With this task the reporting entity user can request to add or remove an exchange type. After the request is completed, the competent authority needs to access the request and if approved the exchange type will be updated and the process is complete. Only the treaties that are applicable are shown.

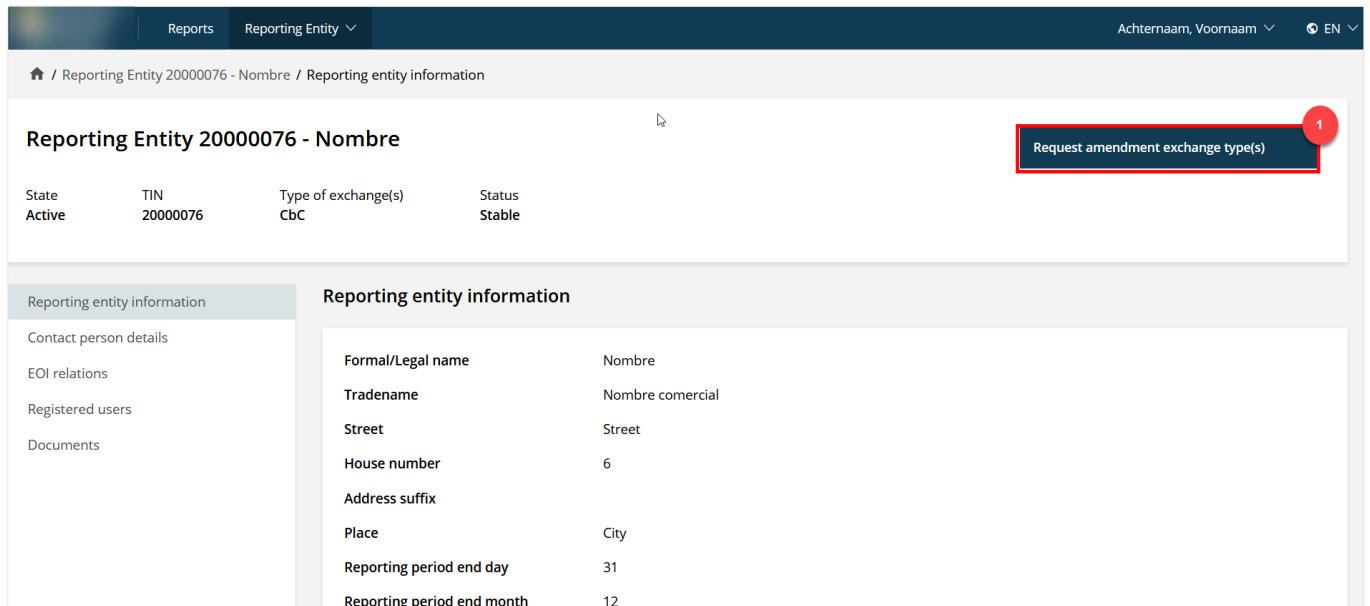


Figure 5-3 My account overview

When clicking on the task **“Request amendment exchange type(s)”** the system navigates to the ‘Request amendment exchange type(s) form. Complete the form by checking or unchecking the exchange type(s) to be added or removed and enter all required information.

Figure 5-4 Request amendment exchange type(s) form
 Clicking “Next” will prompt for a confirmation of the change. After verifying the change, the request will be sent to the Competent Authority by clicking on “Finish”.

Figure 5-5 Request amendment exchange type confirmation screen

5.1.1.2 [Task] Edit user profile

A logged in user can change the profile information by clicking on the task “Edit user profile” (1). The task is located at the top righthand corner.

