SWISS SECURIUM®

HIGH-SECURITY COLLABORATION

CONTROLIUM AND ACCESS SECURIUM™
USER MANUAL

THIS USER MANUAL APPLIES TO

ALPEIN SOFTWARE SECURE PLATFORM SWISS SECURIUM®

Document version 1.4
19.08.2018

CONTENTS

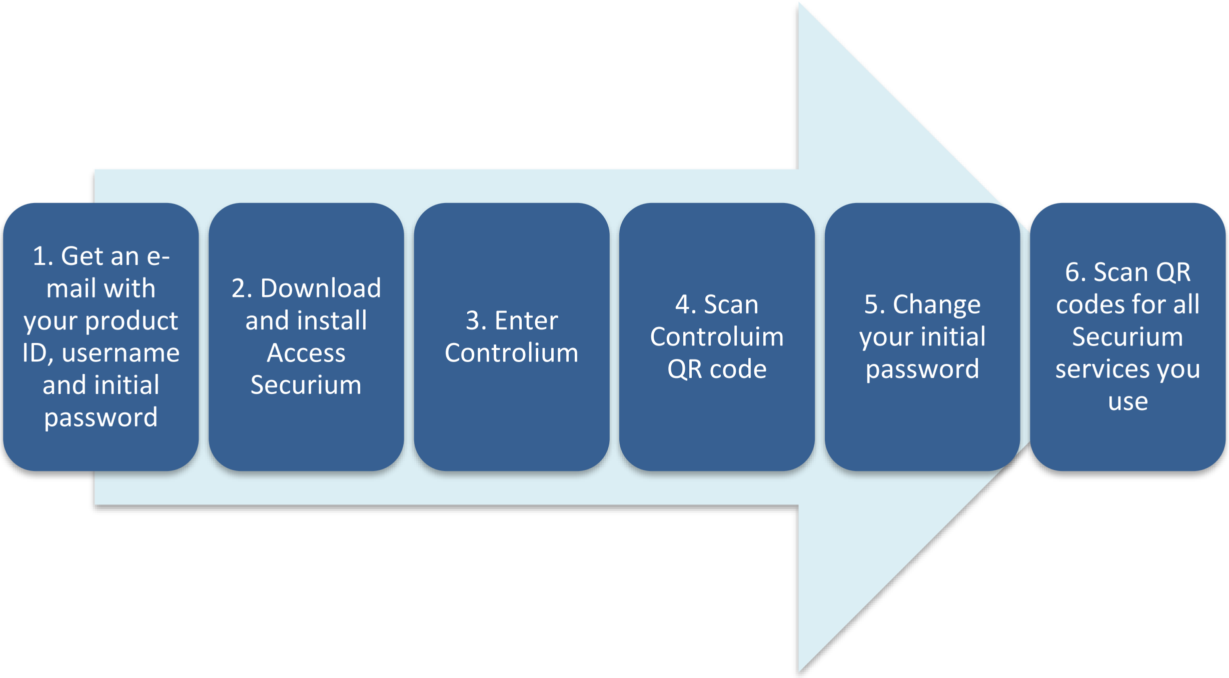
INTRODUCTION

The SWISS **SECURIUM**® Platform is a special platform for secure communication, storage and exchange of information and documents. The reliable data centre ensures maximum physical security.

Since foundation we have been successfully protecting communication. The highest corporate communication security is our main goal.

100% are made and protected in Switzerland.

1. GETTING STARTED PROCESS



1. Get an e-mail with your product ID, username and initial password
2. Download and install Access Securium
3. Enter Controlium
4. Scan Controluim QR code
5. Change your initial password
6. Scan QR codes for all Securium services you use

2. GETTING STARTED INSTRUCTIONS

There are 6 simple steps to start secure communication:

2.1. Get an email with your product ID, username and initial password

All users of SWISS **SECURIUM**® receive email with their credentials, as well as link on **Controlium** and archive of manuals for applications, including this instruction.

2.2. Download and install AccessSecurium™

You need to use One-time passwords (OTP) to log into SWISS **SECURIUM**® services via web interface.

To use One-time passwords you need to install **ACCESS** SECURIUM™ app from Google Play if you use Android or from App Store if you use iOS. The app is free.

2.3. Enter Controlium

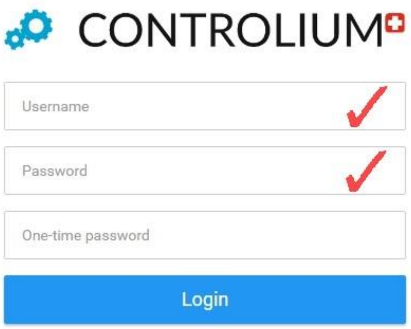
Controlium is a web-based interface for system administration. Link to web services has the following structure:

*https://**ProductID**.securium.ch*

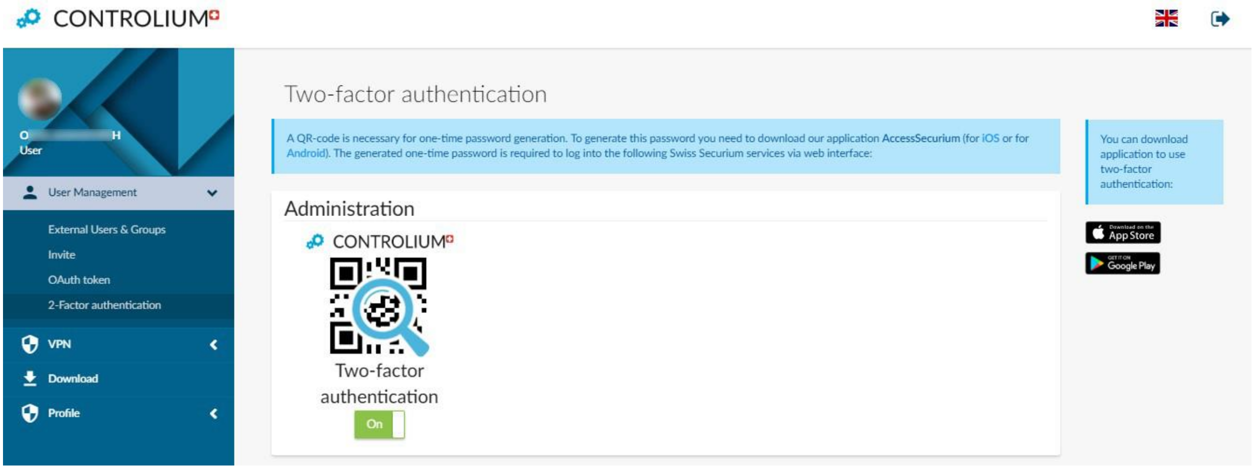
For example, your product ID is “company”, so link to Controlium would be:

