

Von	Geht an
Swisscom (Schweiz) AG	Portal Benutzer
Datum	
22.03.2022	
Thema	
FAQ zum Swisscom Wholesale Portal	

Swisscom Wholesale Portal

FAQ_Häufig gestellte Fragen

Q & A

Nr.	Frage	Antwort
1.	Wer kann für mich einen Benutzeraccount einrichten?	Der SuperUser des Kunden verwaltet die Benutzeraccounts und kann neue Accounts einrichten. Er kann sich durch Administratoren (Admin) unterstützen lassen. Die Admin werden durch den Superuser eingerichtet.
2.	Wer kann meinen Benutzeraccount entsperren?	Der SuperUser und die Admin des Kunden können ihre Benutzeraccounts entsperren.
3.	Mein SuperUser Account ist gesperrt. An wen kann ich mich wenden?	SuperUser Accounts können durch den Swisscom Service Desk Wholesale entsperrt werden. ServiceDesk.Wholesale@swisscom.com +41 800 803 803
4.	Wer kann einen Service Account entsperren?	Service Accounts können durch den Swisscom Service Desk Wholesale entsperrt werden. ServiceDesk.Wholesale@swisscom.com +41 800 803 803
5.	Was ist eine 2FA?	2FA steht für zwei Faktoren Authentifizierung. Bei einer 2FA wird bei einer Anmeldung auf dem Wholesale Portal eine Bestätigung auf einem zweiten Weg eingefordert.



6.	Kann im Feld Mobilephone eine Telefonnummer aus dem Ausland eingegeben werden?	Ja, mit einer international normierten Landeskennziffer beginnend mit "+" (z.B. "+31234567890"). Die Mobilenummer muss in der Lage sein, SMS zu empfangen.
7.	Was ist ein Service Account?	Als Service Account wird ein Account bezeichnet, der im Maschine-to-Maschine Modus (B2B) für Webservices genutzt wird. Diese Accounts werden durch Swisscom Wholesale administriert. Neue Service Accounts oder Änderungen an bestehenden sind bei Swisscom zu bestellen. Accountteam.Wholesale@swisscom.com
8.	Welche Parameter müssen bei Service Accounts hinterlegt werden: - E-Mail-Adresse? - Mobilenummer? - Whitelist Einträge	Die Service Accounts werden durch Swisscom Wholesale angelegt. Dazu muss zwingend eine durch den Kunden kommunizierte E-Mail-Adresse definiert werden. Das Initialpasswort wird an diese E-Mail-Adresse versendet. Eine Mobilenummer ist optional, kann für eine schnellere Kommunikation im Fehlerfall aber sehr hilfreich sein. Um die Sicherheit auf den Service Accounts sicher zu stellen, wird die sendende IP-Adresse mit den in einer Whitelist hinterlegten Werten verglichen. Nur Zugriffe, welche von in der Whitelist definierten IP-Adressen herkommen, werden erlaubt. Deshalb ist es notwendig, dass der Superuser die IP-Adressen oder IP-Ranges für den Eintrag in die Whitelist bei der Einrichtung von Service Accounts an Swisscom kommuniziert.
9.	Was sind B2B Berechtigungen? Wie erkenne ich solche?	Die B2B Berechtigungen werden für Service Accounts verwendet. Die B2B Berechtigungen weisen folgende Merkmale auf: <ul style="list-style-type: none">Für Massenprodukte beginnt der Service mit "WS WSG" (nicht mit "WSG")Für Lösungsprodukte lautet der Service mit "FWS Portal (b2b)"
10.	Was sind GUI Berechtigungen? Wie erkenne ich solche?	GUI steht für grafische Benutzeroberfläche. Dies entspricht dem Wholesale Portal, manchen auch als WSG bekannt. Auf diesem arbeitet der Benutzer auf dem von Swisscom zur Verfügung gestellten Benutzeroberfläche. Die GUI Berechtigungen weisen folgende Merkmale auf: <ul style="list-style-type: none">Für Massenprodukte beginnt der Service mit "WSG" (nicht mit "WS WSG")Für Lösungsprodukte lautet der Service mit "Wholesale Portal"