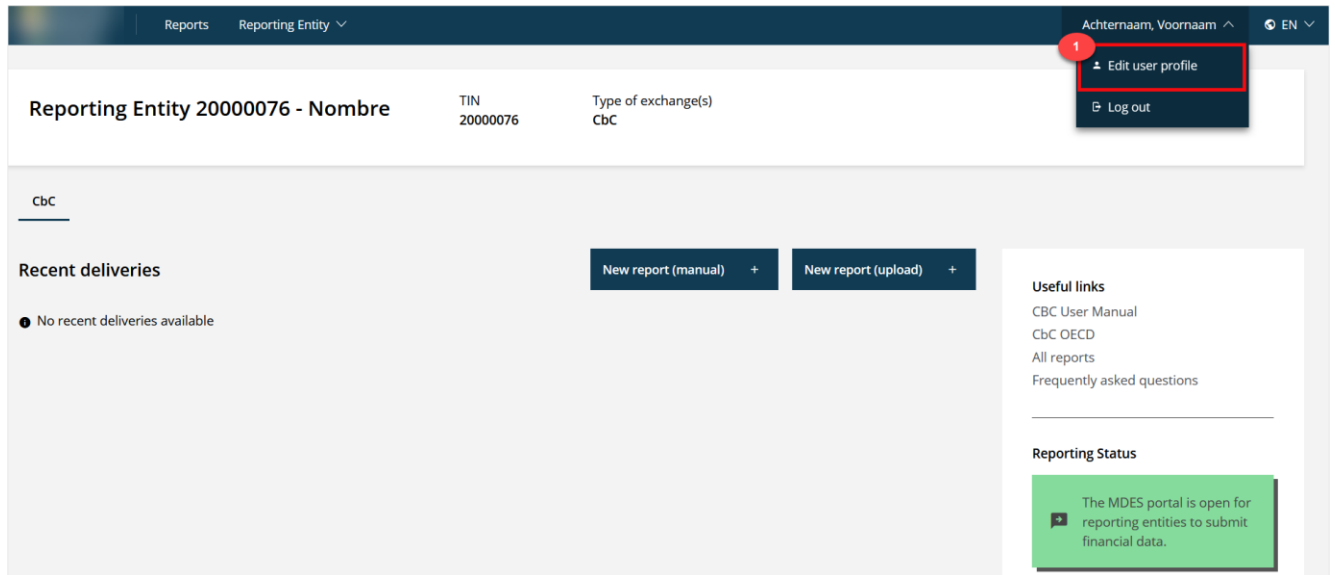


Figure 5-6 Task Edit user profile at the top righthand corner.

