

From	To be sent to
Swisscom (Switzerland) Ltd	SuperUsers and Admins
Date	
21.02.2022	
Topic:	
User administration for the Swisscom Wholesale Portal	

Swisscom Wholesale Portal User Administration

Doc ID	Handbook Wholesale Portal
Version:	2-0
Replaces version	1-0
Issue date	21/02/2022
Valid from	21/02/2022
Valid until	Recall
Document name	EN_Handbook_Wholesale_Portal_Superuser_Admin_V2-0.docx

Table of contents

1.	Introduction	3
1.1.	Goal and purpose	3
1.2.	Document scope.....	3
1.3.	Target audience	3
1.4.	Portal access requirements	3
1.5.	Wholesale Portal out of service.....	3
1.6.	Terms, abbreviations.....	4
1.7.	Updates	4
1.8.	Reference documents	4
2.	Brief outline of Wholesale Portal Access	5
2.1.	Access to the Swisscom Wholesale Portal.....	5
2.2.	Two-factor authentication	5
2.3.	Whitelist	6
2.4.	User roles and access	8
3.	Superusertool functionalities.....	9
3.1.	Opening the Superusertool	9
3.2.	User account set-up.....	11
3.3.	Add user rights.....	14
3.3.1.	Additional data for WSG rights	14
3.3.2.	Distinction between production and test for WSG rights.....	14
3.4.	Export user report	15
3.5.	View of customer master data	16
4.	Annex.....	17
4.1.	Further information about the 2FA solution	17
4.1.1.	2FA e-mails.....	17
4.1.2.	Sending SMS with 2FA	17
4.2.	Best practice	17
4.2.1.	Efficient new user creation and notification	17
5.	Annex.....	18
5.1.	List of tables	18
5.2.	List of figures:.....	18

1. Introduction

Swisscom (Switzerland) Ltd provides the Wholesale Portal to give you quick and easy customer access to Swisscom's wholesale offers.

The Wholesale Portal affords an overview of your entire portfolio of services purchased from Swisscom (Switzerland) Ltd.

SuperUser accounts and *Service Accounts* for web services are set up and administered by Swisscom Wholesale.

As *SuperUser*, you can set up and administer additional user accounts for your company. You can also define administrators (*Admin*), who in turn can set up users for your company.

1.1. Goal and purpose

This document outlines how to set up new users and the rights and roles that can be assigned.

It also outlines additional options for you to access the Wholesale Portal.

1.2. Document scope

This document was created for *SuperUsers* and *Admins* of the Wholesale Portal of Swisscom (Switzerland) Ltd. User permissions are described in the separate document *User Rights Matrix Overview.pdf*.

1.3. Target audience

This Handbook is for *SuperUsers* and *Admins* of wholesale customer companies who have a valid contract for usage of the Wholesale Portal.

1.4. Portal access requirements

The portal contract and the corresponding product contracts must be signed in order to access all of the functionalities of the Wholesale Portal. Products are released in the portal and are available upon signing of the contracts.

1.5. Wholesale Portal out of service

If the portal is out of service due to a fault, please contact the service desk during office hours (OH) on **0800 803 803**.

During non-office hours (NOH), please send an e-mail to: servicedesk.wholesale@swisscom.com

1.6. Terms, abbreviations

Term	Description
2FA	Two-factor authentication for login to the Wholesale Portal
WSG	Web Service Gateway for the wholesale bulk business

Table 1: Terms and abbreviations

1.7. Updates

Date	Description
21/07/2019	Completely new version
21/02/2022	addition

Table 2: Updates

1.8. Reference documents

Ref. no.	Document name/ID
1	Overview User Rights Matrix.pdf
2	Handbook Wholesale Portal - Users.pdf
3	Terms of use of the Wholesale Customer Portal.pdf
4	Anhang zu Nutzungsbestimmungen-Portal.pdf

Table 3: Referenced documents

2. Brief outline of Wholesale Portal Access

2.1. Access to the Swisscom Wholesale Portal

The prerequisite for access is signing of the "Terms of use of the Wholesale Customer Portal".

All users of the Swisscom Wholesale Portal must complete an authentication procedure in the **Powergate** of Swisscom (Switzerland) Ltd.

You as a customer have the option of access via the web interface (WebGUI).

Web services are additionally offered for access to Swisscom services which also require authentication via the **Powergate**.

Access is authenticated in the **Powergate** and allowed in accordance with the stored authorisations for the customer and user.

Access is administered via the **Superusertool** which you have access to as the customer's *SuperUser* or *Admin*.

2.2. Two-factor authentication

Two-factor authentication (2FA) has been introduced for accessing the Swisscom Wholesale Portal to enhance the security of customer data and the services to be provided.

Distinction is made between the following 2FA methods.

