From	To be sent to
Swisscom (Switzerland) Ltd	Superusers and admins

Date

21.07.2019

Topic:

User administration for the Swisscom Wholesale Portal

Swisscom Wholesale Portal User Administration

Doc ID	Handbook Wholesale Portal
Version:	1.0
Replaces version	-
Issue date	Wednesday 21/07/2019
Valid from	Wednesday 21/07/2019
Valid until	Recall
Document name	EN_Handbook_Wholesale_Portal_Superuser_Admin_V1.0.docx

Table of contents

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, 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 administrators 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 administrators 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 have to 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

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

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 Wholesale Portal Terms of Use.

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 *Superuser Tool* which you have access to as the customer's superuser or administrator.

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. E-mail 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.

Important advisories:

- Every 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 e-mail TAN, affording a more efficient workflow.
- There is no cost to the user for use of Mobile ID or SMS TAN.
- The e-mail 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.
  For this solution to be used, the superuser has to disclose the IP addresses from which users will access the Wholesale Portal via e-mail TAN. This data flows into a whitelist which is referenced at login.

2.3 Whitelist

Customers who use these account types must provide IP addresses (individual addresses or IP ranges) to allow greater security for service accounts and accounts with which the e-mail TAN 2FA method is used.

These IP addresses define from what IP addresses a service account or account with e-mail TAN 2FA method the Wholesale Portal can be logged into. A login attempt of one of these user types which does not match the stored IP address data returns the standard error message "User name or password incorrect".

It can be defined whether the whitelist data are only active for service accounts or for both service accounts and accounts with the e-mail TAN 2FA.

The whitelist is administered by Swisscom. Requests to Swisscom to change the whitelist settings must always be submitted to the superuser.

2.4 User roles and access

Various user roles are defined in order 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 administrator (admin) rights.

An admin can create additional new users, but not further administrators.

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 Superuser Tool functionalities

3.1 Opening the Superuser Tool

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.

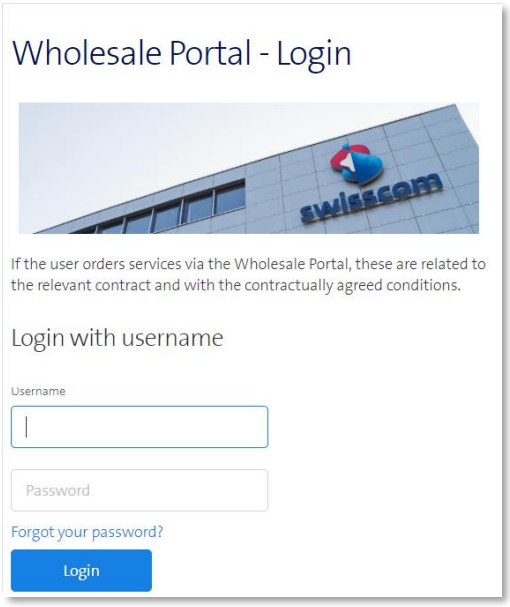

Figure 1, Wholesale Portal login

Confirm the user name and password entered via *Login*.

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

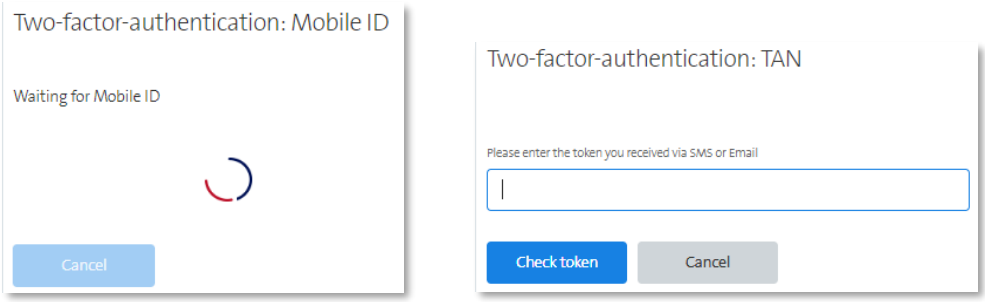

Figure 2, 2FA confirmation

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.

