



StealthMail Management Tool for Administrators and Security Officers

User Guide

Version 1.3.0.2

Table of Contents

1. About this guide	3
2. About this application	3
3. Overview of user functions	3
4. Authorization	4
5. Administrator functions	5
5.1 Changing personal password	5
5.2 Changing a phone number of an external user	6
5.3 Getting information about user events	7
6. Security Officer functions	8
6.1 Changing personal password	8
6.2 Changing password of an Add-In user	9
6.3 Changing a phone number of an external user	10
6.4 Setting a personal limit on the number of user devices	11
6.5 Setting a global limit on the number of user devices	12
6.6 Getting information about user devices	13
6.7 Getting information about user events	14
7. Logging out	16

1. About this guide

This guide provides step-by-step instructions for StealthMail Administrators and Security Officers on how to use the StealthMail Management Tool.

2. About this application

StealthMail Management Tool is an application developed to manage users who use StealthMail service to create and view secure emails (StealthMail Add-In, StealthMail Desktop App, StealthMail Mobile Viewer for iOS and Android).

The application is developed for **Administrators** and **Security Officers**.

3. Overview of user functions

Functions available to the **Administrator**:

- Changing personal password;
- Changing a phone number of an external user;
- Getting information about user events.

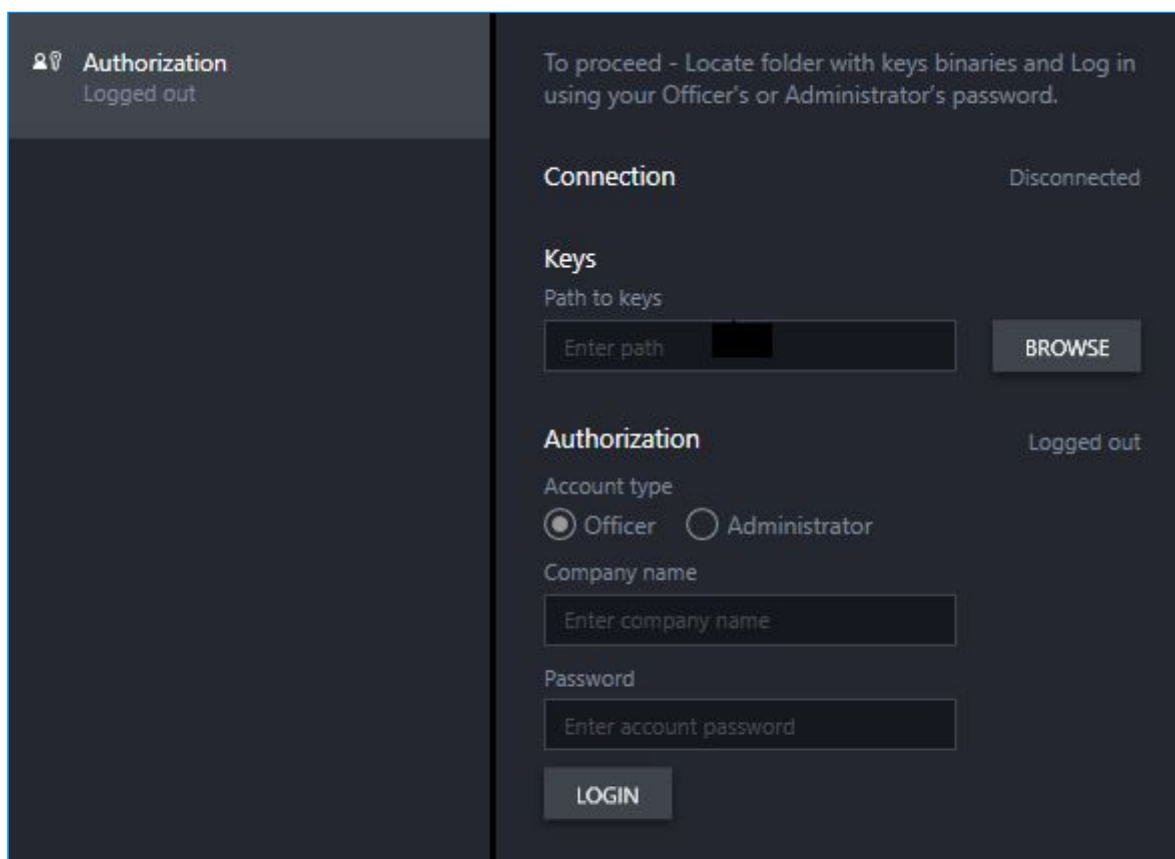
Functions available to the **Security Officer**:

- Changing personal password;
- Changing Add-In user's password;
- Changing a phone number of an external user;
- Setting a limit on the number of user devices;
- Setting a limit on the global number of devices;
- Getting information about the user's devices.