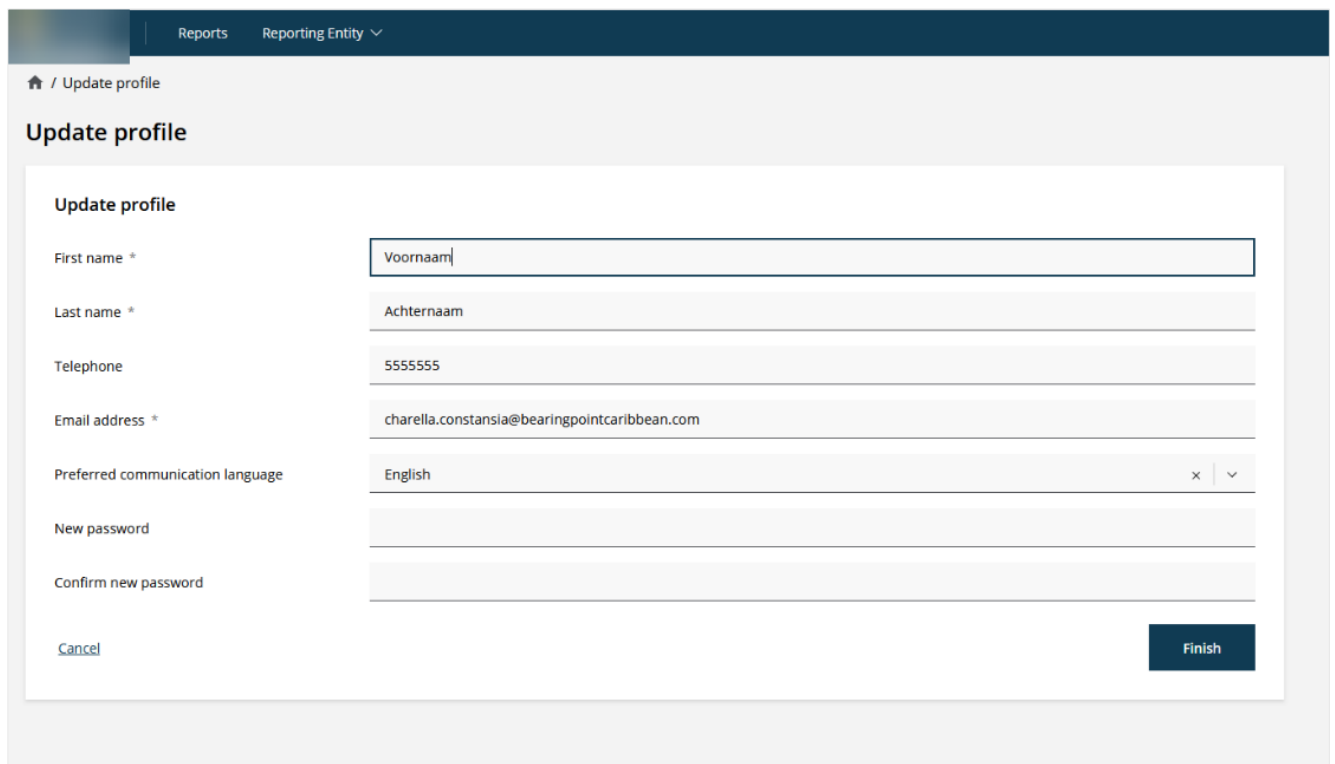


Figure 5-7 Click on the task Update profile and fill in the information

An e-mail will be sent after the e-mail address or password have been changed by the user.

5.1.1.3 [Task] Create reporting entity user

The task “Create reporting entity user” for a Reporting Entity user to create another user is available in the panel Registered users (1).

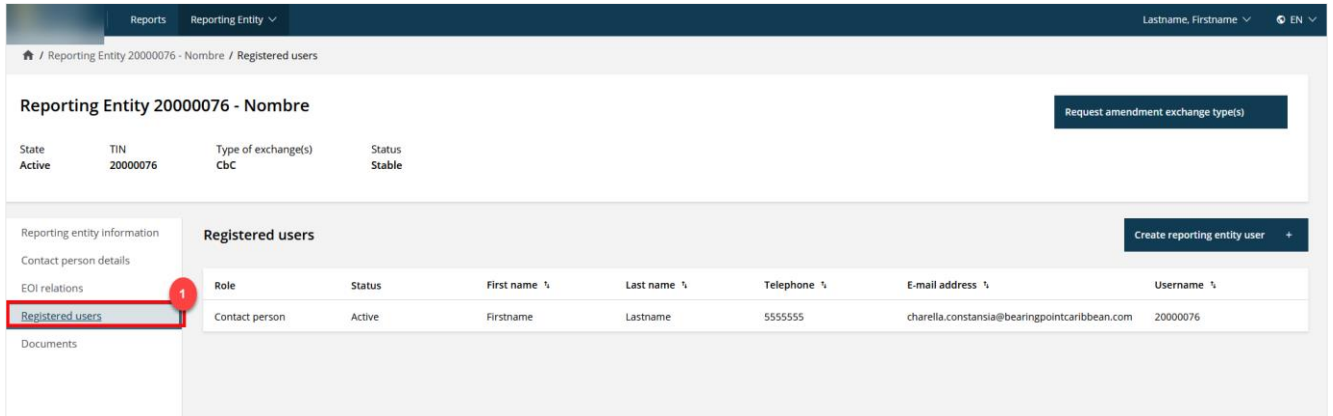


Figure 5-8 My account overview - Registered users

With this task the contact person can create another entity user. This user will then be able to also log in and submit deliveries.