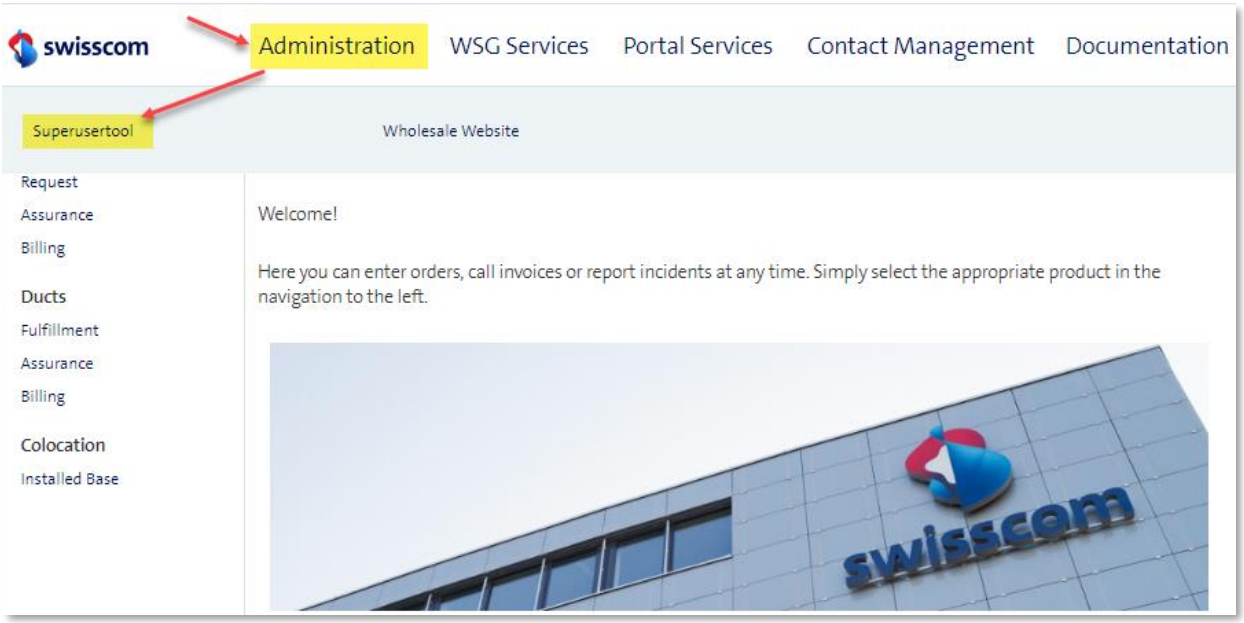

Figure 3, Wholesale Portal start page

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

Note:

If the *Superuser Tool* 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 10,

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.

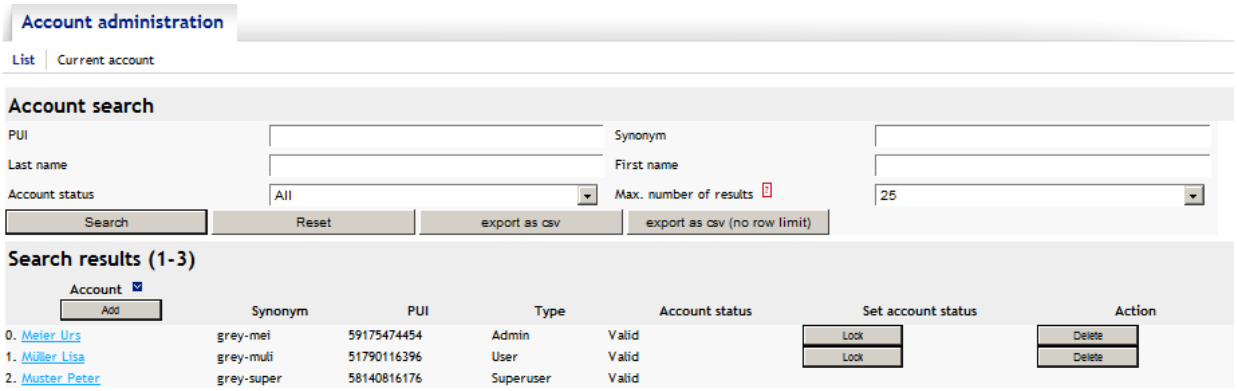

Figure 4, List of accounts

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*.