1. **Mobile ID** → Excellent security
At login, users are prompted to authenticate via Mobile ID on their mobile device.
If you are unfamiliar with the Mobile ID procedure, information is available here:
<https://www.mobileid.ch/en>
2. **SMS/TAN** → Good security
Users are prompted to enter a token at login for verification.
The token is sent via SMS to the mobile device number on file.
3. **eMail/TAN** → Low security
Users are prompted to enter a token at login for verification.
The token is sent via e-mail to the e-mail address on file.
This 2FA type can only be assigned to user type *User*. *SuperUser* and *Admin* must use one of the two types, Mobile ID or SMS/TAN, for better security.
4. **None** → No 2FA is applied.
This 2FA type is exclusively assigned to the user type *Service Account*. The *Service Accounts* receive access to the portal without using a 2FA.
The following requirements apply for setting up *Service Accounts*:
 - a. It is mandatory that the customer has an active whitelist.
 - b. The whitelist usage is of the type "Only for Service Accounts" or "For all Accounts".
More on this in chapter 2.3.

Important advisories:

- *SuperUser* and *Admin* must be careful to ensure that the highest respective security level is enabled for their users. Confirmation via Mobile ID and SMS/TAN is usually faster than with eMail/TAN, affording a more efficient workflow.
- There is no cost to the user for use of Mobile ID or SMS/TAN.
- The eMail/TAN solution is only offered as a fall-back solution if users do not have mobile devices at the customer's site or are not allowed to use them at the workplace. If this solution is necessary for access by your users, a request must be filed with your Swisscom Wholesale account manager.
- 2FA cannot be activated for *Service Accounts*. These accounts are operated with 2FA "None". Accordingly, it is necessary to set up and activate a whitelist. For this solution to be used, the *SuperUser* must disclose the IP addresses from which his *Service Accounts* will access the Wholesale Portal. This data flows into a whitelist which is referenced at login. More on this in chapter 2.3.

2.3. Whitelist

The IP addresses entered in the whitelist (individual addresses or IP ranges) define from which IP addresses certain users may log into the Wholesale Portal.

It is mandatory to set up and activate a whitelist for the customer ...

- if the customer uses *Service Accounts* for a B2B connection.
The whitelist usage of the type "**Only for Service Accounts**" is used for this purpose. In this way, the authenticity of accesses from *Service Accounts* with the 2FA type None is additionally guaranteed by comparison with whitelist entries.
- if all user accesses of a customer are to take place exclusively from his network, the control can be extended to all users by means of whitelist.
With the whitelist usage of the type "**For all Accounts**", a check of the outgoing IP addresses is activated for all users.

The definition of the whitelist entries and the Whitelist Usage is made by Swisscom when setting up a customer. Changes to this information require a request from the SuperUser and are also made by Swisscom.

By selecting the whitelist usage type, you can define how the whitelist information affects the user login.

The following table shows the dependencies that apply.

"IP WhiteList usage" Type	Whitelist needed?	User type	2FA type			
			Mobile ID	SMS/TAN	eMail/TAN	None
Not used	No	<i>User</i>	X	X	X ¹⁾	
		<i>Admin</i>	X	X		
		<i>SuperUser</i>	X	X		
		<i>Service Account</i>	No Service Accounts allowed			
Only for Service Accounts	Yes	<i>User</i>	X	X	X ¹⁾	
		<i>Admin</i>	X	X		
		<i>SuperUser</i>	X	X		
		<i>Service Account</i>				X
For all Accounts	Yes	<i>User</i>	X	X	X ¹⁾	
		<i>Admin</i>	X	X		
		<i>SuperUser</i>	X	X		
		<i>Service Account</i>				X

	The 2FA must always be applied
	User access is checked via the whitelist. An attempt by one of these user types to log in from another IP address than stored in the whitelist leads to the standard error message "Invalid net: You are trying to connect from an unsupported net."
X ¹⁾	The assignment of the 2FA type eMail/TAN is only added upon request by the <i>SuperUser</i> .

Table 4: Whitelist dependencies

2.4. User roles and access

Various user roles are defined to ensure a high level of security for customer data and the services to be provided.

Swisscom creates the user account of the customer's *SuperUser* upon conclusion of a portal contract and subsequently administers it.

A *SuperUser* can create new users and grant them *Admin* rights.

An *Admin* can create additional new users, but not further *Admins*.

Users with a *SuperUser* or *Admin* role are responsible for creating and managing their user accounts. They open their user accounts and assign appropriate rights to each user.

The rights to be assigned depend on the roles and the type of access specified per contracts with Swisscom Wholesale. See the document [User Rights Matrix.pdf](#) for an overview of user rights.

Users and *Admins* contact their *SuperUser* for any questions regarding administration of rights and authorisations.

The *SuperUser* can call the Wholesale Service Desk on **0800 803 803** or contact the Desk by e-mail at servicedesk.wholesale@swisscom.com.