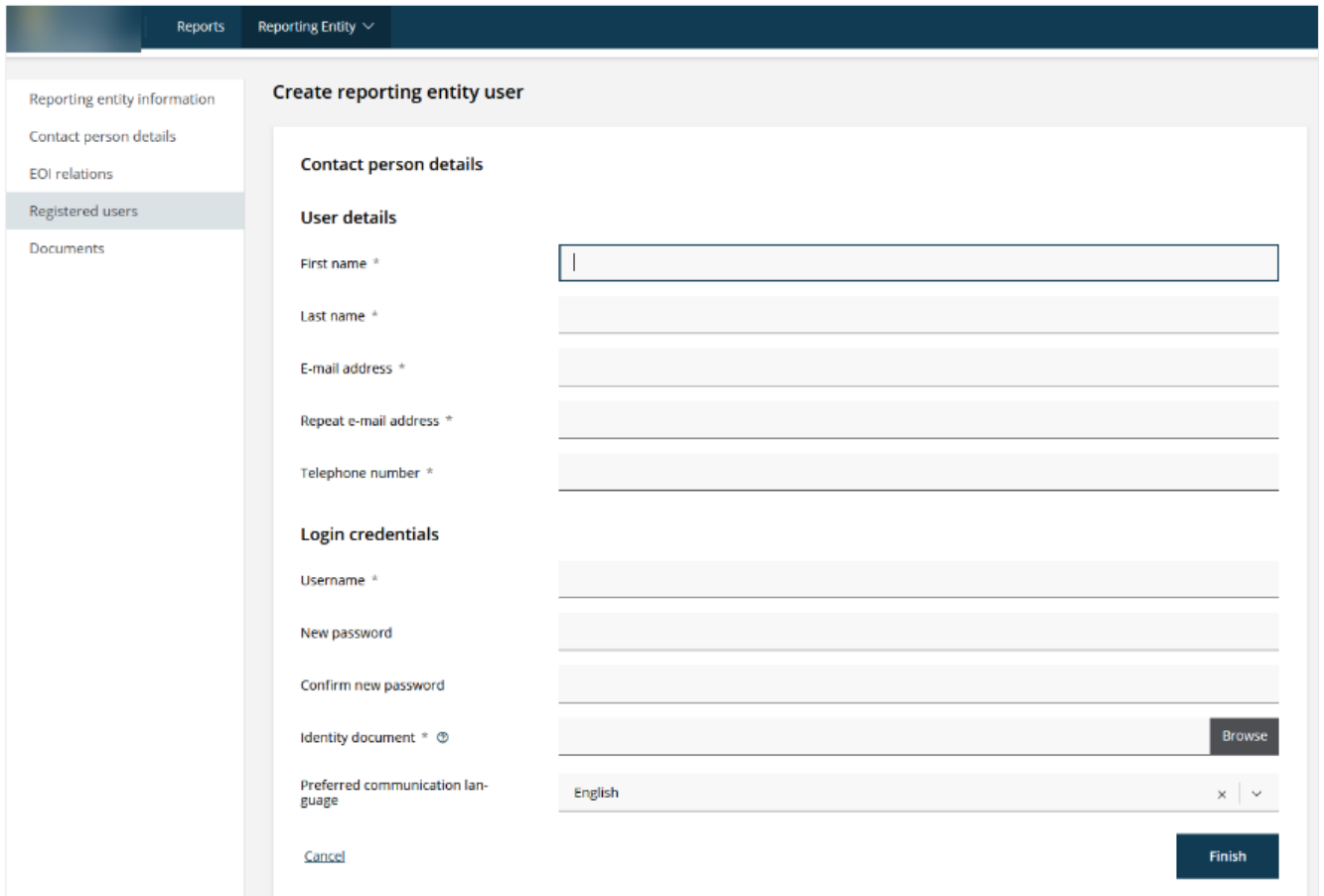


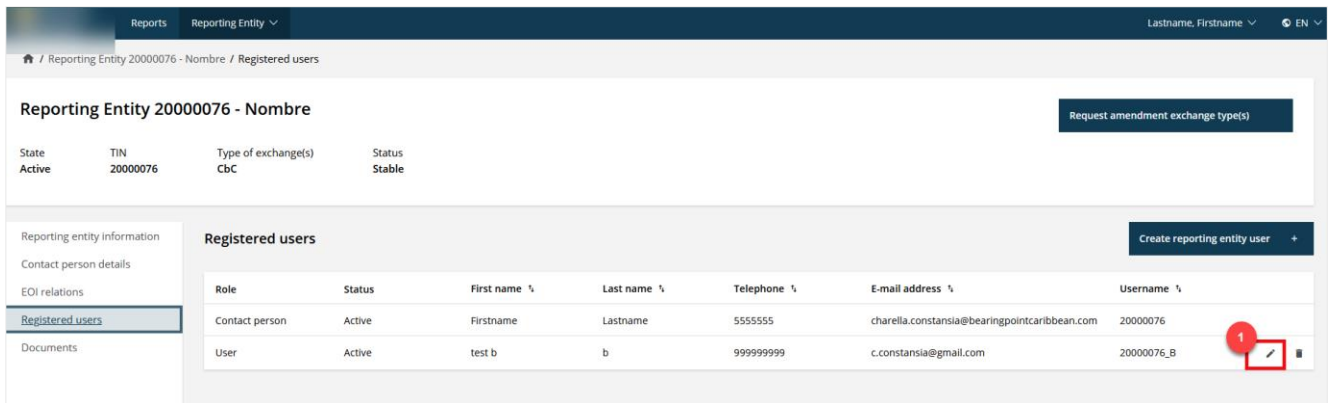
Figure 5-9 Create reporting entity user

To complete the request for a new user, the relevant fields should be entered. All fields with an asterisk are mandatory. If these fields are not entered, the user will receive a notification to complete the mandatory fields before being able to continue to the next screen.

After all information is entered and the Finish button is clicked, the user is created. The first time the user will login, the user will be prompted to set a new password.

5.1.1.4 Transfer administrator role