11.	Der Benutzer Account verfügt über keine Mobilenummer. Gibt es eine Alternativlösung?	Sollte keine Mobilenummer hinterlegt werden können, ist die 2 Faktoren Authentifizierung auch per eMail/TAN möglich. Diese Option bietet jedoch eine geringere Sicherheit. Damit die Option 2FA über eMail/TAN freigegeben wird, muss der Superuser die Freigabe der Option bei Swisscom bestellen. Mögliche Gründe für diese Lösung: Mitarbeiter besitzen kein Mobile, arbeiten an einem Ort ohne Mobileempfang oder dürfen an ihrem Arbeitsplatz kein Mobile nutzen.
12.	Welches Vorgehen wird bei unpersönlichen Accounts empfohlen? (z.B. Customer Service Desk)	Unpersönliche Accounts sollten nicht vergeben werden. Eine Nachvollziehbarkeit ist bei solchen Accounts nicht gegeben. Bei unpersönlichen Accounts muss deshalb durch den Kunden eine für den Account verantwortliche Person bestimmt werden (z.B. der SuperUser). Wie bei der Lösung für Benutzer Accounts ohne Mobilenummer wird hierfür die 2 Faktoren Authentifizierung über eMail/TAN benötigt.
13.	Können die Zugriffe zusätzlich geschützt werden? Beispielsweise, dass auch Benutzerzugriffe nur möglich sind, wenn sie aus einem spezifischen Firmennetz heraus erzeugt wurden?	Der Ansatz einer Whitelist wurde in erster Linie für die Zugriffe der Service Accounts geschaffen. Es ist jedoch auch möglich, sämtliche Zugriffe über die Einträge in der Whitelist zu prüfen. Dann können Zugriffe nurmehr von in der Whitelist hinterlegten IP-Adressen aus erfolgen. Für das Einrichten dieser Lösung liefert der Superuser die IP-Adressen oder IP-Ranges an Swisscom. Diese Angaben werden durch Swisscom eingepflegt und für alle Benutzer des Kunden aktiviert.

**14. Wie erstelle ich als SuperUser oder Admin einen neuen Nutzer?**

Dies ist im Detail beschrieben im "[Handbuch_Wholesale_Portal – SuperUser /Admin](#)"

Kurzbeschrieb:

Einstieg über Administration -> Superusertool.



In der Benutzerübersicht kann über die Schaltfläche "Add" eine Eingabemaske geöffnet werden.

The screenshot shows a table with columns "Account" and "Synonym". A yellow box highlights the "Add" button at the bottom of the table.

In dieser Maske füllt der Superuser oder Administrator die Benutzer-Informationen aus.
(Name, Vorname, Synonym, E-Mail und Mobile-Nr.)

The screenshot shows a form for creating a new user. It includes fields for "Last name" (Lester), "First name" (Tester), "Type" (User selected), "Synonym" (lester.tester), "Email" (t.lester@grey.ch), "Mobilephone" (+41796989734), and "2nd Factor" (check mobile id). There are also radio buttons for "Admin" (selected) and "User", and for "Mobile ID" and "SMS/TAN". A yellow box highlights the "Add" button at the bottom.

Die Mobilenummer kann auf Mobile-ID Fähigkeit geprüft werden. Dazu dient "check mobile id".
Falls verfügbar, soll immer diese sicherste Variante gewählt werden.

Mittels "Add" wechselt die Ansicht in die Benutzeradministrationsmaske.

In dieser Maske können die Eingaben geprüft und ergänzt werden.

The screenshot shows a detailed user administration form. It includes sections for "Current account" and "Portfolios". The "Data" tab is active. It contains fields for "Last name" (Lester), "First name" (Tester), "Type" (User selected), "Synonym" (lester.tester), "Email" (t.lester@grey.ch), "Mobilephone" (+41796989734), "PUI" (59914334977), "Role" (User selected), "2nd Factor" (check mobile id), "Account status" (Valid), "Deactivation delay (in days)" (120 selected), "Password status" (Dormant), "Password validity (in days)" (120 selected), "Password change deadline" (04.03.2022 17:04:59), "Last login" (0), "Number of blocks" (0), "Last modified (by)" (04.03.2022 17:08:24 (54020025110)), and buttons for "Save", "Lock", "new password", "Convert to UAMS", and "Delete". A yellow box highlights the "Data" tab.



Dem Benutzer müssen unter "Portfolio" noch Berechtigungen zugefügt werden.
Die verfügbaren Rechte sind abhängig von den Verträgen.