3. Superusertool functionalities

3.1. Opening the Superusertool

Access is via WebGUI at the URL: <https://wholesale.swisscom.com>

On the start screen, the number originally received with the account (PUI no.) or the name subsequently linked as synonym may be used.

See chapter 3.2 on generating a synonym.

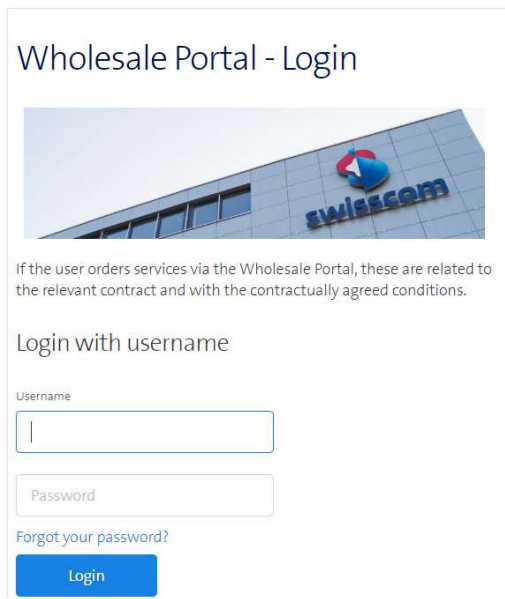


Figure 1, Wholesale Portal login

Confirm the username and password entered via **Login**.

One of the following screens then appears depending on the 2FA method you are employing.

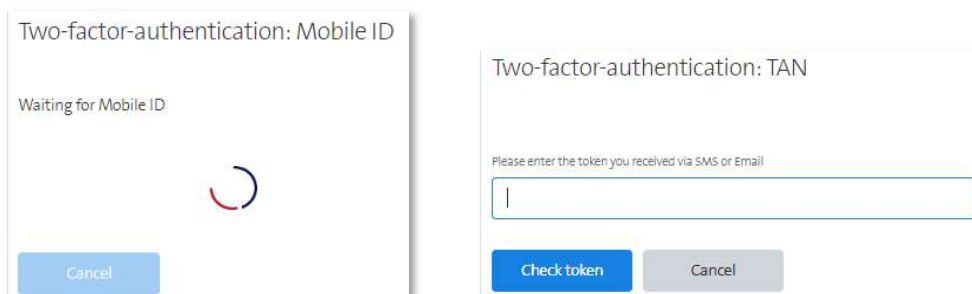


Figure 2, 2FA confirmation

Enter the Mobile ID on your mobile device or copy and paste the token sent to you into the corresponding field on the screen.

When you have successfully logged in, you see the start page for online services.