4. Authorization

To authorize, follow the instructions below (Fig. 4.1):

1. In the **Authorization** menu, in the **Keys** section, click **Browse**.
2. In the opened dialog box, specify the path to the folder with the security key.
3. In the **Authorization** section, select the account type - **Officer** or **Administrator**.
4. In the **Company name** field, enter the name of your company.
5. In the **Password** field, enter your password.
6. Click **LOGIN**.



The screenshot shows the main window of the StealthMail Management Tool. The title bar reads 'Authorization' and 'Logged out'. The main content area is divided into two sections. The top section is titled 'Keys' and contains a 'Path to keys' label, a text input field with the placeholder 'Enter path', and a 'BROWSE' button. The bottom section is titled 'Authorization' and contains a 'Logged out' status indicator, an 'Account type' section with radio buttons for 'Officer' (selected) and 'Administrator', a 'Company name' label, a text input field with the placeholder 'Enter company name', a 'Password' label, a text input field with the placeholder 'Enter account password', and a 'LOGIN' button.

Figure 4.1 Main window

After authorization, a **10-minute session** will be set up.

At the end of the session, you will be transferred to the **Authorization** page, where, if necessary, you will be able to re-authorize.

5. Administrator functions

This section provides information about the functions which an administrator can perform in StealthMail Management tool.

5.1 Changing personal password

This function allows to change the current password of an administrator.

To change a password (Fig. 5.1):

1. Start the application and log in as **an administrator**.
2. Go to the **Change password** menu.
3. In the **Password** field, enter a new password, adhering the guidelines for length and character set.
4. In the **Password confirmation** field, repeat the new password.
5. Click **SET PASSWORD**.

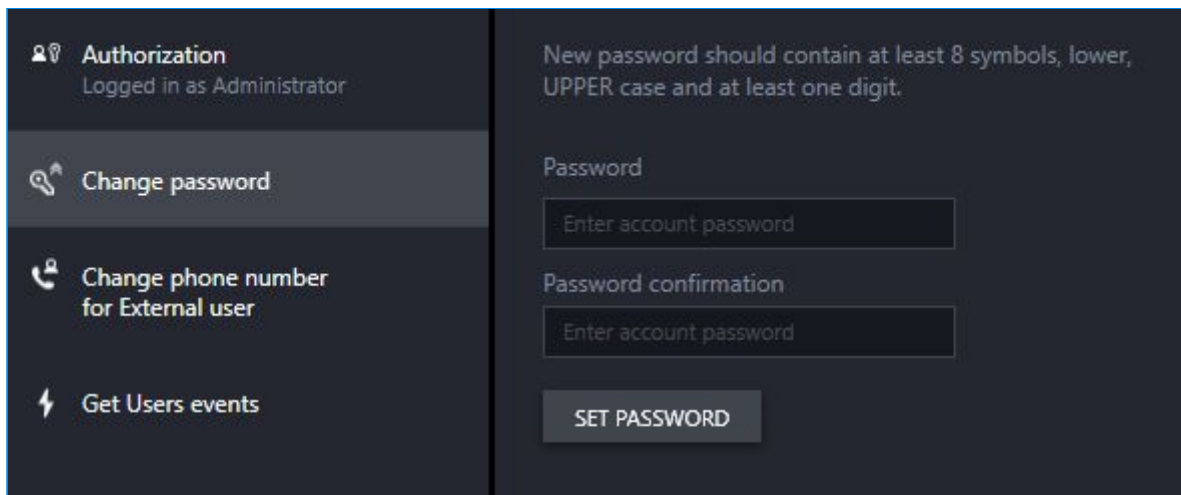
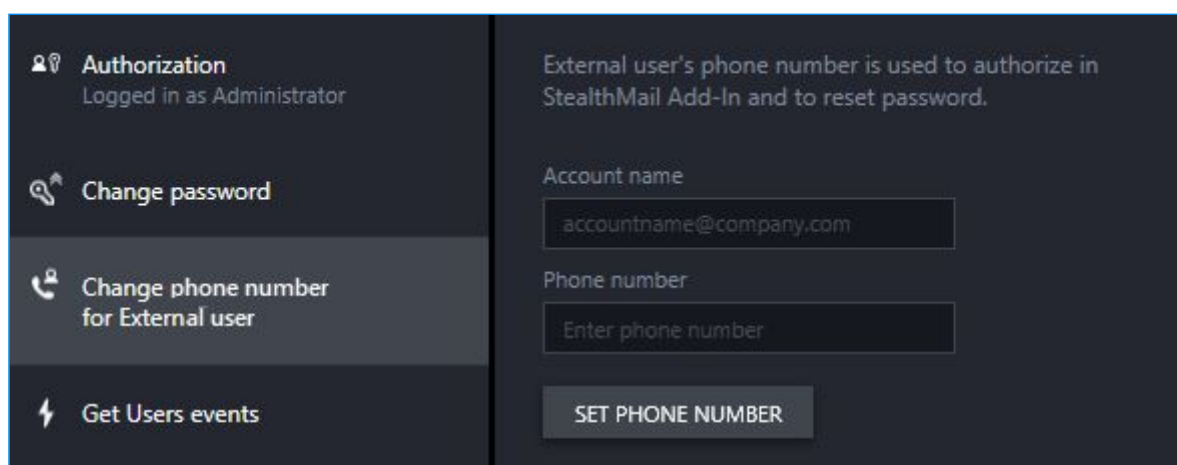