https://company.securium.ch

To log into Controlium click on gears icon, then fill only <Username> and <Password> fields. If you turn on OTP access then next time you’ll need to log in Controlium entering Username, Password and One-time password generated with the **Access**Securium™ app.



After entering Controlium for the first time you will get on <2-Factor authentication> tab.



A QR-code is necessary for one-time password generation. To generate this password you need to download our application AccessSecurium (for iOS or for Android). The generated one-time password is required to log into the following Swiss Securium services via web interface:

You can download application to use two-factor authentication:

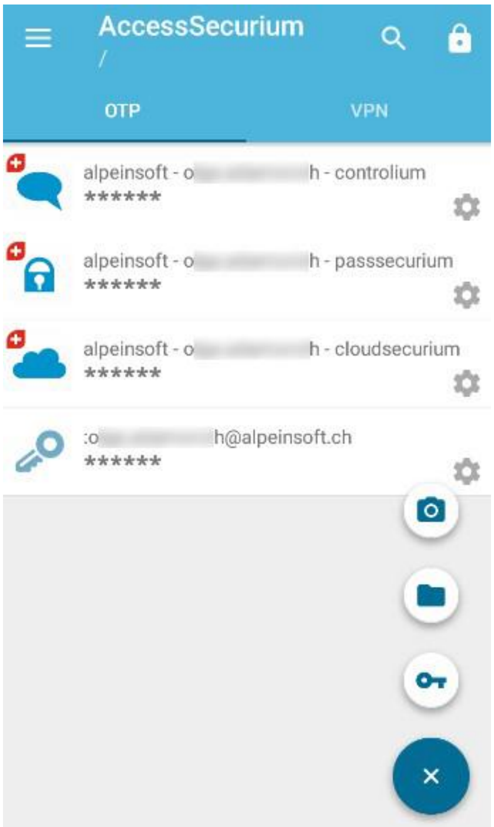
Please, if you turn on 2-factor authentication, don’t log out from Controlium before scanning Controlium QR code.

2.4. Scan Controlium QR code

A QR code is necessary for One-time password generation.

1. Enter your **Controlium** cabinet.
2. Click <2-Factor authentication> tab in <User Management> section.
3. Turn on Controlium Two-factor authentication to open QR code.
4. Scan Controlium QR code using AccessSecurium™ on your smartphone:

   - Tap on the Add icon + .
   - Tap camera icon 📷 .
   - Scan QR code for **Controlium**.



AccessSecurium
/
OTP VPN

alpeinsoft - o[redacted]h - controlium
******

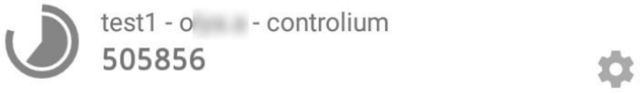
alpeinsoft - o[redacted]h - passsecurium
******

alpeinsoft - o[redacted]h - cloudsecurium
******

:o[redacted]h@alpeinsoft.ch
******

After that you can log into **Controlium** using One-time password generated with the **Access**Securium™ app.

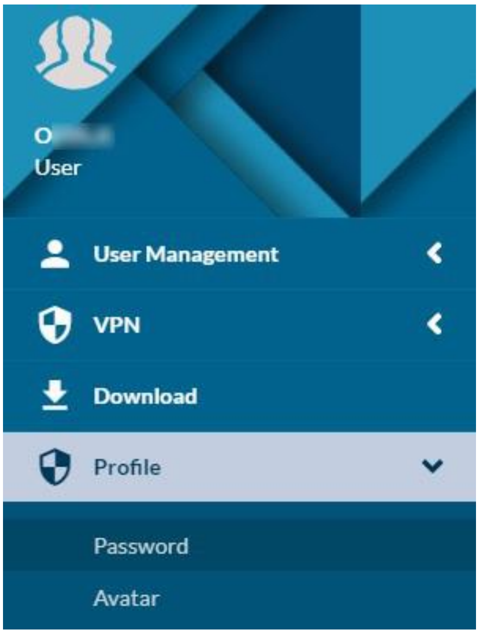
To generate a One-time password for logging into a web application, just click on the title of this application in **Access**Securium™ on your smartphone.



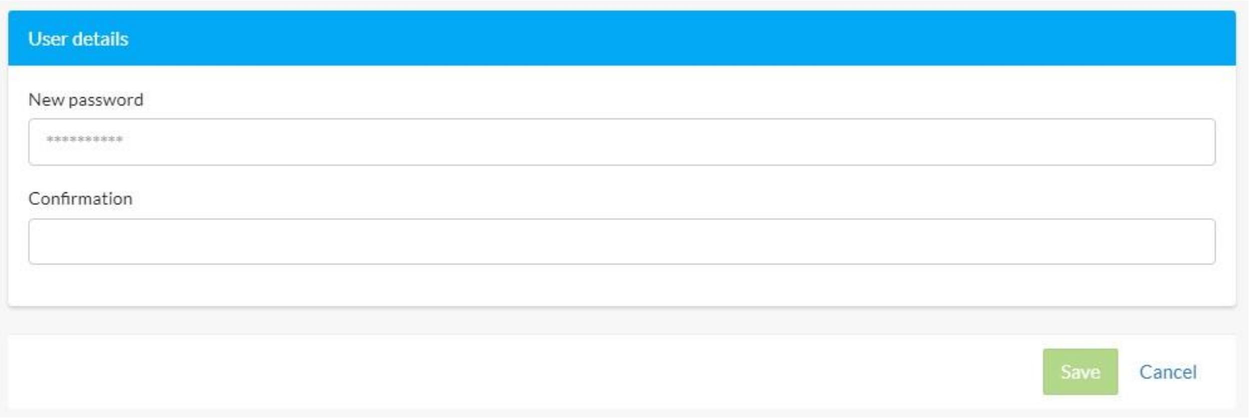
test1 - o[redacted] - controlium
505856

2.5. Change initial password

1. After logging into **Controlium** click tab <Password> in the drop-down menu of <Profile> section.
2. Enter new password into the <New password> field.
3. Than enter new password into the <Confirmation> field.
4. Click <Save>.