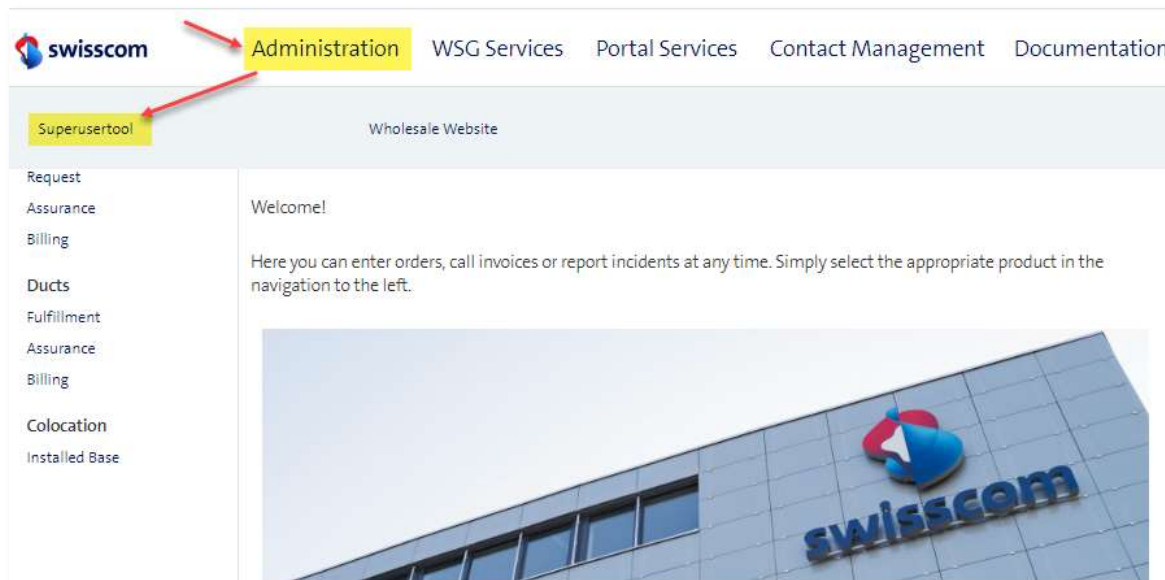


Figure 3, Wholesale Portal start page

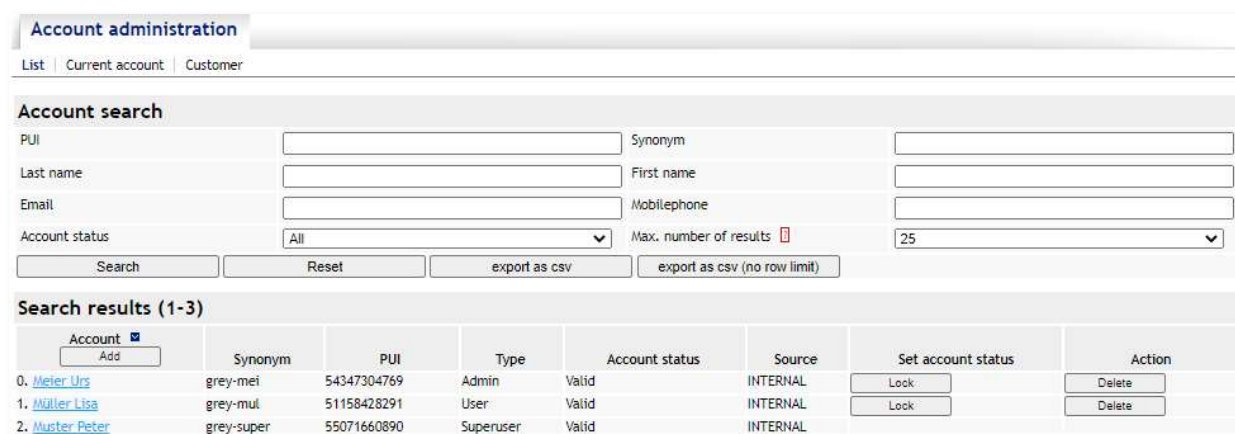
Click on **Administration** to navigate to the menu item **Superusertool**. Click again to navigate to administration of your user accounts.

Note:

If the **Superusertool** functionality is available, the user account is lacking the required user type "Admin". The user type "Admin" is only assignable by the **SuperUser**. See also Figure 7, page 12,

You can click on Search to get an organised list of all of your users, stating user type and current account status.

You can utilise various search criteria found in the upper part of the screen for targeted searching.



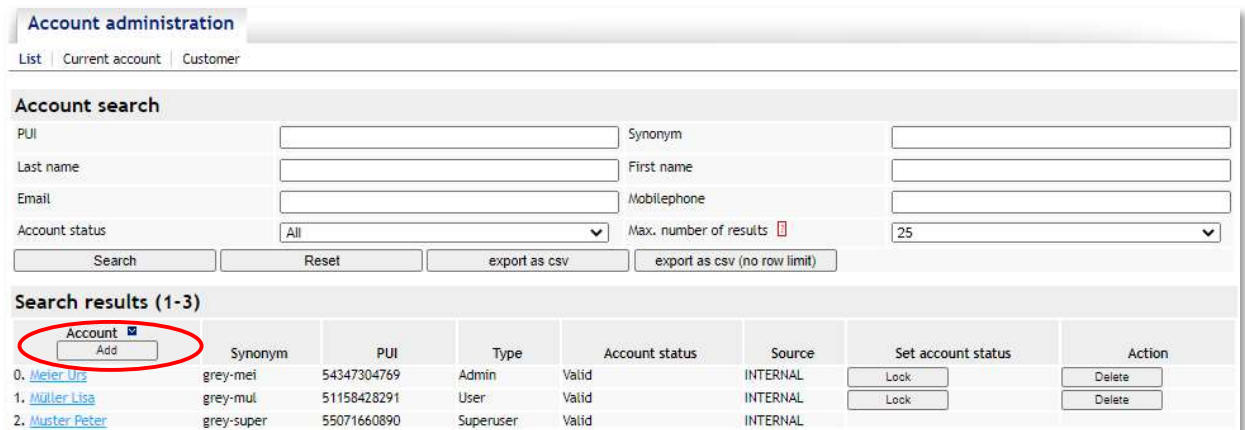
Account	Synonym	PUI	Type	Account status	Source	Set account status	Action
0. Meier Urs	grey-mei	54347304769	Admin	Valid	INTERNAL	<input type="button" value="Lock"/>	<input type="button" value="Delete"/>
1. Müller Lisa	grey-mul	51158428291	User	Valid	INTERNAL	<input type="button" value="Lock"/>	<input type="button" value="Delete"/>
2. Muster Peter	grey-super	55071660890	Superuser	Valid	INTERNAL		

Figure 4, List of accounts

Here you can use **Lock** to quickly lock out a user or **Delete** to delete a user. A locked user may be reactivated at any time via **Unlock**. Once deleted however, a user would have to be recreated.

3.2. User account set-up

To create a new account you have to click the button **Add**.



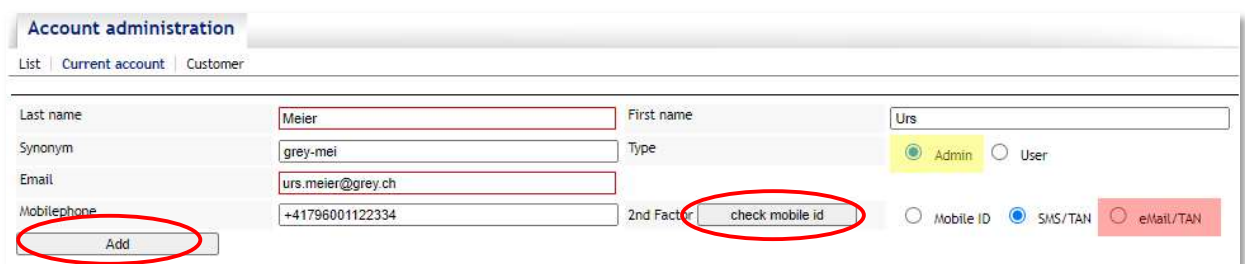
The screenshot shows the 'Account administration' interface. At the top, there are tabs for 'List', 'Current account', and 'Customer'. Below this is the 'Account search' section with input fields for PUI, Last name, First name, Email, Mobilephone, and Account status. There are also buttons for 'Search', 'Reset', 'export as csv', and 'export as csv (no row limit)'. Below the search section is a table titled 'Search results (1-3)'. The table has columns: Account, PUI, Type, Account status, Source, Set account status, and Action. The 'Account' column has a red circle around the 'Add' button. The table lists three accounts: 0. Meier Urs (Admin), 1. Müller Lisa (User), and 2. Muster Peter (Superuser).

Account	PUI	Type	Account status	Source	Set account status	Action
0. Meier Urs	grey-mei	Admin	Valid	INTERNAL	Lock	Delete
1. Müller Lisa	grey-mul	User	Valid	INTERNAL	Lock	Delete
2. Muster Peter	grey-super	Superuser	Valid	INTERNAL	Lock	Delete

Figure 5, Current accounts, new accounts

Enter the new user's surname and first name and confirm your entries by hitting **Add**.

You can specify a synonym in the field so you do not have to remember the long PUI number that is created after adding. This simplifies initial login for a new user.



The screenshot shows the 'Account administration' interface for adding a new account. It has input fields for Last name, First name, Synonym, Email, and Mobilephone. There are radio buttons for 'Admin' (selected) and 'User'. There is a '2nd Factor' section with radio buttons for 'Mobile ID', 'SMS/TAN', and 'eMail/TAN'. There is a 'check mobile id' button. There is an 'Add' button. There is a red circle around the 'Add' button and a red circle around the 'check mobile id' button.

Figure 6, Setting up a new account

The selection choice marked in yellow for creating a new **Admin** is only available to the **SuperUser**. The **SuperUser** can also convert an existing user into an **Admin**.

The selection choice marked in red of **eMail/TAN** as 2FA is only available if the **SuperUser** has agreed a corresponding exception with the Swisscom Wholesale account manager.

A greater level of security via **Mobile ID** or **SMS/TAN** is required for **SuperUsers** and **Admins**.

The button "Check mobile ID" is for verifying whether a mobile number is ready for **Mobile ID**. The check result is displayed just above the mobile number.

After completing the fields and generating the account using the **Add** button, the advanced display appears showing the following details.