Figure 5.1 Changing administrator's password

5.2 Changing a phone number of an external user

To change a phone number (Fig. 5.2):

1. Start the application and log in as **an administrator**.
2. Go to the **Change phone number For External user** menu.
3. In the **Account name** field, enter the full name of the external user account you want to change the phone number for.
4. In the **Phone number** field, enter a new phone number.
5. Click **SET PHONE NUMBER**.



The screenshot shows a dark-themed user interface. On the left is a vertical sidebar with four menu items: 'Authorization' (with a user icon and 'Logged in as Administrator'), 'Change password' (with a key icon), 'Change phone number for External user' (with a phone icon and highlighted), and 'Get Users events' (with a lightning bolt icon). The main content area on the right has a heading: 'External user's phone number is used to authorize in StealthMail Add-In and to reset password.' Below this are two input fields: 'Account name' containing 'accountname@company.com' and 'Phone number' containing 'Enter phone number'. At the bottom right is a button labeled 'SET PHONE NUMBER'.

Figure 5.2 Changing a phone number of an external user

5.3 Getting information about user events

The administrator can request different information about user events within a certain period of time: by months, weeks or days.

The administrator can also monitor user activity by sorting the event by specific filters.

In addition to the time period, the application also has such filters as Event name, Account, Device ID, Operating system and IP address.

To get information about user events (Fig. 5.3-1):

1. Start the application and log in as **an administrator**.
2. Go to the **Get user events** menu.
3. In the **Filter** section, in the **From** field, specify the beginning of the time period.
4. In the **Filter** section, in the **To** field specify, the end of the time period.
5. To sort the events by additional parameters, click **ADD FILTER OPTION**.
6. After setting the event sorting parameters, click **GET EVENTS**.