It is possible to transfer the role of administrator to the new user. By doing this, the first user will not be an administrator anymore. This can be done by clicking on the Pencil icon (1).



A confirmation screen will appear where you need to agree on the change for it to be applied. By selecting “Yes” and clicking on “Finish” the role is transferred to the new user. The user will need to login again.

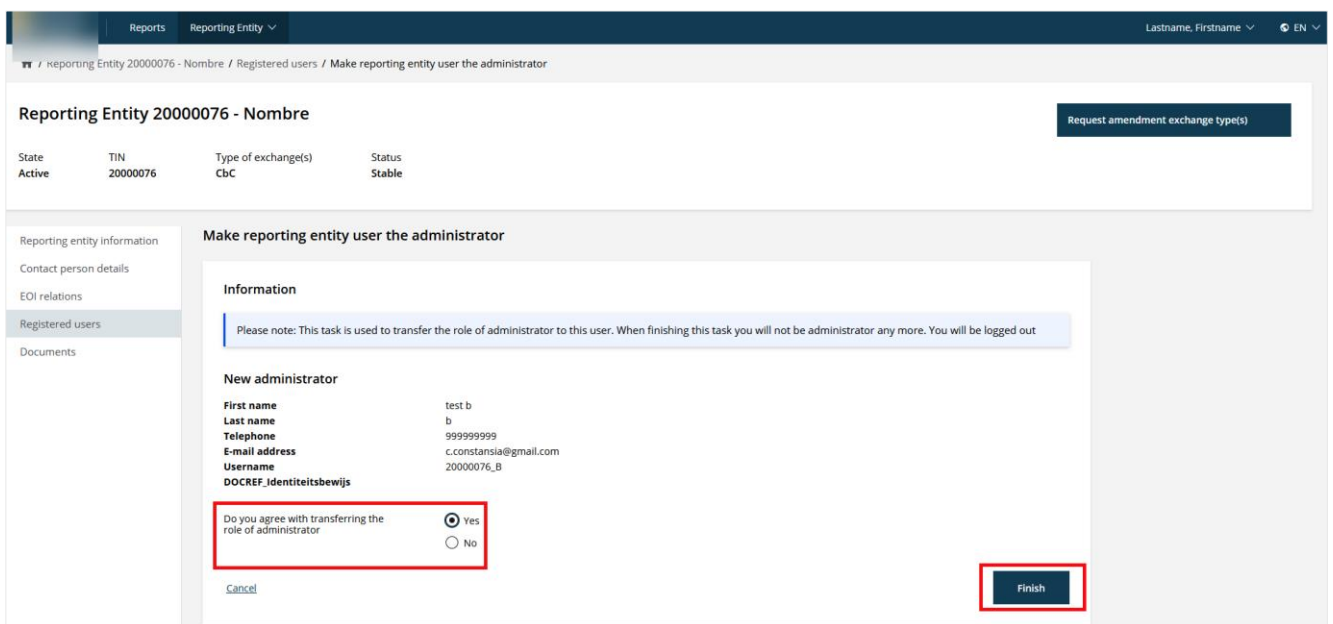


Figure 5-10 Transfer administrator role

5.1.2 My requests

Summary

The “My request” tab (1) shows all the requests of the reporting entity.

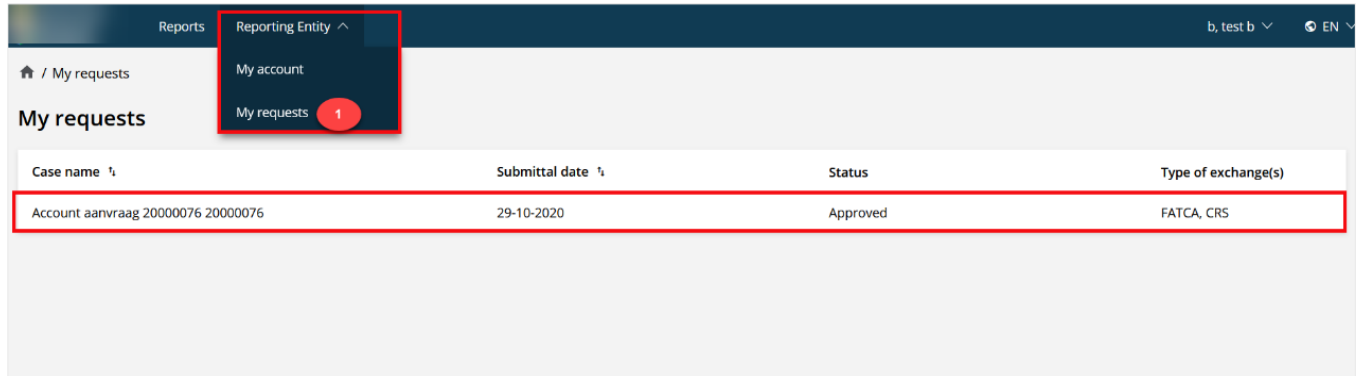


Figure 5-11 My request tab

By clicking on a request, it will open a screen with detailed information regarding the request.

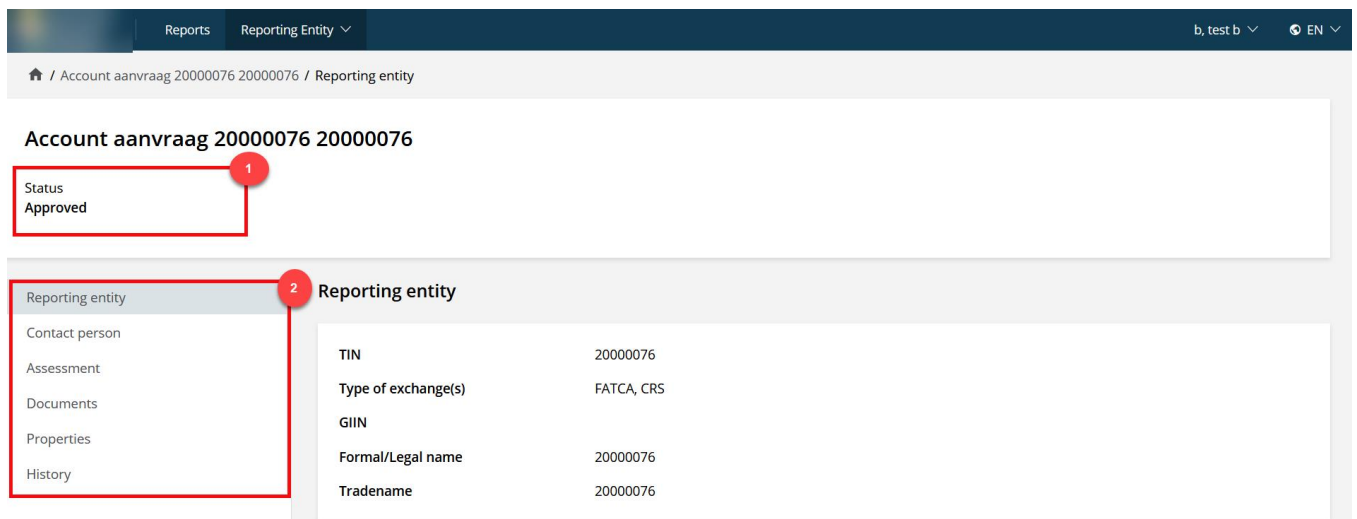


Figure 5-12 My request information

In the header, the status of the request is shown (1).

The panels with the different information regarding the request are (2):

- Reporting entity
- Contact person
- Assessment
- Documents
- Properties
- History



BearingPoint®