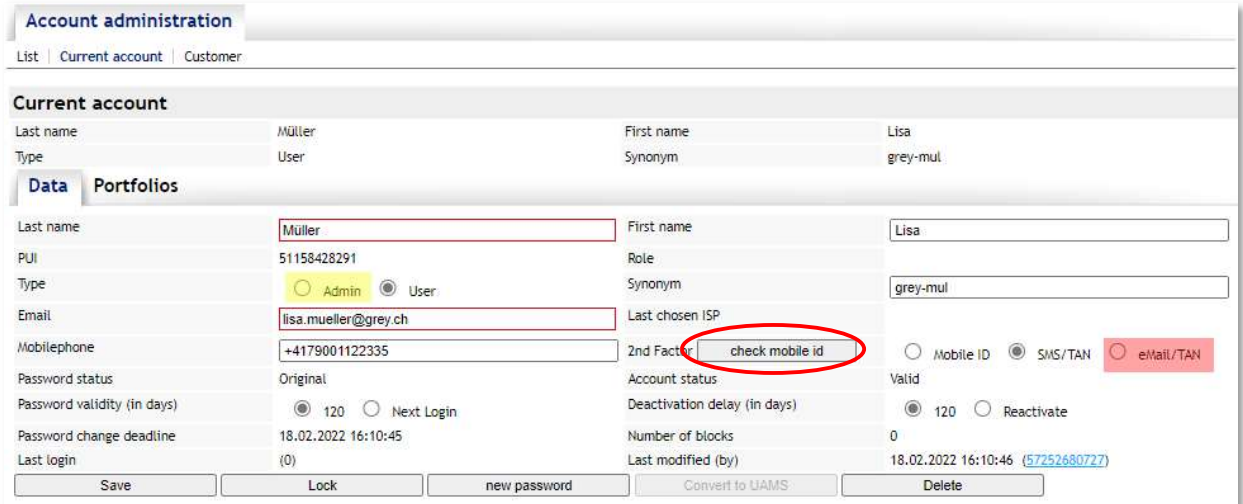


Figure 7, Current account, details, data

The restrictions outlined in the text above apply for the selection choices marked in yellow and red.

The user has been assigned a unique PUI number.

The Check mobile ID button can also be used on this screen to check whether a mobile number is ready for Mobile ID.

Password validity

- The default password validity horizon value is **120** days.
- The function **Next Login** can be used at any time to force a password change at the next login.

Deactivation delay

- The default setting for user account deactivation is **120** days. The user account status changes to "Account expired" if there is no login for more than 120 days. After another 360 days without login the account is deleted by the system.
Users are notified in good time of an impending deactivation. Thus, they receive an info email 30 days before the 120 days expire. If there is no reaction to this, a reminder email is triggered 7 days before the 120 days expire. And at the time of deactivation, a corresponding deactivation email is triggered.
This has reduced the effort for reactivating users as much as possible.
- An expired account can be reactivated via **Reactivate**. The user also must log in again for reactivation.
- The deactivation delay period starts upon password expiration.

Next save the user via **Save**.

The new user now needs to be notified of the access data for his/her account.
This is done in two steps:

1. Sending of the username (PUI and/or synonym) via e-mail or another method. Notify the user that he/she is about to receive the password.
2. Automated sending of the password. To send the initial password, first generate the password via the button **new password**. The initial password is sent directly to the new user.

Confirm this first message via OK.

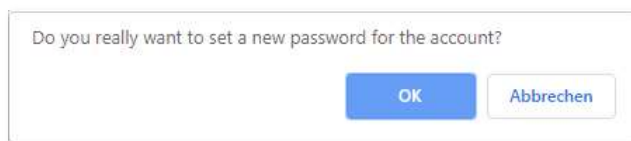


Figure 8, Confirm password reset

The transfer channel depends on the 2FA type recorded for the user.

The user receives the password via SMS (for Mobile ID and SMS/TAN 2FA methods):

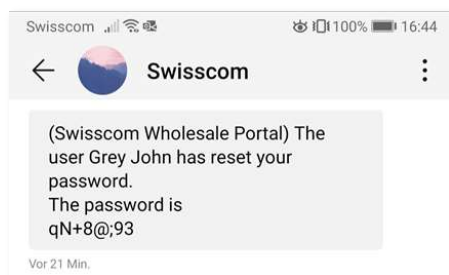


Figure 9, Sending of a new password via SMS

Or via e-mail (with eMail/TAN).

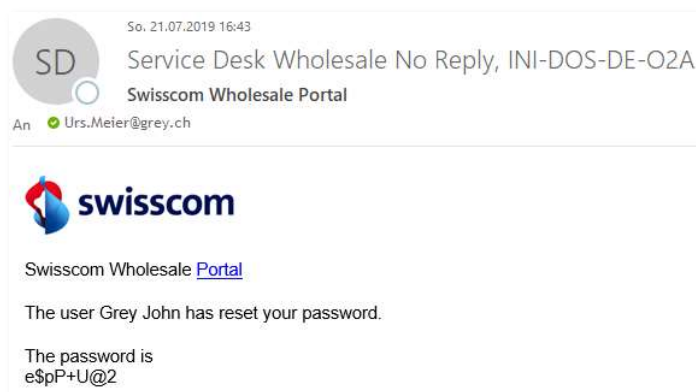


Figure 10, Sending of a new password via e-mail

The message containing the password does not contain username data, thus the username must be communicated in advance in step 1 for security reasons.

3.3. Add user rights

Now you must assign the corresponding services to the user. To do so, switch to the **portfolio** tab.



Figure 11, Current account, details, portfolios

In the pull-down menu, select a service under Subservice and select **Add** to add it for the user.

For an overview of the available services and subservices see the official document [User Rights Matrix.pdf](#).

3.3.1. Additional data for WSG rights

The **UserClass** is additionally determined for individual rights for the wholesale bulk business.