O[redacted]
User



User details

New password

****

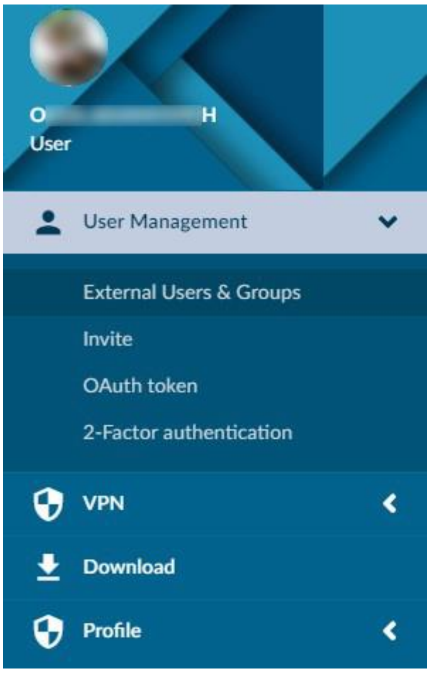
Confirmation

2.6. Scan QR codes for all SWISS SECURIUM® services you use

To scan QR codes for SWISS **SECURIUM**® services follow the same algorithm as in step 2.4.

3. ADDITIONAL USER SETTINGS

3.1. Invite external users

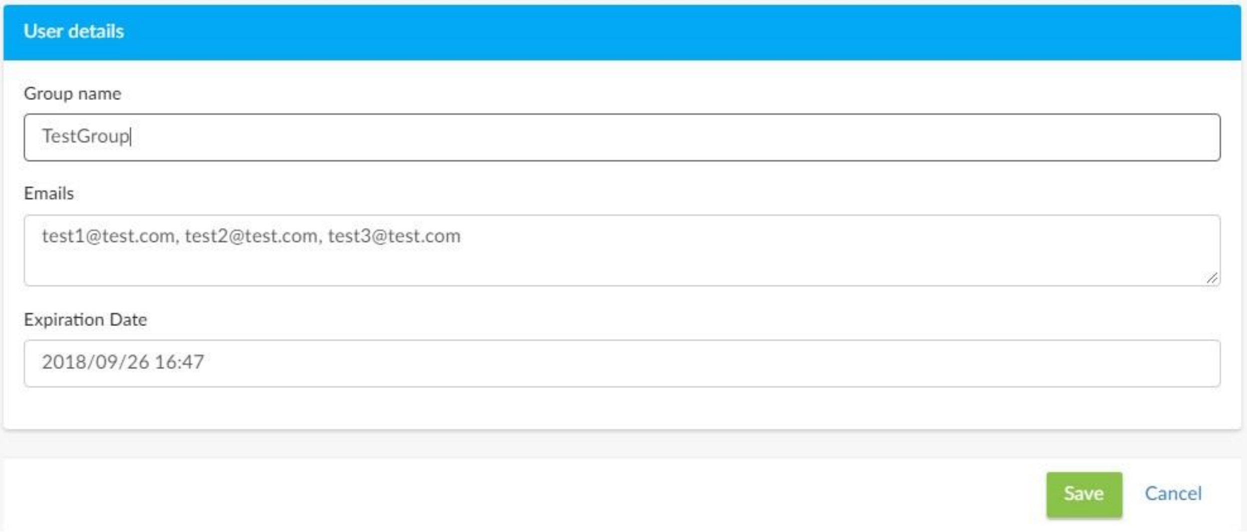


On the <Invite> tab in the <User Management> section of your **Controlium** cabinet you can invite external users (which wasn't created by the administrator of the SWISS **SECURIUM**® platform) to **Swiss**Securium™ chat.

Attention! Firstly, the invited user should install the **Swiss**Securium™ application from **<u>Google Play</u>** or **<u>iTunes</u>**, and then he/she will be able to use invitation link.

To create an invitation, you should fill following fields:

1. <Group name> – name of the user group which will be displayed in the **Swiss**Securium™ messenger for invited participants.
2. <Emails> – emails of invited participants. The number of invited users is limited to the maximum number of users of this platform, i.e. if your platform is designed for 100 users and it already has 40, then you can invite 60 users. After the expiration of the invitation, the user's space is cleared.
3. <Expiration date> – the duration of the invitation (after this date the chat will no longer be available to invited users, all data from it will be completely removed).



User details

Group name

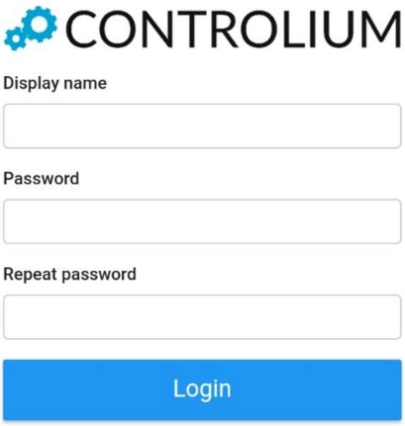
TestGroup

Emails

test1@test.com, test2@test.com, test3@test.com

Expiration Date

2018/09/26 16:47



CONTROLIUM

Display name

Password

Repeat password

Users invited via **Controlium** must choose a Display name (which will be visible to chat participants instead of an email address) and set a password for logging in.