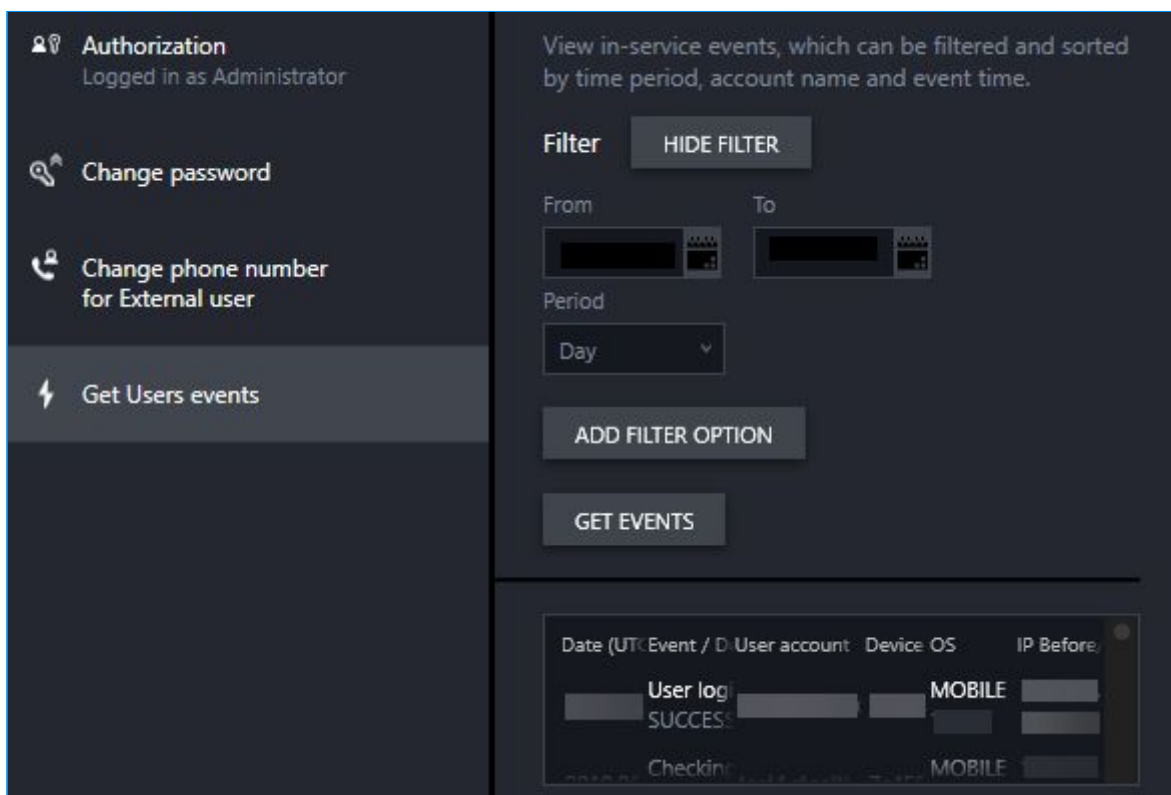


Figure 5.3-1 Getting information about user events

6. Security Officer functions

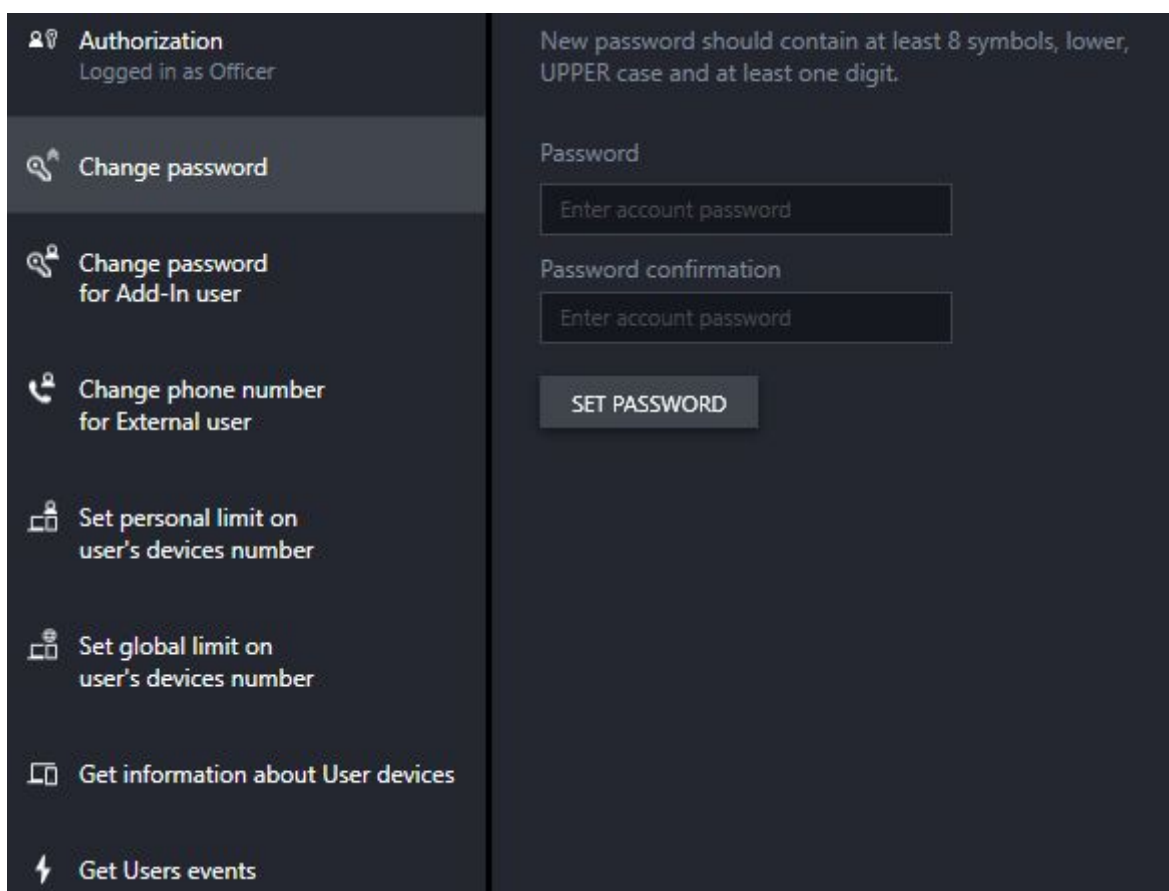
This section provides information about the functions which a security officer can perform in StealthMail Management tool.