Depending on the rights, distinction is made between **ReadOnlyISP**, **Users** and **SuperUsers**.

3.3.2. Distinction between production and test for WSG rights

The test environment for the wholesale bulk business can also be reached via the productive Wholesale Portal. It is thus important to select the correct service. Here is the definition:

Production: WSG PROD

Test environment: WSG ISP

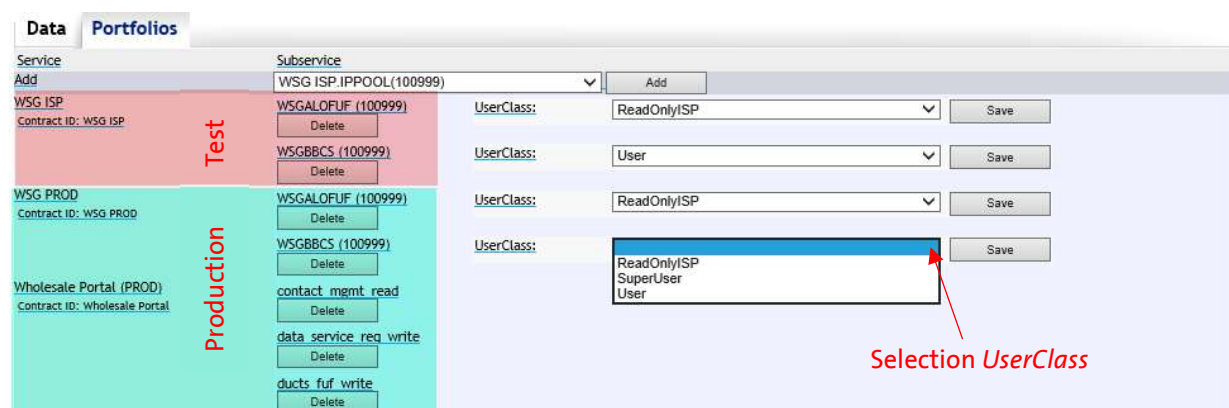
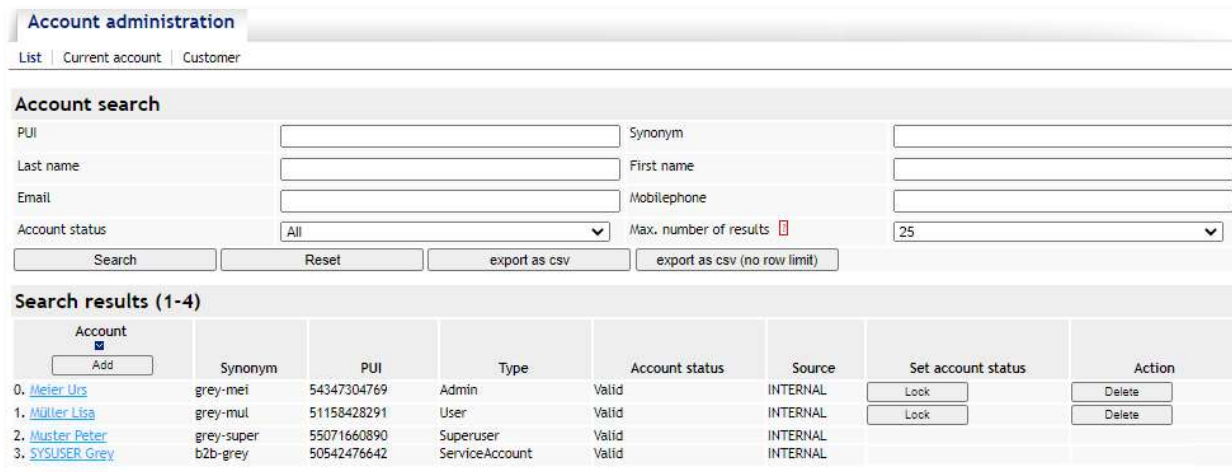


Figure 12, Portfolio with production and test rights

You can add on additional subservices for the user in the same manner. You can easily remove a subservice erroneously added or no longer needed via the **Delete** button.

You can return to the overview via **List** or by restarting the **Superusertool**. The new user account now appears in the list.



The screenshot shows the 'Account administration' interface. At the top, there are tabs for 'List', 'Current account', and 'Customer'. Below this is the 'Account search' section with input fields for PUI, Last name, Email, First name, and Mobilephone. There is also a dropdown for 'Account status' (set to 'All') and a 'Max. number of results' dropdown (set to '25'). Buttons for 'Search', 'Reset', 'export as csv', and 'export as csv (no row limit)' are present. Below the search section is the 'Search results (1-4)' table.