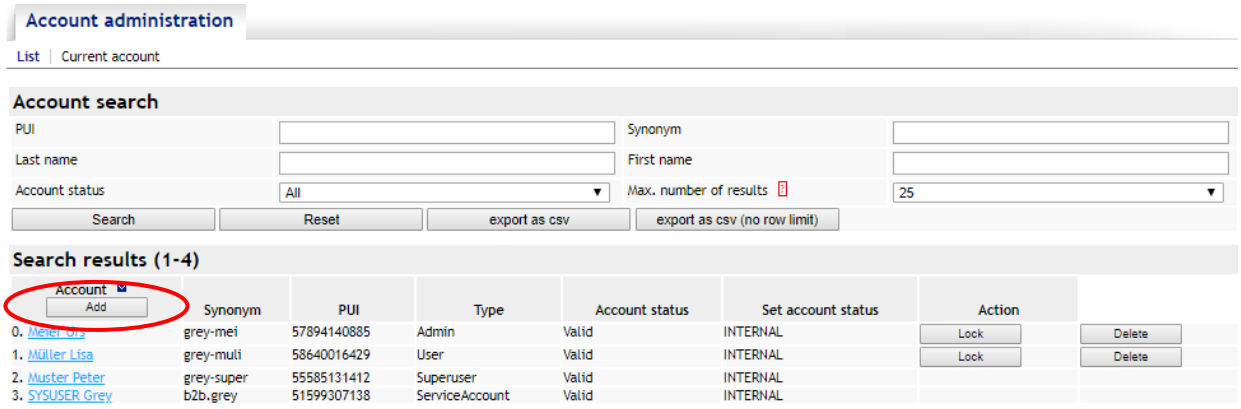

Figure 5, Current accounts, new accounts

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.

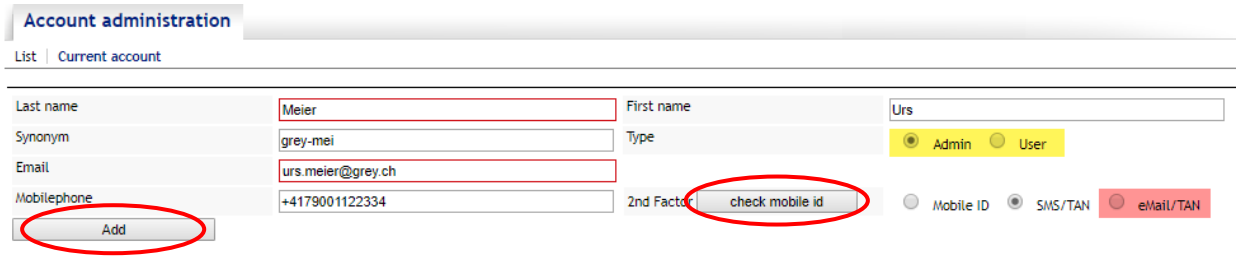

Figure 6, Setting up a new account

The selection choice marked in yellow for creating a new administrator is only available to the superuser. The superuser can also convert an existing user into an admin.

The selection choice marked in red of e-mail 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 administrators.

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.