For maximum convenience, it's best to use Google Chrome for Android or Safari for iOS.

If an error occurred during login, simply go to the **Swiss**Securium™ application and log in directly to it. You should enter the highlighted part of your invitation link (characters right after // and up to the first dot .) in the <Product ID> field.
Example:
https://**alpeinsoft**.securium.ch/en/controlium/invite...
Enter your email address to which you received the invitation as Username.

After such registration, the user will be able not only to participate in the **Swiss**Securium™ chat, but also to use the other platform services: **Cloud**Securium™ (secure cloud for files, download for **Android** or **iOS**), **Pass**Securium™ (password manager, download for **Android** or **iOS**), **Controlium** cabinet. To securely access services through a browser, the user should install the **Access**Securium™ application for two-factor authentication for **Android** or **iOS**.

After the invitation expiration, these services will also no longer be available to the invited user.

3.2. OAuth tokens

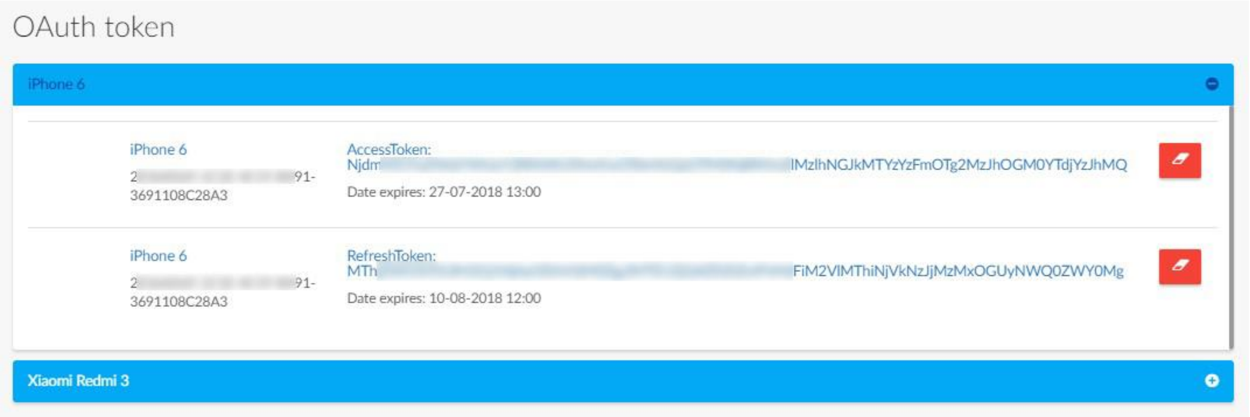
On <OAuth token> tab in <User Management> section of your **Controlium** you can track and, if necessary, recall tokens for the various devices from which you have logged into **Swiss**Securium™ under your account.

Tokens prevent the storage of the account password on the user's device. This increases security if in case of the device loss someone attempts to scan the device and get a password.

If you notice tokens for unfamiliar device in **Controlium**, you can recall the token by clicking on the eraser icon ⌫ opposite it. This way you can block the **Swiss**Securium™ messenger on the unfamiliar device for which the token has been recalled. Its user will need to enter the account password again.

To be sure that no one can view your data from other platform applications, change also the account password in <Profile> → <Password> according to the algorithm described in section 2.5.

The **Controlium** system creates 2 tokens for each device: AccessToken (for primary access from the device) and RefreshToken (for subsequent access). To block SwissSecurium™ you need to recall both tokens.



OAuth token

iPhone 6

iPhone 6
2[redacted]91-3691108C28A3
AccessToken:
Njdm[redacted]IMzlhNGJkMTYzYzFmOTg2MzJhOGM0YTdjYzJhMQ
Date expires: 27-07-2018 13:00

iPhone 6
2[redacted]91-3691108C28A3
RefreshToken:
MTh[redacted]FiM2VlMThiNjVkNzJjMzMxOGUyNWQ0ZWY0Mg
Date expires: 10-08-2018 12:00

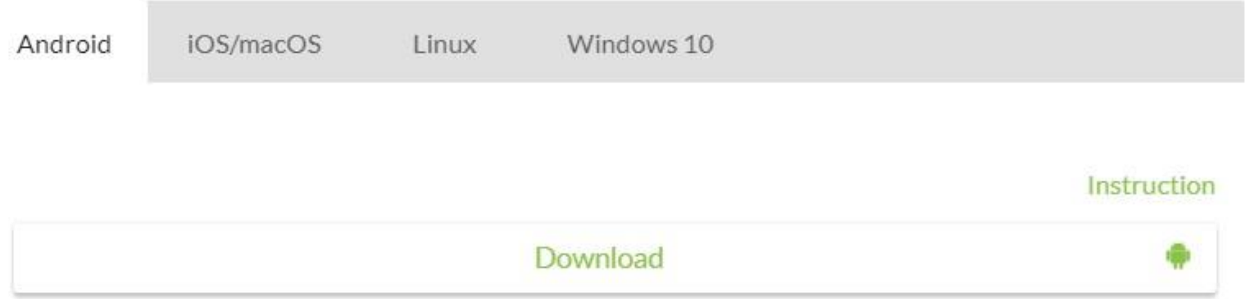
Xiaomi Redmi 3

3.3. VPN

In this section you can download files for configuring the VPN, see the instructions for your operating system and also set a password for your VPN access.

VPN access allows authorized users to access the services of the platform. An unauthorized user (not created in **Controlium**) will not be able to enter the private network where our services are available.

VPN connection can be used for access to the SWISS **SECURIUM**® platform web-services only. You will not be able to use it for Internet or other services access.