	Account	Synonym	PUI	Type	Account status	Source	Set account status	Action
0.	Meier Urs	grey-mei	54347304769	Admin	Valid	INTERNAL	<input type="button" value="Lock"/>	<input type="button" value="Delete"/>
1.	Müller Lisa	grey-mul	51158428291	User	Valid	INTERNAL	<input type="button" value="Lock"/>	<input type="button" value="Delete"/>
2.	Muster Peter	grey-super	55071660890	Superuser	Valid	INTERNAL		
3.	SYSUSER Grey	b2b-grey	50542476642	ServiceAccount	Valid	INTERNAL		

Figure 13, User list report

3.4. Export user report

Data entered for the user can be exported. This allows you to easily check the status of the users you administer.

The command <export as csv> gives you 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 simply get all your users.

Account	Synonym	PUI	Type	Role	Source	Email	Mobilephone	2nd Factor Type	Account Status	Last Login
Meier Urs	grey-mei	54347304769	Admin	-	INTERNAL	urs.meier@grey.ch	*+41790011223	MOBILETAN	Valid	16.02.2022 11:53
Müller Lisa	grey-mul	51158428291	User	-	INTERNAL	lisa.mueller@grey.ch	*+41790011224	EMAILTAN	Valid	16.02.2022 11:45
Muster Peter	grey-super	55071660890	Superuser	-	INTERNAL	peter.muster@swisscom.com	*+41790011222	MID	Valid	16.02.2022 11:25
SYSUSER Grey	b2b.grey	50542476642	ServiceAccount	-	INTERNAL	peter.muster@swisscom.com	-	NONE	Valid	16.02.2022 11:28


Figure 14, Exporting user data

The file is exported in ".csv" format, making the data easy to use for further purposes.

3.5. View of customer master data

As *SuperUser*, you can view the details of the IP addresses entered in the whitelist as well as the use of the whitelist.

Under Customer, the master data of the customer are displayed. This also includes the stored IP addresses.



Account administration

List | Current account | **Customer**

Customer

Company	Grey GmbH	ISP Code(PTS)	100996
Customer Identification (CUI)		Account limit	100
Customer status	Active	eMail/TAN allowed	<input checked="" type="checkbox"/>
Change Username	<input checked="" type="checkbox"/>	IP Whitelist usage	<input checked="" type="checkbox"/> Only for Service Accounts
IP Range	192.168.10.32/27; 192.168.11.32/255.255.255.252; 192.168.10.36 - 192.168.10.63; 192.168.20.; 192.168.30.40;		

Figure 15, View of master data

The view of the IP addresses can be expanded by dragging the lower right corner.

4. Annex

4.1. Further information about the 2FA solution

4.1.1. 2FA e-mails

E-mails sent by the 2FA solution are dispatched from this e-mail account:

NoReply.ServiceDeskWholesale@swisscom.com

You can therefore tell whether you are receiving undesired e-mail in your inbox.

The following e-mails can be generated (depending on the available communication channels):

- E-mails with a token for the user configured for eMail/TAN 2FA upon every login to the Wholesale Portal.
- E-mails with a validation request after a completed change of user data (change in e-mail address/mobile number/2FA method/password/synonym).

4.1.2. Sending SMS with 2FA

SMS sent by the 2FA solution are dispatched from the NoReply number:

+41798072275

"Swisscom" is displayed as sender on the recipient's mobile phone.

See Figure 9, page 13.

4.2. Best practice

4.2.1. Efficient new user creation and notification

The following procedure may be used so that a new user is automatically sent the synonym first, then the password thereafter:

- a) Enter all user data without synonym and without generating a new password.
Save this data.
- b) The second step is then to add the synonym and re-save.
This generates an SMS and/or e-mail providing notification of the change from (empty) to the new value. The user thus receives the username info (synonym) for the newly created account.
- c) The initial password can then be generated, which is also automatically sent to the new user.

Important note:

This procedure makes new account creation more efficient. It also lowers data security however. This is because the username and password data are both sent via the same channel within a short period of time.

5. Annex

5.1. List of tables

Table 1: Terms and abbreviations	4
Table 2: Updates	4
Table 3: Referenced documents	4
Table 4: Whitelist dependencies	7

5.2. List of figures:

Figure 1, Wholesale Portal login	9
Figure 2, 2FA confirmation.....	9
Figure 3, Wholesale Portal start page	10
Figure 4, List of accounts.....	10
Figure 5, Current accounts, new accounts	11
Figure 6, Setting up a new account.....	11
Figure 7, Current account, details, data	12
Figure 8, Confirm password reset.....	13
Figure 9, Sending of a new password via SMS	13
Figure 10, Sending of a new password via e-mail.....	13
Figure 11, Current account, details, portfolios	14
Figure 12, Portfolio with production and test rights.....	14
Figure 13, User list report.....	15
Figure 14, Exporting user data.....	15
Figure 15, View of master data	16