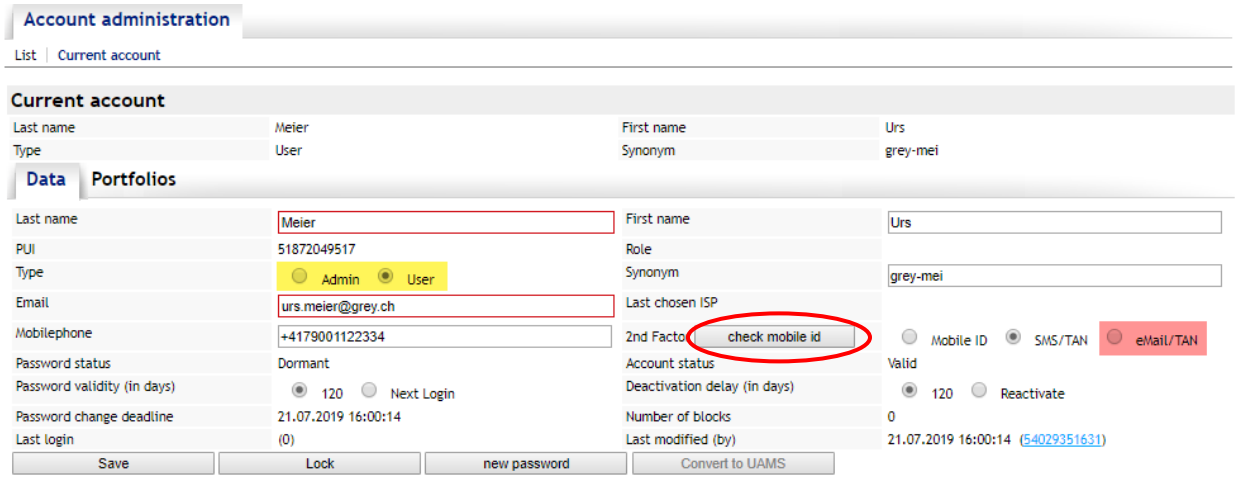

Figure 7, Current account, details, data

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.
- An expired account can be reactivated via *Reactivate*. The user also has to log in again for reactivation.
- The deactivation delay period starts upon password expiration.

Next save the user via *Save*.

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

1. Sending of the user name (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*.

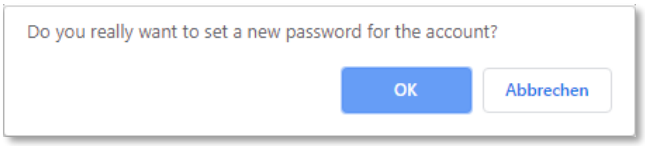

Figure8, Confirm password reset

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 e-mail TAN).

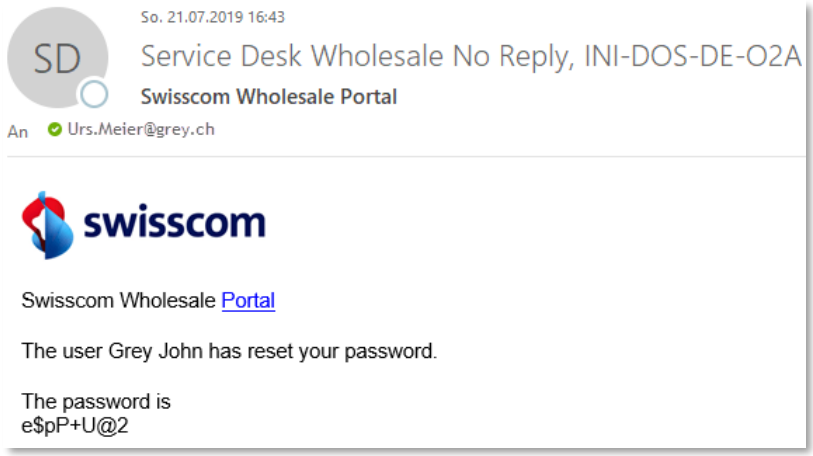

Figure 10, Sending of a new password via e-mail

The message containing the password does not contain user name data, thus the user name has to be communicated in advance in step 1 for security reasons.

Note:

In an upcoming release, the text of the initial password message will be different from the message for password resets.