Current account

Last name	Lester	First name	Tester
Type	User	Synonym	lester.tester

Data Portfolios

Service Add Subservice

WSG PROD.WSGT(100999)

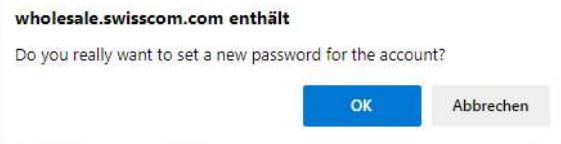
WSG PROD.WSGBBILLING(100999)
WSG PROD.WSGBBCS(100999)
WSG PROD.WSGINFOSRV(100999)
WSG PROD.WSGTT(100999)
WSG PROD.WSGULL(100999)
Wholesale Portal (PROD).billing_write
Wholesale Portal (PROD).col_inb_write
Wholesale Portal (PROD).contact_mgmt_write
Wholesale Portal (PROD).data_service_asr_write

Mit "Add" werden die einzelnen Berechtigungen zugefügt.

Danach wieder auf "Data" zurück wechseln.

Nun muss dem Benutzer noch ein Initialpasswort gesendet werden.
Dies erfolgt direkt über "new password".

Die Hinweismeldung mit OK quittieren.



Der Versand des Passworts wird angezeigt.

Current account

Last name	Lester	First name	Tester
Type	User	Synonym	lester.tester

A new password has been generated for the following user: Lester Tester (59914334977)
The new password has been sent to the following phone number: +41796989734
For security reasons the user should change password immediately following the first login.

Data Portfolios

Last name: Lester
PUI: 59914334977
Type: Admin (radio button selected)
Email: t.lester@grey.ch
Mobilephone: +41796989734
Password status: Original
Password validity (in days): 120 (radio button selected)
Password change deadline: 04.03.2022 17:22:33
Last login: (0)
First name: Tester
Role: check mobile id
Synonym: lester.tester
Last chosen ISP: Mobile ID SMS/TAN eMail/TAN
2nd Factor: Valid
Account status: 120 Reactivate
Deactivation delay (in days): 0
Number of blocks: 0
Last modified (by): 04.03.2022 17:22:33 (54020025110)

Buttons: Save, Lock, new password, Convert to UAMS, Delete

Damit ist der neue Account angelegt.



15.	<p>Wie kann ich meinen eigenen Account pflegen?</p> <p>Die Selbstpflege wird über den Namen oben rechts erreicht.</p> <p>Nach Auswahl des zu ändernden Parameters werden die dafür geltenden Richtlinien für die Änderung jeweils rechts angezeigt.</p> <p>Je nach Grundeinstellung des Kunden sind nicht alle Parameter durch den Benutzer selbst änderbar.</p>	
	<p>Benutzername ändern</p> <p>Der Benutzername (auch Synonym genannt) kann durch den Benutzer selbst geändert werden. Bei einigen Kunden ist dies nicht verfügbar. In dem Fall muss der Benutzer sich an seinen SuperUser oder Admin wenden, um ein neues Synonym zu erhalten.</p>	
	<p>Passwort ändern</p> <p>Um das Passwort zu ändern, muss das alte Passwort eingegeben werden. Ist dieses nicht mehr bekannt, muss der Benutzer sich an seinen SuperUser oder Admin wenden, um ein neues Initialpasswort zu erhalten.</p>	
	<p>eMail ändern</p> <p>Die E-Mail-Adresse kann durch den Benutzer selbst geändert werden. Eine gültige E-Mail-Adresse ist zwingend erforderlich.</p>	
	<p>Mobilenummer ändern</p> <p>Die Mobilenummer kann durch den Benutzer selbst geändert werden. Die Mobilenummer muss SMS fähig sein, um die 2FA Methoden SMS/TAN oder Mobile ID zu nutzen.</p>	
	<p>2FA Methode ändern</p> <p>Es gibt drei 2FA Methoden:</p> <ul style="list-style-type: none">• Mobile ID Die 2FA Methode Mobile ID bietet zurzeit die höchste Sicherheit. Benutzer benötigen ein Mobile ID fähiges Mobile. Dabei muss zur Bestätigung auf dem Mobile eine Anfrage mit dem persönlichen Code beantwortet werden. Die Funktion von Mobile ID und deren Verfügbarkeit wird hier beschrieben: Sicher online einloggen mit Mobile ID (mobileid.ch)• SMS/TAN Bei der Nutzung der 2FA SMS/TAN werden SMS mit einem Token (Code) an das Mobile gesendet.• eMail/TAN Bei der Nutzung der 2FA eMail/TAN wird das Token (Code) per E-Mail am Benutzer gesendet. Diese Methode steht nicht allen Kunden zur Verfügung.	