VPN configuration may differ for different operating systems:

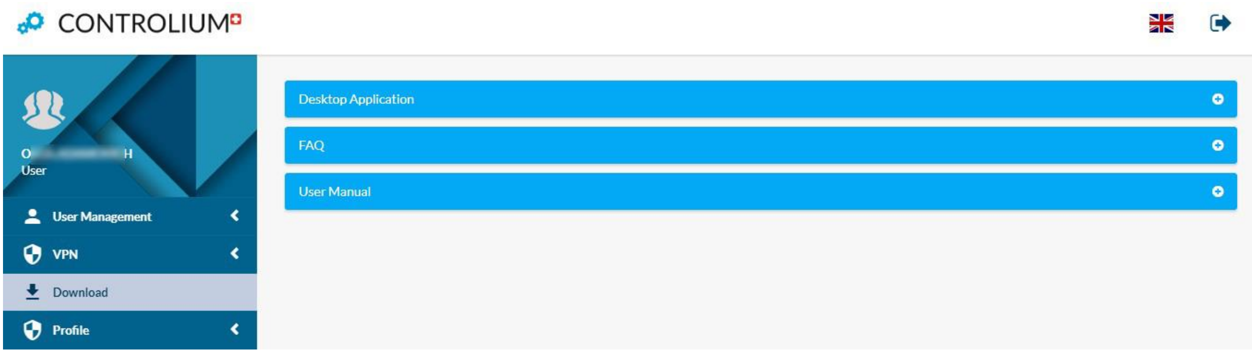
Android / iOS: set in your **Controlium** cabinet a password for the VPN in the <VPN> → <VPN Password> section, go to your smartphone in the AccessSecurium™ application. On the VPN tab in the application, select the account for which you want to enable the VPN, and enter the password that you set in Controlium.

macOS: you need to run the file downloaded from the **Controlium** with .mobileconfig extension, it will make all the necessary settings. After that go to the Wi-Fi settings of your computer and select the just configured VPN connection in the connections list.

VPN configuration for **Windows 10** and **Linux**: at the moment it can cause certain difficulties for common users, please, ask your administrator for help.

3.4. Downloads

In <Download> section of your **Controlium** you can download desktop version of **Swiss**Securium™ messenger for different operating systems, user manuals for the SWISS **SECURIUM**® platform applications and read answers on frequently asked questions about the platform.



CONTROLIUM

[redacted]
User

User Management
VPN
Download
Profile

Desktop Application
FAQ
User Manual

3.5. Other settings of Controlium and AccessSecurium™.

You can set an avatar for your account on <Avatar> tab in <Profile> section of **Controlium**.

You can create folders in **Access**Securium™ to organize storage of your OTP keys. To do this, click on the add icon ⊕ on OTP tab of the application, then tap on folder icon 📁, enter name and choose parent folder for new folder.

To move OTP key in a folder, tap the settings icon ⚙ opposite the key, choose <edit>, change the parent folder for this key.

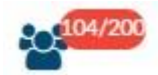
The **Access**Securium™ application allows to store OTP keys not only for SWISS **SECURIUM**® platform applications, but also for side apps and services providing OTP. You can add a key to **Access**Securium™ by QR code scanning or do it manually:

1. Tap on the add icon ⊕.
2. Tap on the key icon 🔑.
3. Enter a name for creating key.
4. Enter a secret (special symbol set which can be suggested instead of QR code).
5. Tap the tick icon ✓ to save the key.

4. ADMINISTRATOR SETTINGS IN CONTROLIUM

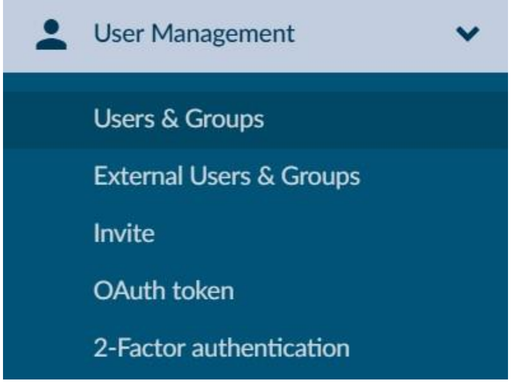
In the **Controlium** cabinet a user with administrator access can view additional information and manage other users and SWISS **SECURIUM**® platform settings.

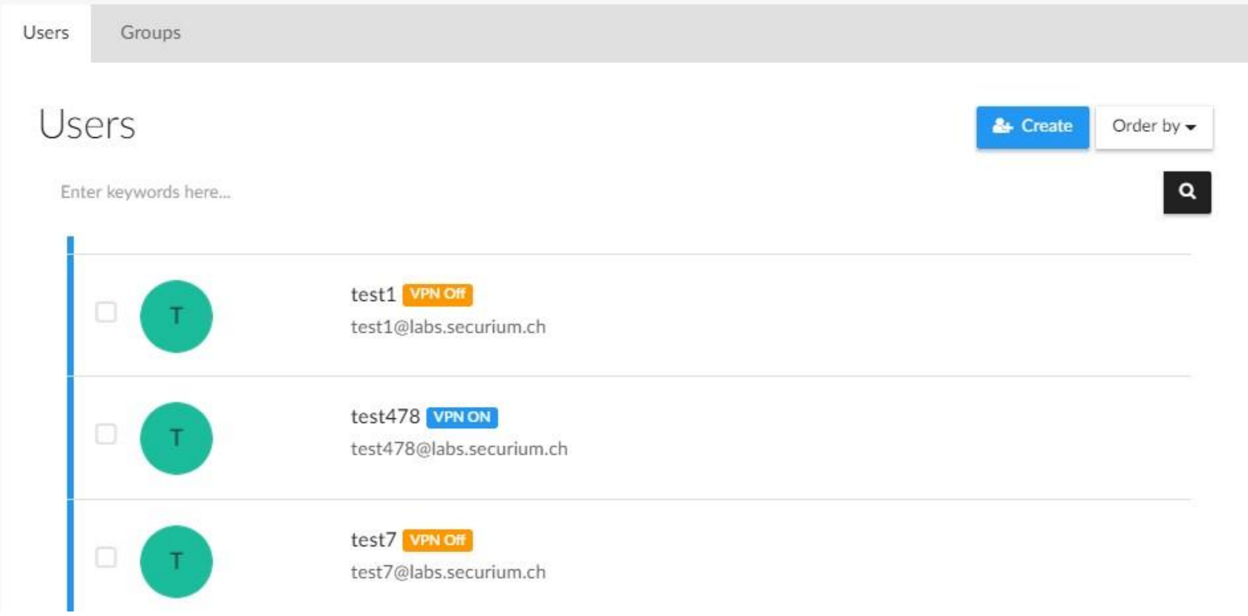
In the upper right corner of the screen you can see how many users have already been created for the instance and the maximum number of users of this instance.