3.3 Add user rights

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

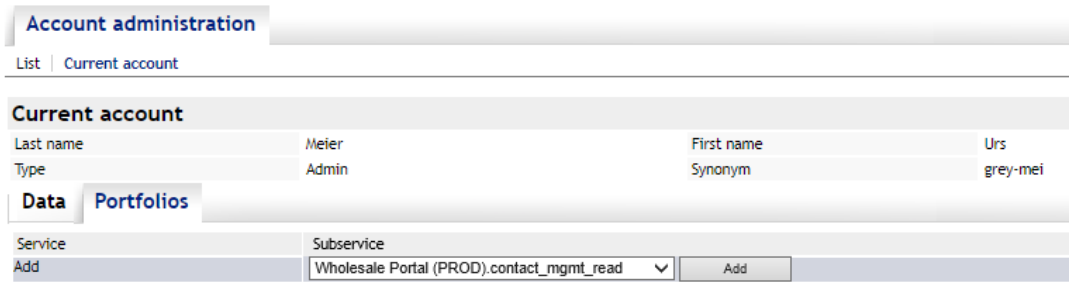

Figure 11, Current account, details, portfolios

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

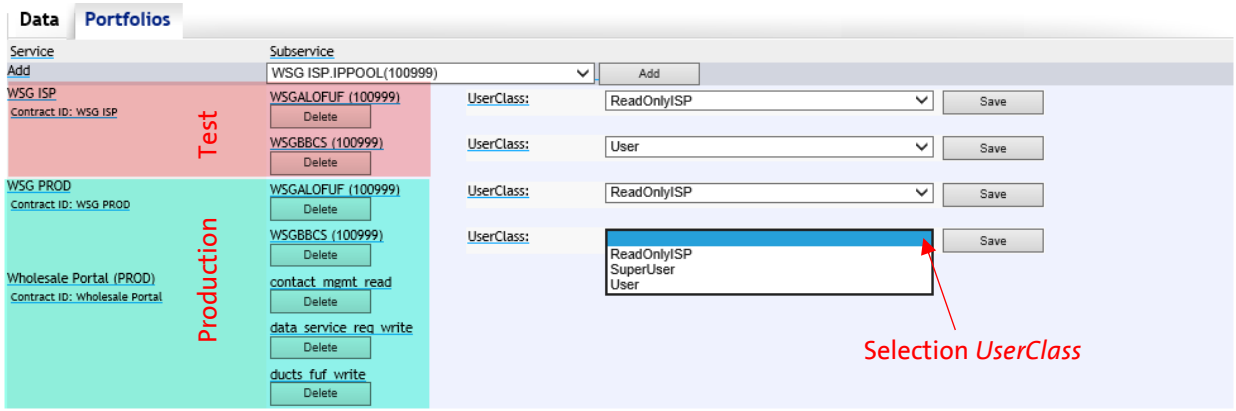

Figure12, Portfolio with production and test rights

You can add on additional subservices for the user in the same manner. You can easily remove a subservice erroneously added via the *Delete* button.

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

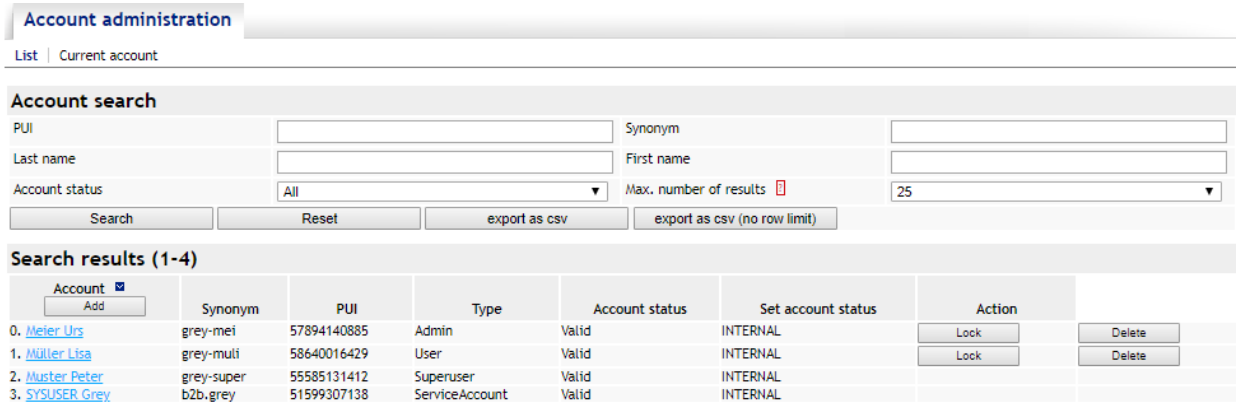

Figure 13, User list report

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 of your users.

Account	Synonym	PUI	Type	Role	Source	Email	Mobilephone	2nd Factor Type	Account Status	Last Login
Meier Urs	grey-mei	57894140885	Admin	-	INTERNAL	urs.meier@grey.ch	'+4179001122334	MOBILETAN	Valid	22.03.2019 12:53
Müller Lisa	grey-muli	58640016429	User	-	INTERNAL	lisa.mueller@grey.ch	'+4179001122335	EMAILTAN	Valid	21.03.2019 08:53
Muster Peter	grey-super	55585131412	Superuser	-	INTERNAL	peter.muster@swisscom.com	'+4179001122333	MID	Valid	22.03.2019 11:33
SYSUSER Grey	b2b.grey	51599307138	ServiceAccount	-	INTERNAL	peter.muster@swisscom.com	-	NONE	Valid	22.03.2019 16:25

Figure14, Exporting user data

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

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 e-mail TAN 2FA upon every login to the Wholesale Portal.
- From June 2019, 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 11.

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 user name 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 user name and password data are both sent via the same channel within a short period of time.

5 Annex

5.1 List of tables

5.2 List of figures: