From	Goes to
Swisscom (Switzerland) Ltd.	Portal users

Date

22.03.2022

Subject

FAQ to the Swisscom Wholesale Portal

Swisscom Wholesale Portal

FAQ_Frequently Asked Questions

Q & A

No.	Question	Answer
1.	Who can set up a user account for me?	The customer's SuperUser manages the user accounts and can set up new accounts. He can be supported by administrators (Admin). The Admin are set up by the SuperUser.
2.	Who can unlock my user account?	The customer's SuperUser and Admin can unlock their user accounts.
3.	My SuperUser account is locked. Who can I contact?	SuperUser accounts can be unblocked by the Swisscom Service Desk Wholesale. ServiceDesk.Wholesale@swisscom.com +41 800 803 803
4.	Who can unblock a Service Account?	Service Accounts can be unblocked by the Swisscom Service Desk Wholesale. ServiceDesk.Wholesale@swisscom.com +41 800 803 803
5.	What is a 2FA?	2FA stands for two-factor authentication. With a 2FA, a confirmation is requested via a second path when logging into the wholesale portal.

6.	Can a telephone number from abroad be entered in field Mobilephone?	Yes, with an internationally standardised country code number beginning with "+" (e.g., "+31234567890").
		The mobile number must be able to receive SMS.
7.	What is a Service Account?	A Service Account is an account that is used in machine-to-machine mode (B2B) for web services.
		These accounts are administered by Swisscom Wholesale.
		New service accounts or changes to existing ones must be ordered from Swisscom.
		Accountteam.Wholesale@swisscom.com
8.	Which parameters must be defined for Service Accounts? - E-mail address? - Mobile number? - Whitelist entries	The Service Accounts are created by Swisscom Wholesale. For this purpose, it is mandatory to define an e-mail address communicated by the customer. The initial password is sent to this e-mail address.
		A mobile number is optional, but it can be very helpful for faster communication in the event of an error.
		To ensure security on the Service Accounts, the sending IP address is compared with the values stored in a whitelist. Only accesses coming from IP addresses defined in the whitelist are allowed.
		It is therefore necessary for the SuperUser to communicate the IP addresses or IP ranges for the entry in the whitelist to Swisscom when setting up Service Accounts.
9.	What are B2B permissions? How do I recognise them?	The B2B permissions are used for Service Accounts. The B2B permissions have the following characteristics: • For mass products, the service starts with "WS WSG " (not with "WSG ") • For solution products the service starts with "FWS Portal (b2b)".
10.	What are GUI permissions? How do I recognise them?	GUI stands for graphical user interface. This corresponds to the Wholesale Portal, also known to some as WSG. On this, the user works on the user interface provided by Swisscom.
		The GUI permissions have the following characteristics: • For bulk products, the service starts with "WSG " (not with "WS WSG "). • For solution products, the service starts with "Wholesale Portal ".

11.	The user account does not have a mobile number. Is there an alternative solution?	If no mobile number can be used, the 2-factor authentication is also possible via eMail/TAN. However, this option offers less security. To enable the 2FA option via eMail/TAN, the SuperUser must order the release of the option from Swisscom. Possible reasons for this solution: Employees do not have a mobile, work in a location without mobile reception or are not allowed to use a mobile at their workplace.
12.	Which procedure is recommended for impersonal accounts? (e.g., Customer Service Desk)	Impersonal accounts should not be assigned. Such accounts are not traceable. In the case of impersonal accounts, the customer must therefore designate a person responsible for the account (e.g., the SuperUser). As with the solution for user accounts without a mobile number, 2-factor authentication via e-mail/TAN is required for this.
13.	Can the accesses be additionally protected? For example, that user accesses are also only possible if they were generated from a specific company network?	The approach of a whitelist was primarily created for the accesses of the Service Accounts. However, it is also possible to check all accesses via the entries in the whitelist. In this case, access can only take place from IP addresses stored in the whitelist. To set up this solution, the SuperUser supplies the IP addresses or IP ranges to Swisscom. This information is entered by Swisscom and activated for all users of the customer.

14.	**How do I create a new user as a SuperUser or Admin?**

This is described in detail in the " [Wholesale Portal Manual - Superuser / Admin](#)".

Short description:
Access via Administration -> Superusertool

In the user overview, an input mask can be opened via the "Add" button.

In this screen, the superuser or administrator fills in the user information.
(Name, first name, synonym, e-mail and mobile no.)

The mobile number can be checked for mobile ID capability. This is done with "check mobile id".
If available, this safest variant should always be selected.

By clicking on "Add", the view changes to the user administration screen.

In this screen, the entries can be checked and completed.

Permissions must still be added to the user under "Portfolio".
The available rights depend on the contracts.

The individual permissions are added with "Add".

Then switch back to "Data".

Now the user must be sent an initial password.
This is done directly via "new password".

Confirm the message with OK.

Der Versand des Passworts wird angezeigt.

The new account is now created.

15.	**How can I maintain my own account?** Self-maintenance is accessed via the name in the top right-hand corner. After selecting the parameter to be changed, the applicable guidelines for the change are displayed on the right. Depending on the basic setting of the customer, not all parameters can be changed by the user himself.	
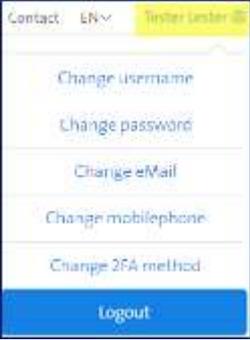
Change username

The username (also called synonym) can be changed by the user himself. For some clients this is not available. In that case, the user must contact their SuperUser or Admin to obtain a new synonym.

Change password

To change the password, the old password must be entered. If this is no longer known, the user must contact their SuperUser or Admin to obtain a new initial password.

Change eMail

The e-mail address can be changed by the user himself. A valid e-mail address is mandatory.

Change mobilephone

The mobile number can be changed by the user. The mobile number must be SMS-enabled to use the 2FA methods SMS/TAN or Mobile ID.

Change 2FA method

There are three 2FA methods:

- **Mobile ID**
  The 2FA method Mobile ID currently offers the highest security. Users need a mobile with Mobile ID capability.
  A request for confirmation on the mobile must be answered with the personal code.
  The function of Mobile ID and its availability are described here:
  Secure online login with Mobile ID (mobileid.ch)
- **SMS/TAN**
  When using the 2FA SMS/TAN, SMS with a token (code) are sent to the mobile.
- **eMail/TAN**
  When using the 2FA eMail/TAN, the token (code) is sent to the user by e-mail. This method is not available to all customers.