4.1. User management

In <User Management> section an administrator can see <Users & Groups> tab on which the admin can create and edit platform users and user groups.

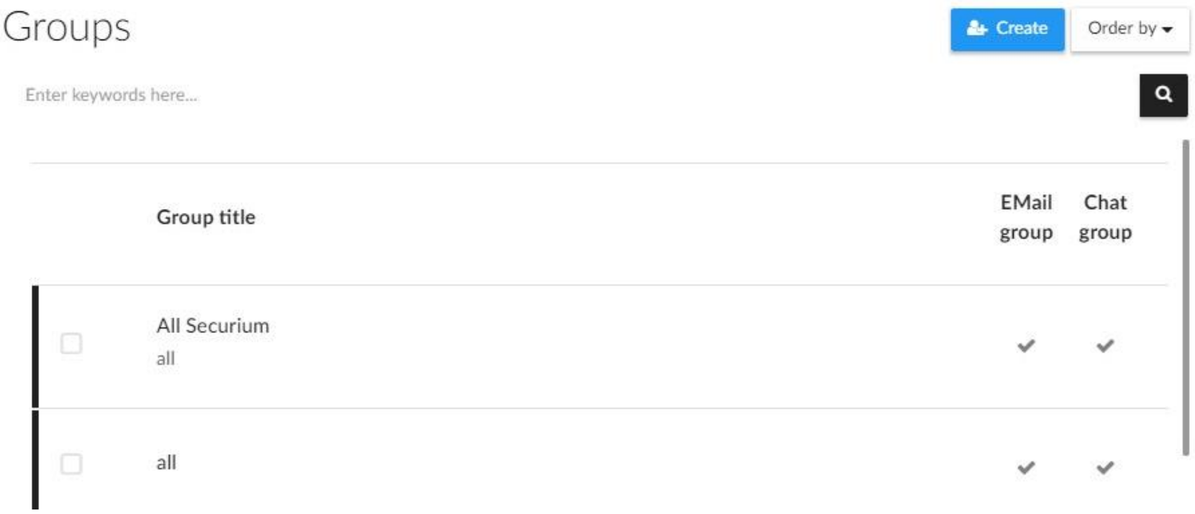




□ T test1 VPN Off
test1@labs.securium.ch

□ T test478 VPN ON
test478@labs.securium.ch

□ T test7 VPN Off
test7@labs.securium.ch



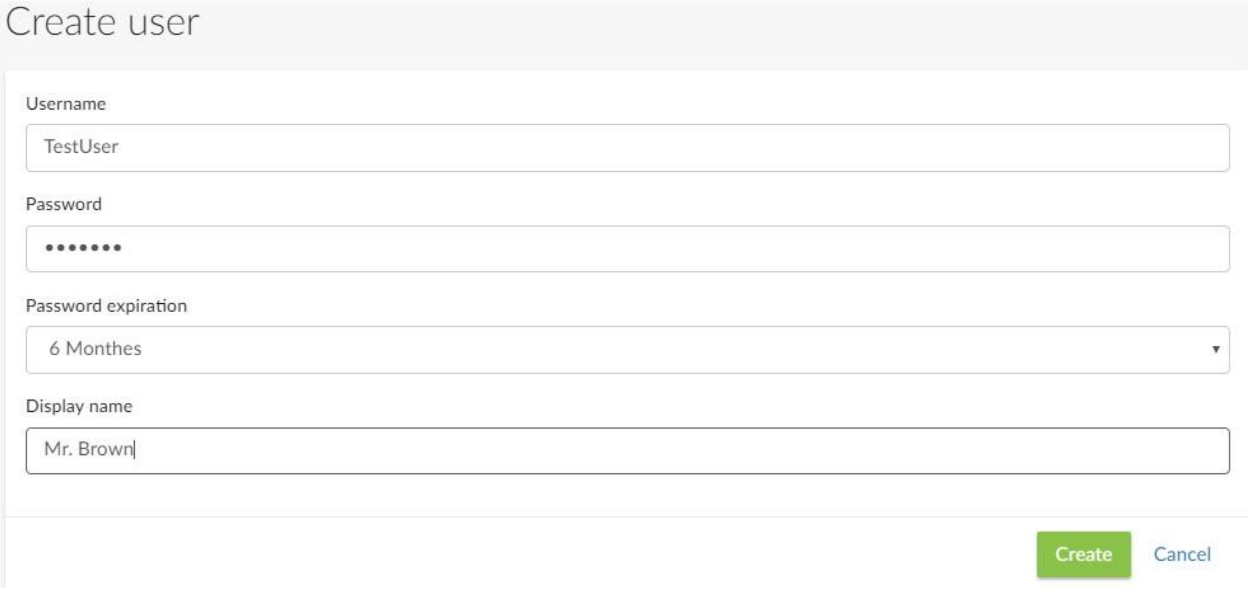
Groups

	Group title	EMail group	Chat group
□	All Securium all	✓	✓
□	all	✓	✓

4.1.1. Creating and editing of users

To create new user:

1. Click <Create> button Create in the upper right corner on the <Users> tab.
2. Fill the fields: Username (this name will be used to sign in to the SWISS **SECURIUM**® user account), Password (for the SWISS **SECURIUM**® account), Password expiration, Display name (the username that will appear in contact lists and other similar lists, it can’t be used to sign in to the user account).
3. Save new user.



Create user

Username: TestUser

Password: •••••••

Password expiration: 6 Monthes

Display name: Mr. Brown

To edit user data and settings:

1. Click on the avatar or the username on <Users> tab in <Users & Groups> section.
2. Change user data and settings.
3. Save or cancel.

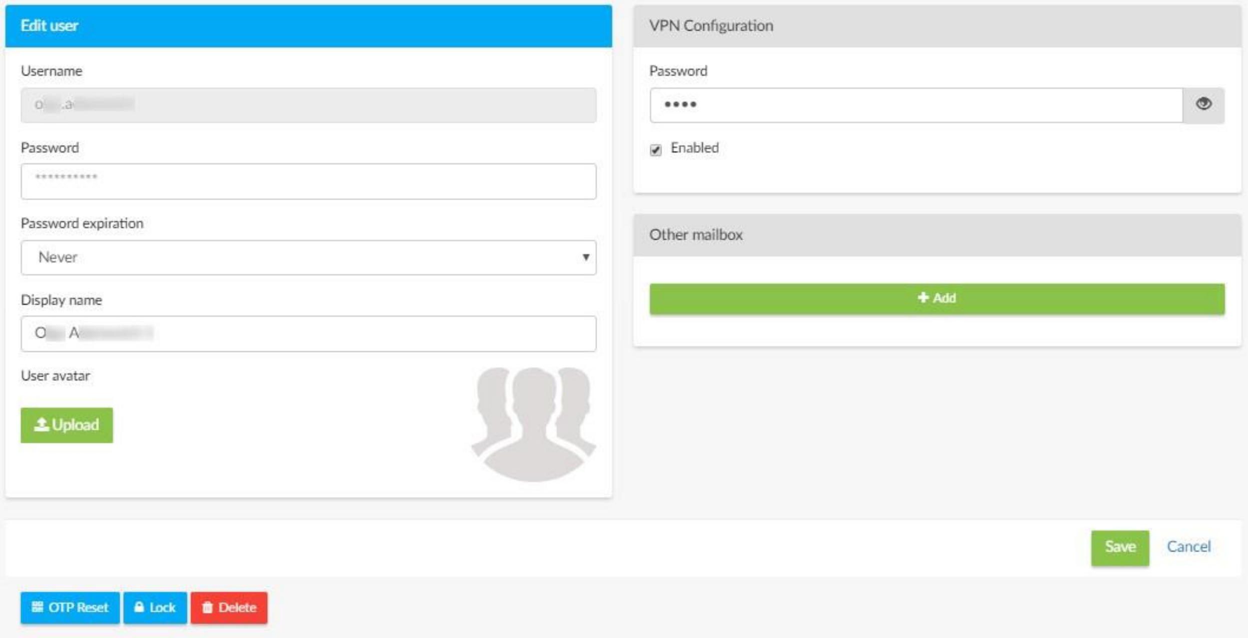
The administrator can change Username, SWISS **SECURIUM**® account password, Password expiration, Display username and user avatar.

The administrator can also turn on / off VPN access for users and set a password for it.

In <Other mailbox> field you can add alias for user platform email.

There are 3 buttons for managing user access at the bottom left:

- Button OTP Reset resets the user's OTP access to the applications. To re-enable OTP, the user must log into his Controlium cabinet and scan again all QR codes.
- Button Lock blocks the access to all SWISS **SECURIUM**® services.
- Button Delete removes the user and all his data from the instance without the possibility of recovery.


Edit user

Username: o[redacted].a[redacted]

Password: **********

Password expiration: Never

Display name: O[redacted] A[redacted]

User avatar

VPN Configuration

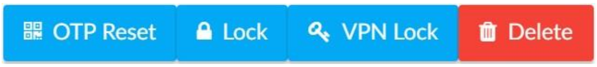
Password: ••••

☑ Enabled

Other mailbox

Mass actions with users:

On <Users> tab in <Users & Groups> section tick all users you want to perform one of the mass actions to. The panel with buttons for mass actions will appear in the upper right corner:



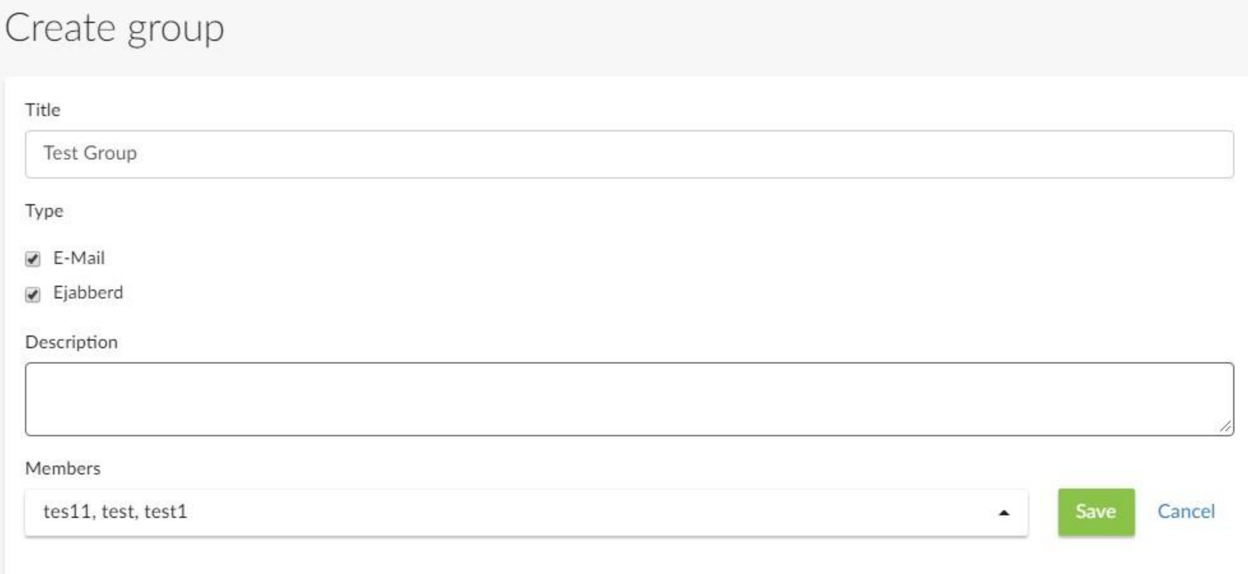
- <OTP Reset> button resets the chosen users OTP access to the web-applications. To re-enable OTP, the users must log into their **Controlium** cabinets and scan again all QR codes.
- <Lock> button blocks the users access to all SWISS **SECURIUM**® services.
- <VPN Lock> button changes on / off status of the VPN access for the users.
- <Delete> button removes the chosen users.

4.1.2. Creating and editing of groups

To create new group:

1. Click the <Create> button Create in the upper right corner on the <Groups> tab.

2. Fill the fields: Title (group name), choose a group Type (E-mail creates a distribution group and includes selected users in it, Ejabberd creates a chat group in the **Swiss**Securium™ messenger and adds selected users there), Description (optional), group Members (choose from the drop-down list).
3. Save or cancel.



Create group

Title

Test Group

Type

☑ E-Mail

☑ Ejabberd

Description

Members

tes11, test, test1

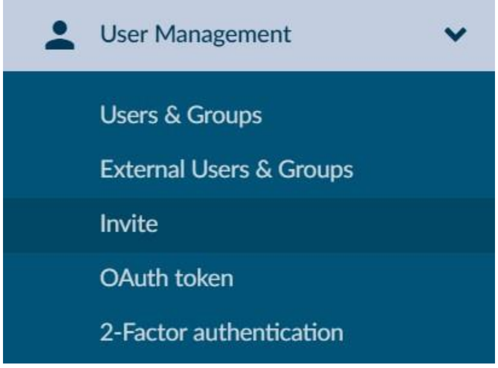
To edit a group:

1. Click on a group name in the list on the <Groups> tab.
2. Edit necessary fields: Title, Type, Description, Members.
3. Save.

To delete a group:

1. Tick groups from the list on the <Groups> tab, click 🗑 Delete in the upper right corner of the screen to remove all ticked groups.
2. In the group edit mode, you can delete the group by clicking the <Delete> button 🗑 Delete in the upper right corner.

4.1.3. Inviting of external users



You can invite external users (which are not set on the corporate platform SWISS **SECURIUM**®) on the <Invite> tab of the <User Management> section.

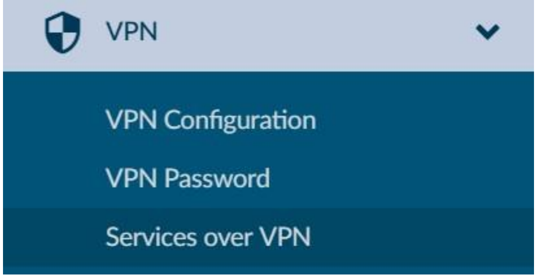
Enter the Group name or select an existing group from the drop-down list for invited users, enter the e-mails to which invitations will be sent and the expiration date of the invitation (after which the platform services will no longer be available to these users).

Attention! Before clicking on the invitation link, external users should install the **Swiss**Securium™ application on their device.

External users and groups can be viewed and edited on the <External Users & Groups> tab of the <User Management> section.

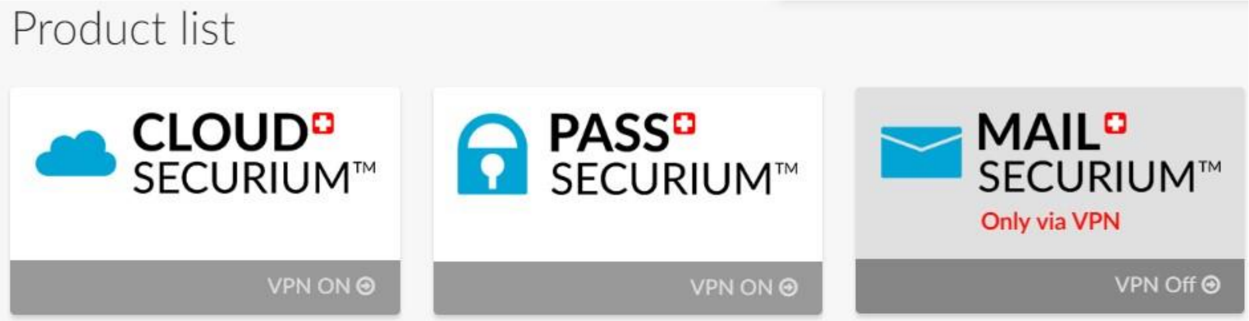
You can invite new external users until you reach the maximum number of users for your SWISS **SECURIUM**® corporate instance.

4.2. Turning on/off VPN access to the platform services

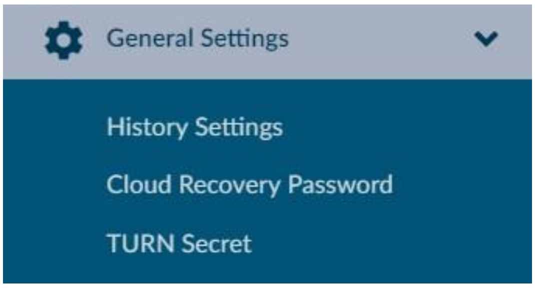


In the <VPN> section on the <Services over VPN> tab, administrator can turn on and off the VPN access to the separate services of SWISS **SECURIUM**® platform.

If you enable access only through VPN for a service, users who haven't configured VPN will not be able to use this service.



4.3. General settings

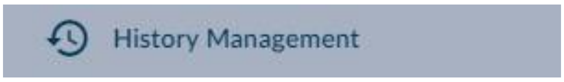


On the <History Settings> tab you can set history storage period for the **Swiss**Securium™ messenger.

On the <Cloud Recovery Password> tab you can find a password for restoring access to **Cloud**Securium™ in case a user forgets his password. All files are stored in an encrypted form and they can't be decrypted without a user password. But with the help of this recovery password the administrator can restore the user access to the files. This process is automated in the SWISS **SECURIUM**® platform, so the administrator simply needs to change the user's account password.

On the <TURN Secret> tab you can set a secret for encryption of voice calls in **Swiss**Securium™.

4.4. History



In the <History Management> section the administrator can see all changes made in **Controlium** by other users and administrators.