swisscom

C1 - Public

Two Factors Authentication Phase 2

Content

1 Introduction

In the second phase, the functionality of the two-factor authentication (2FA) is activated. This means that after activating a 2FA type, a user must go through the appropriate login procedure.

2 Auswahl de34r 2FA

Swisscom Wholesale has created three new options for increasing security when entering the wholesale portal:

1. Mobile ID → Excellent security
   When logging in, the user is prompted to authenticate with their Mobile ID on their mobile device.
   If you do not know the offer of Mobile ID yet, you can find information on:
   https://www.mobileid.ch/en
2. SMS/TAN → Good security
   The user is prompted at login to enter a token for confirmation.
   The token is sent via SMS to the stored mobile device.
3. eMail/TAN → Minimal security
   The user is prompted at login to enter a token for confirmation.
   The token will be sent via email to the deposited email address.

2.1 Right choice of the 2FA type

The right choice depends on the communication options that a user of the customer can use. The aim must be to use the highest possible security when registering.

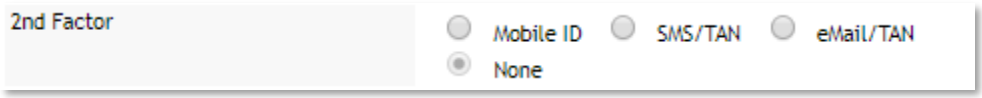


Illustration 1, 2ter Factor

When phase 2 goes live, all accounts will still be migrated without a 2FA type. The accounts will have a "None" active in the 2FA type.

This ensures a smooth implementation of the 2FA.

However, as a superuser or admin, you can always set your users to a higher security level from 03.04.2019.

1. In the best case, your users already use Mobile ID, then you should definitely activate this security level.
2. If your users have mobile devices but no Mobile ID then you should enable the SMS/TAN level.
3. However, if your users do not have a mobile device, you will need to activate the minimum level with the eMail/TAN.

Hints:

A) As soon as you have selected one of the new 2FA types, you can no longer reset the type to "None".

B) When you create new users, you now have only the three 2FA types to choose from. Always use the highest possible level of security for your users.

2.2 Requirements for the 2FA types

The following requirements are necessary for each 2FA type. The superuser tool will alert you accordingly to missing information.

	2FA Type	Mandatory fields
1.	Mobile ID	Last name / Email / Mobilephone
2.	SMS/TAN	Last name / Email / Mobilephone
3.	eMAil/TAN	Last name / Email

table 1, Mandatory fields for 2FA Types

The yellow marked selection of the User Type is visible only to the superuser.

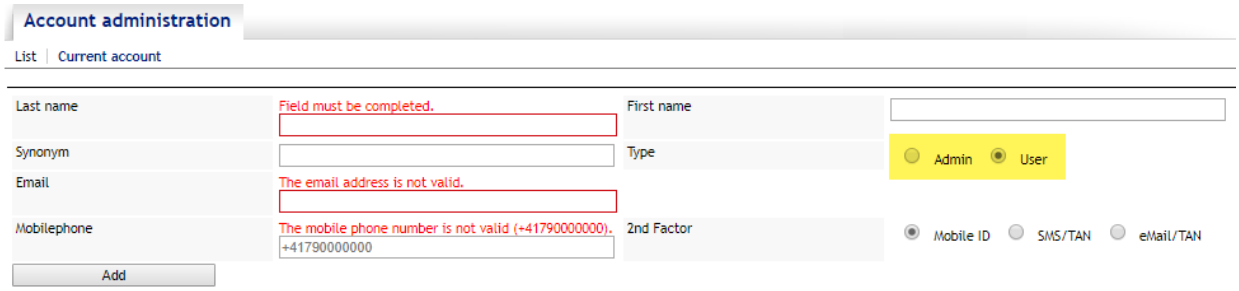


Illustration 2, mandatory fields for 2nd dactor = Mobile ID

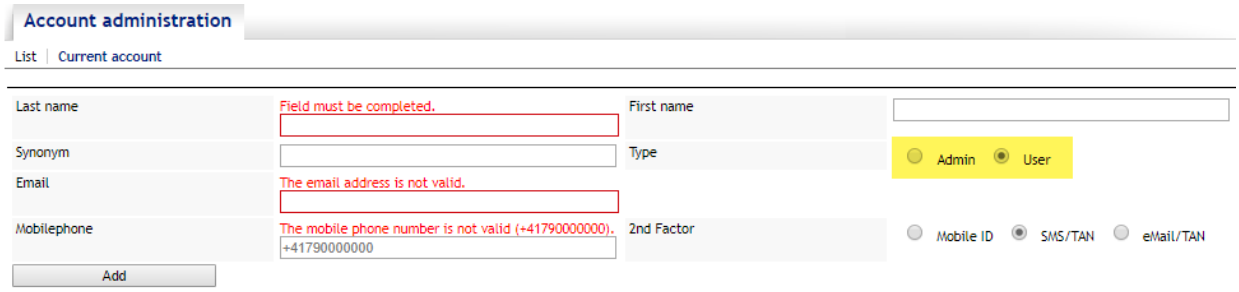


Illustration 3, mandatory fields for 2nd factor = SMS/TAN

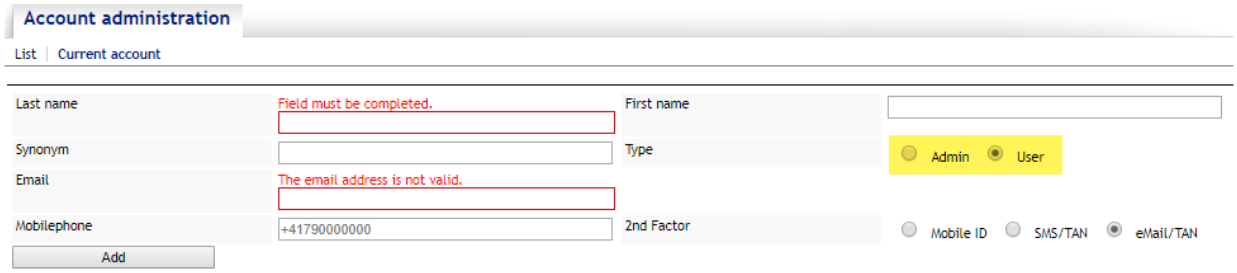


Illustration 4, mandatory fields for 2nd factor = eMail/TAN

3 Password validity and delay of deactivation

In phase 2 the password validity and the delay of the deactivation are not yet hard set. This will only happen in phase 3.

However, we ask you to consider this for new accounts or mutations on existing accounts already now. And to set the two values according to only 120 days.

4 Creation of a new account

The creation of a new account is the same as today, with the changes in the choice of the 2FA type mentioned in chapter 1. The registration of the mobile number has already been possible since 06.02.2019.

5 Effect of 2FA on user registration

What changes for the user when logging in the Wholesale Portal concretely.

The user logs in as usual with his synonym or PUI and the password and confirms with <Login>.

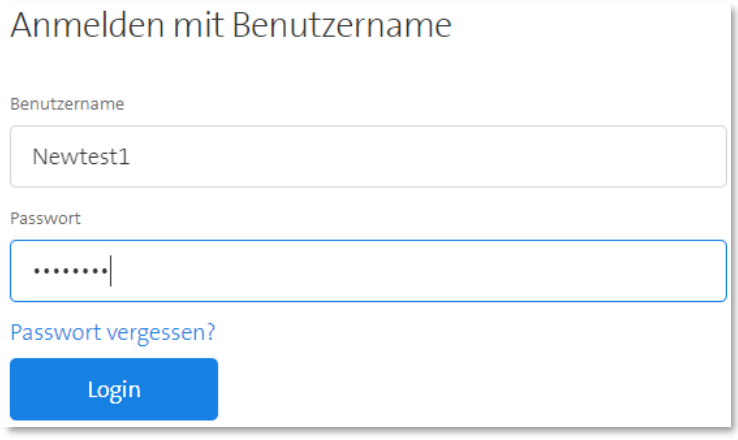


Illustration 5, user login start

The further procedure differs depending on the used 2FA type.

5.1 Login with Mobile ID

After login the following information is displayed to the user.

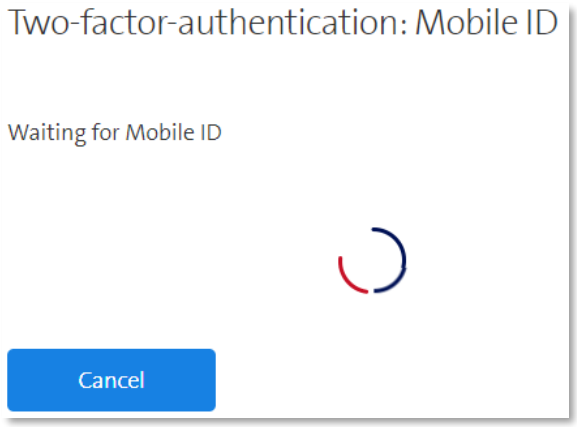


Illustration 6, user login stepp 1, Mobile ID

Now the user on the mobile device is prompted to enter his mobile ID.

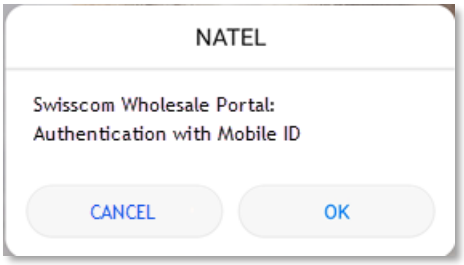


Illustration 7, user login step 2a, Mobile ID

Continue with <OK> the user enters the Mobile ID PIN.

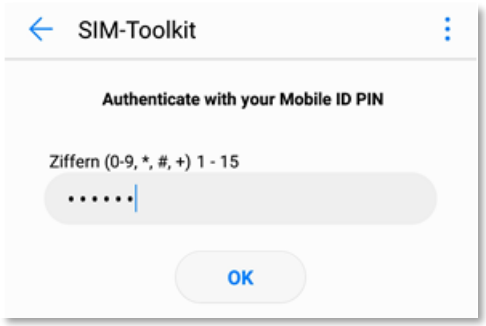


Illustration 8, user login step 2b, Mobile ID

Confirm the entry again with <OK>.

Done, the portal opens.

5.2 Login with SMS/TAN

After login the following information is displayed to the user.

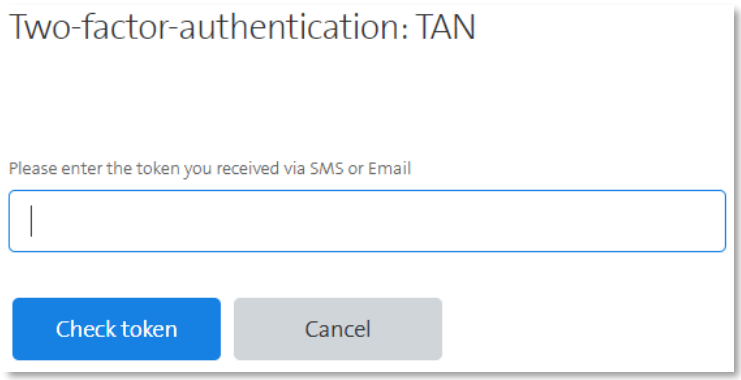


Illustration 9, user login step 1, SMS/TAN

Now the user receives an SMS with the token on the mobile device.

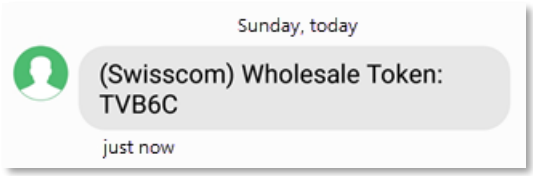


Illustration 10, user login step 2, SMS/TAN

Enter this token in the mask and conclude with <Check token>.

Done, the portal opens.

5.3 Login with eMail/TAN

After login the following information is displayed to the user.

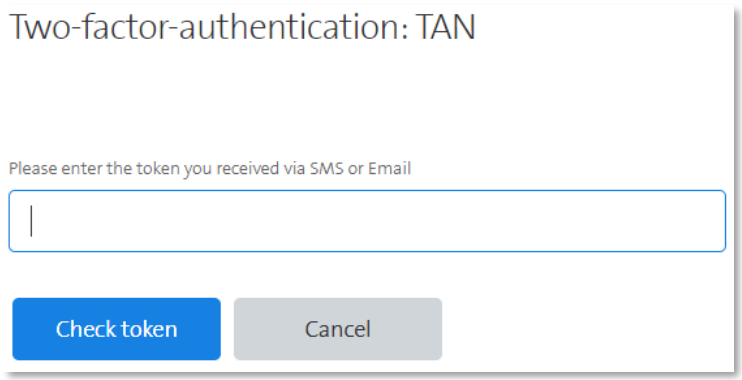


Illustration 11, user login step 1, eMail/TAN

Now the user receives an email account with the token.

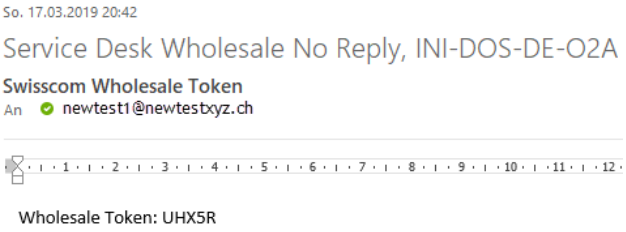


Illustration 12, user login step 2, eMail/TAN

Enter this token in the mask and conclude with <Check token>.

Done, the portal opens.

6 Sender email address from 2FA

You potentially use filters for incoming emails to keep your own network secure.

The eMail/TAN from the 2FA will reach you with the following email address:
NoReply.ServiceDeskWholesale@swisscom.com

This allows you to check at your email entry whether an email is from the 2FA of the Swisscom portal or not.

After the implementation of phase 3, emails for the validation of amendments will also be sent with this email address.

7 Self-test for a user's Mobile ID

A user can test their mobile number to see if the Mobile ID works properly.

The following link serves this purpose: https://www.mobileid.ch/en/faq

On the website, continue with <Test Mobile ID>. The dialog is clear and guides you through an SMS confirmation to enter the Mobile ID.

8 Enhanced reports

Since capturing the email address and the mobile number is important for the next implementation phase, since February 6, you have the option to export your accounts in a table.

This allows you to easily check the status of the users you manage.

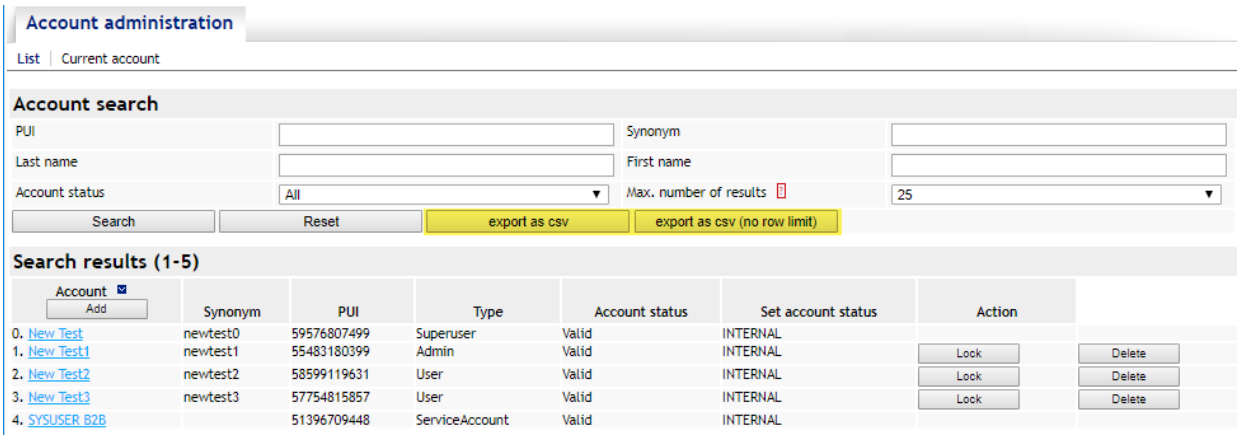


Illustration 13, user reports

With <export as csv> you get the maximum number of entries defined under "Max. Number of results". You can increase the number in the corresponding field.

Or you use <export as csv (no row limit)> to get all your users at once.

	A	B	C	D	E	F	G	H	I	J	K
1	Account	Synonym	PUI	Type	Role	Source	Email	Mobilephone	2nd Factor Type	Account Status	Last Login
2	New Test	newtest0	59576807499	Superuser	-	INTERNAL	newtest0@newtestxyz.ch	+41012345678	NONE	Valid	17.03.2019 15:04
3	New Test1	newtest1	55483180399	Admin	-	INTERNAL	newtest1@newtestxyz.ch	+41012345678	EMAILTAN	Valid	15.03.2019 17:27
4	New Test2	newtest2	58599119631	User	-	INTERNAL	newtest2@newtestxyz.ch	+41012345678	MOBILETAN	Valid	14.03.2019 17:25
5	New Test3	newtest3	57754815857	User	-	INTERNAL	newtest3@newtestxyz.ch	+41012345678	MID	Valid	14.03.2019 17:27
6	SYSUSER B2B	null	51396709448	ServiceAccount	-	INTERNAL	sysuser@newtestxyz.ch	+41012345678	NONE	Valid	17.03.2019 17:45

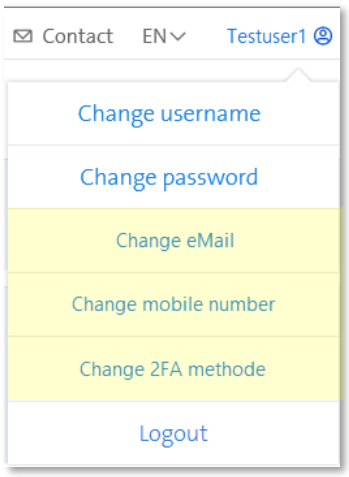
Illustration 14, example user report

9 Outlook for phase 3

The introduction of Phase 3 is scheduled for the end of May 2019. Details will be communicated to you ahead of time.

In the following chapters you will find a preview of what we are currently working on.

9.1 Self-care by the user



Analogous to the name or password change in the entry mask, the self-care of the new user data by the user is enabled in phase 3.

Users will be able to get their email address and to maintain your mobile number yourself.

It is still unclear whether the choice of the 2FA method can be released for the user.

Illustration 15, new self-care

9.2 Change of settings

With the implementation of Phase 3, some settings change:

- The remaining users, who still have the 2FA type "None", are set to the 2FA type "SMS / TAN". Exceptions for setting the minimum level "eMail / TAN or even leaving it to" None "must be requested and justified by the superuser at their wholesale account.
- For all users (superuser, admin and user) the two values for "Password validity" and "Deactivation delay" are set to 120 days.
- The service accounts for web services are not affected by Phase 3. They are already decoupled and maintained by Swisscom.

Effects:

If a user does not have sufficient information at the time of going live of Phase 3, the next time he is asked to do so, he will be asked to supplement his missing information with the self-care mentioned above.

Of course, users can be supplemented before the live production of Phase 3 by the superuser and admin accordingly. This would certainly facilitate the introduction for the users.

9.3 Validation of mutations

With phase 3, a validation message will be generated for changes on the user account (user name, password, eMAil address, mobile number, 2FA method).

Exceptions are changes made by a superuser, admin or Swisscom.

With this validation, the user can immediately recognize if a stranger is trying to change his or her account.

9.4 Initially transfer protected passwords

Initial passwords are now transferred directly to the user without the producer seeing them. For this purpose, an SMS will be sent to the stored mobile number or, if none exists, an e-mail to the stored eMail address.

A corresponding advertisement will inform the superuser or admin about the information sent.

10 Further improvements

In view of the constant security risks, we at Swisscom Wholesale will take further steps to best protect your and our data.

In addition, we also want to refresh the look and feel of the superuser tool and align it with the interface of the portal.

11 Appendix

11.1 List of figures

11.2 List of tables