6.1 Changing personal password

This function allows to set a new password for the current user type.

To set a password (Fig. 6.1):

1. Start the application and log in as a **security officer**.
2. Go to the **Change password** menu.
3. In the **Password** field, enter a new password, adhering the guidelines for length and character set.
4. In the **Password confirmation** field, repeat the new password.
5. Click **SET PASSWORD**.



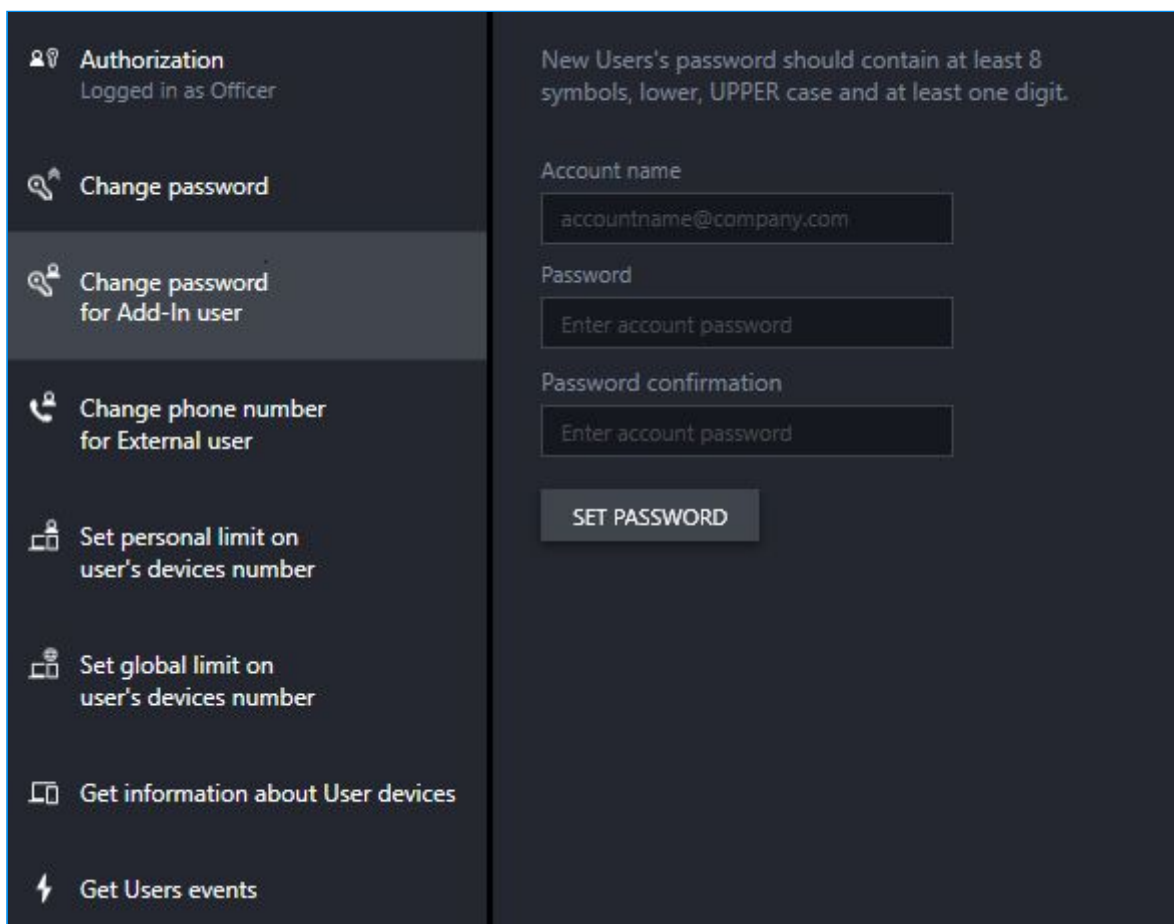
The screenshot displays the user interface for a security officer. On the left, a dark sidebar menu is visible with the following items: 'Authorization' (Logged in as Officer), 'Change password' (highlighted), 'Change password for Add-In user', 'Change phone number for External user', 'Set personal limit on user's devices number', 'Set global limit on user's devices number', 'Get information about User devices', and 'Get Users events'. The main content area on the right shows a form for changing the password. At the top, it states: 'New password should contain at least 8 symbols, lower, UPPER case and at least one digit.' Below this, there are two input fields: 'Password' and 'Password confirmation', both with placeholder text 'Enter account password'. A 'SET PASSWORD' button is located at the bottom of the form.

Figure 6.1 Setting personal password

6.2 Changing password of an Add-In user

To change a password (Fig. 6.2):

1. Start the application and log in as a security officer.
2. Go to the **Change password for Add-In user** menu .
3. In the **Account name** field, enter the full name of the Add-in user account whose password you want to change.
4. In the **Password** field, enter a new password, adhering the guidelines for length and character set.
5. In the **Password confirmation** field, repeat the new password.
6. Click **SET PASSWORD**.



Authorization
Logged in as Officer

Change password

Change password for Add-In user

Change phone number for External user

Set personal limit on user's devices number

Set global limit on user's devices number

Get information about User devices

Get Users events

New Users's password should contain at least 8 symbols, lower, UPPER case and at least one digit.

Account name
accountname@company.com

Password
Enter account password

Password confirmation
Enter account password

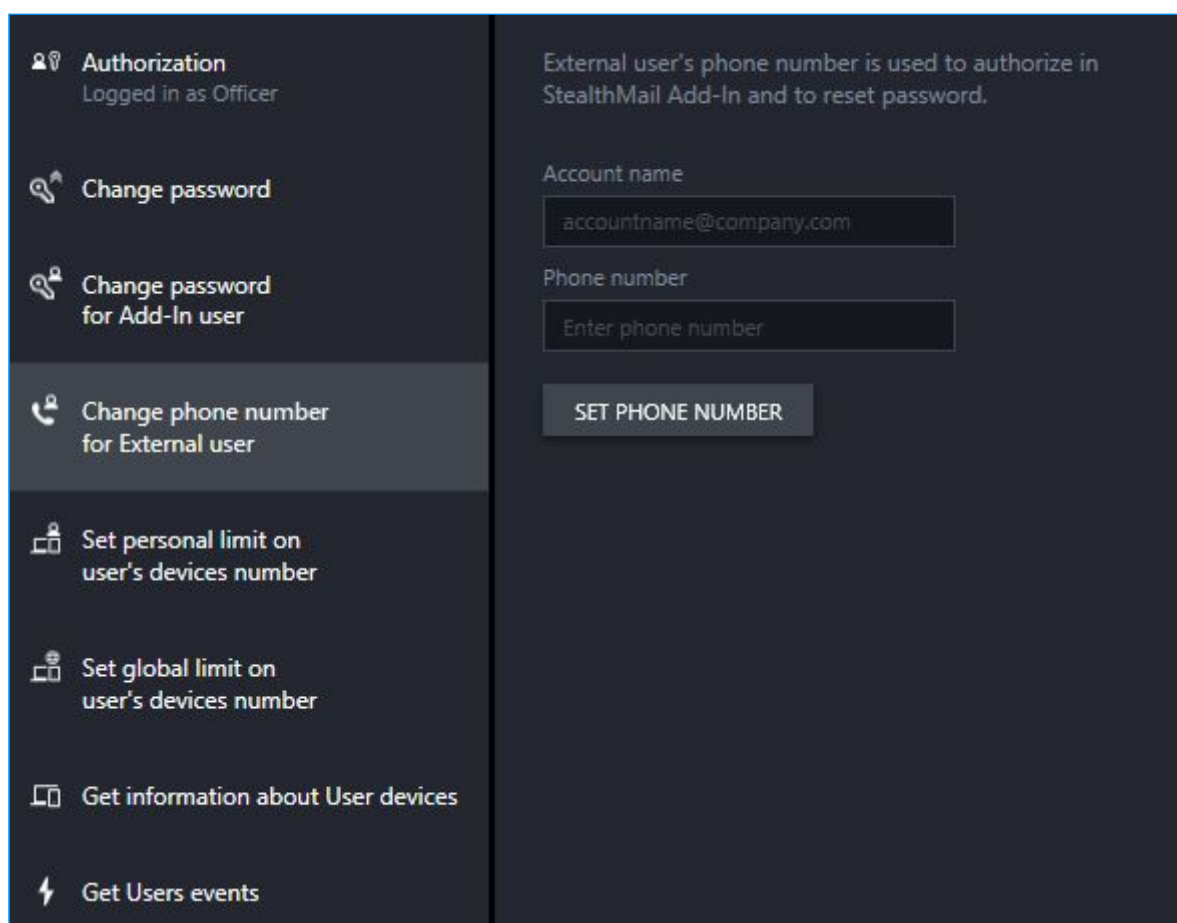
SET PASSWORD

Figure. 6.2 Changing password of an add-in user

6.3 Changing a phone number of an external user

To change a phone number (Fig. 6.3):

1. Start the application and log in as a security officer.
2. Go to the **Change a phone number of an external user** menu .
3. In the **Account** field, enter the full name of the external user account you want to change the phone number for.
4. In the **Phone number** field, enter a new phone number.
5. To complete, click **SET PHONE NUMBER**.



Authorization
Logged in as Officer

Change password

Change password for Add-In user

Change phone number for External user

Set personal limit on user's devices number

Set global limit on user's devices number

Get information about User devices

Get Users events

External user's phone number is used to authorize in StealthMail Add-In and to reset password.

Account name
accountname@company.com

Phone number
Enter phone number

SET PHONE NUMBER

Fig. 6.3 Changing a phone number of an external user

6.4 Setting a personal limit on the number of user devices

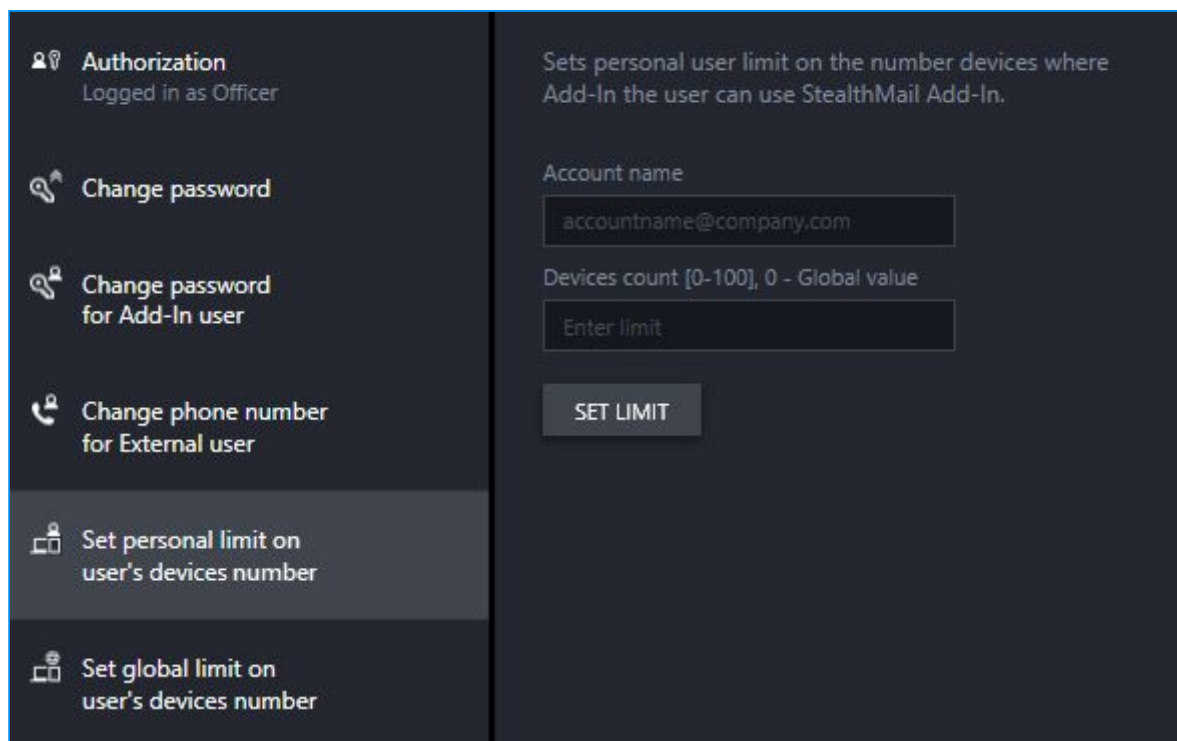
The number of user devices can be set between 0 and 100.

"0" means that a global limit on the number of user devices will be used.

Important: It is recommended to use a **personal limit** for setting the number of user devices as it is considered to be a higher priority than the *global limit*.

To set a personal limit (Fig. 6.4):

1. Start the application and log in as a security officer.
2. Go to **Set personal limit on user's devices number** menu.
3. In the **Account name** field, enter the full name of the user account you want to change the password for.
4. In the **Devices count** field, specify the number of devices which a user can authorize his StealthMail account on.
5. To complete, click **SET LIMIT**.



The screenshot shows a dark-themed user interface. On the left is a vertical menu with several options, each with a lock icon. The option 'Set personal limit on user's devices number' is highlighted in a lighter shade. The main area on the right contains the following text and form elements:

- Header: Sets personal user limit on the number devices where Add-In the user can use StealthMail Add-In.
- Field: Account name with the value accountname@company.com.
- Field: Devices count [0-100], 0 - Global value with the value Enter limit.
- Button: SET LIMIT.

Fig. 6.4 Setting a personal limit on the number of user's devices

6.5 Setting a global limit on the number of user devices

The number of devices can be set between 0 and 100.

"0" means that there is no limit on the number of devices.

To set a global limit (Fig. 6.5):

1. Start the app and log in as a **security officer**.
2. Go to **Set global limit on user's devices number**.
3. In the **Devices count** field, specify the number of devices which users can register their StealthMail account on.
4. To complete, click **SET LIMIT**.

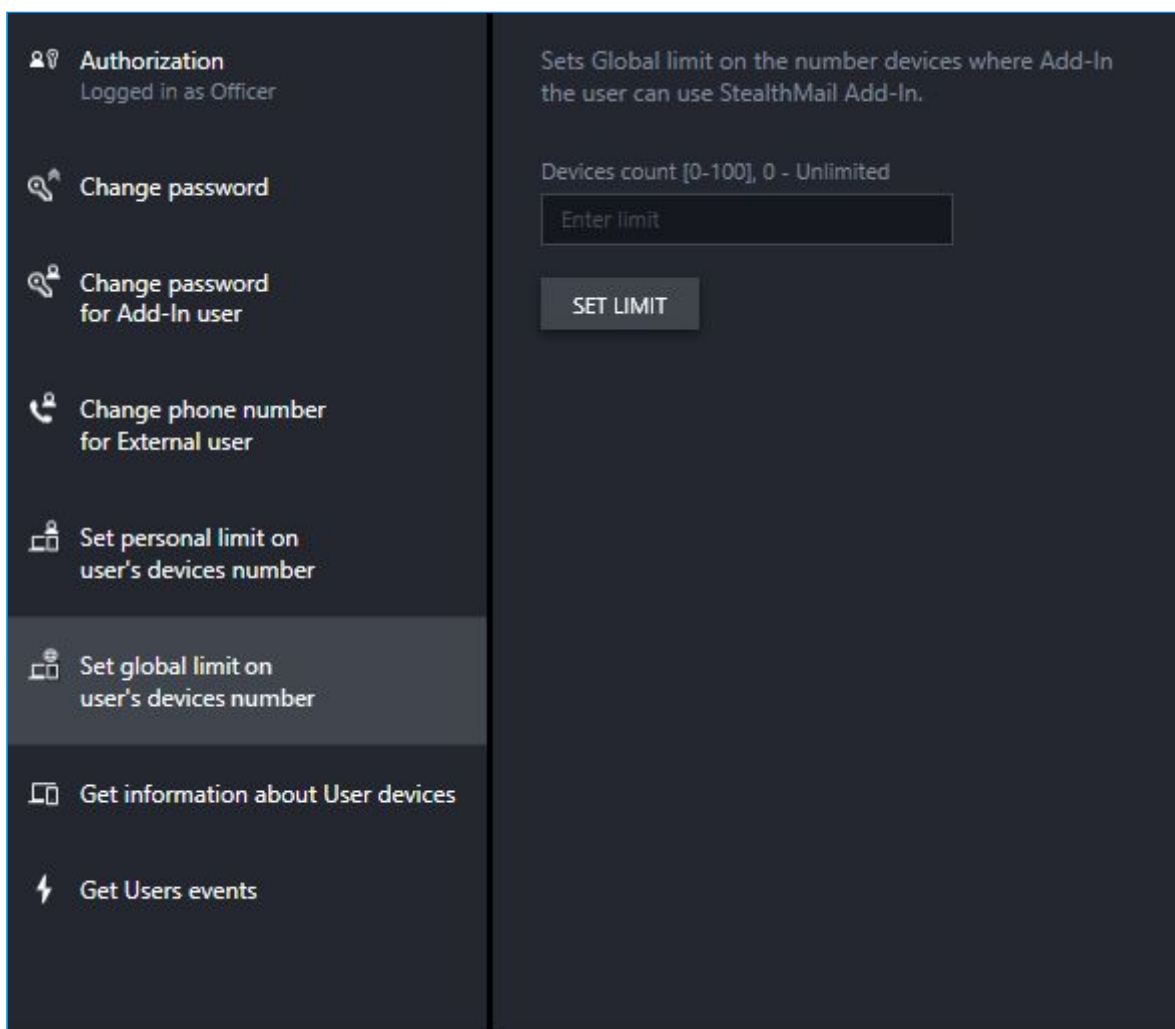


Fig. 6.5 Setting a global limit on the number of user devices

6.6 Getting information about user devices

The security officer can request various information about the devices of the user and, if necessary, block a particular device.

To request information (Fig. 6.6):

1. Start the application and log in as a **security officer**.
2. Go to the **Get information about the user devices** menu.
3. In the **Account name** field, enter the full name of the user account whose device information you want to obtain.

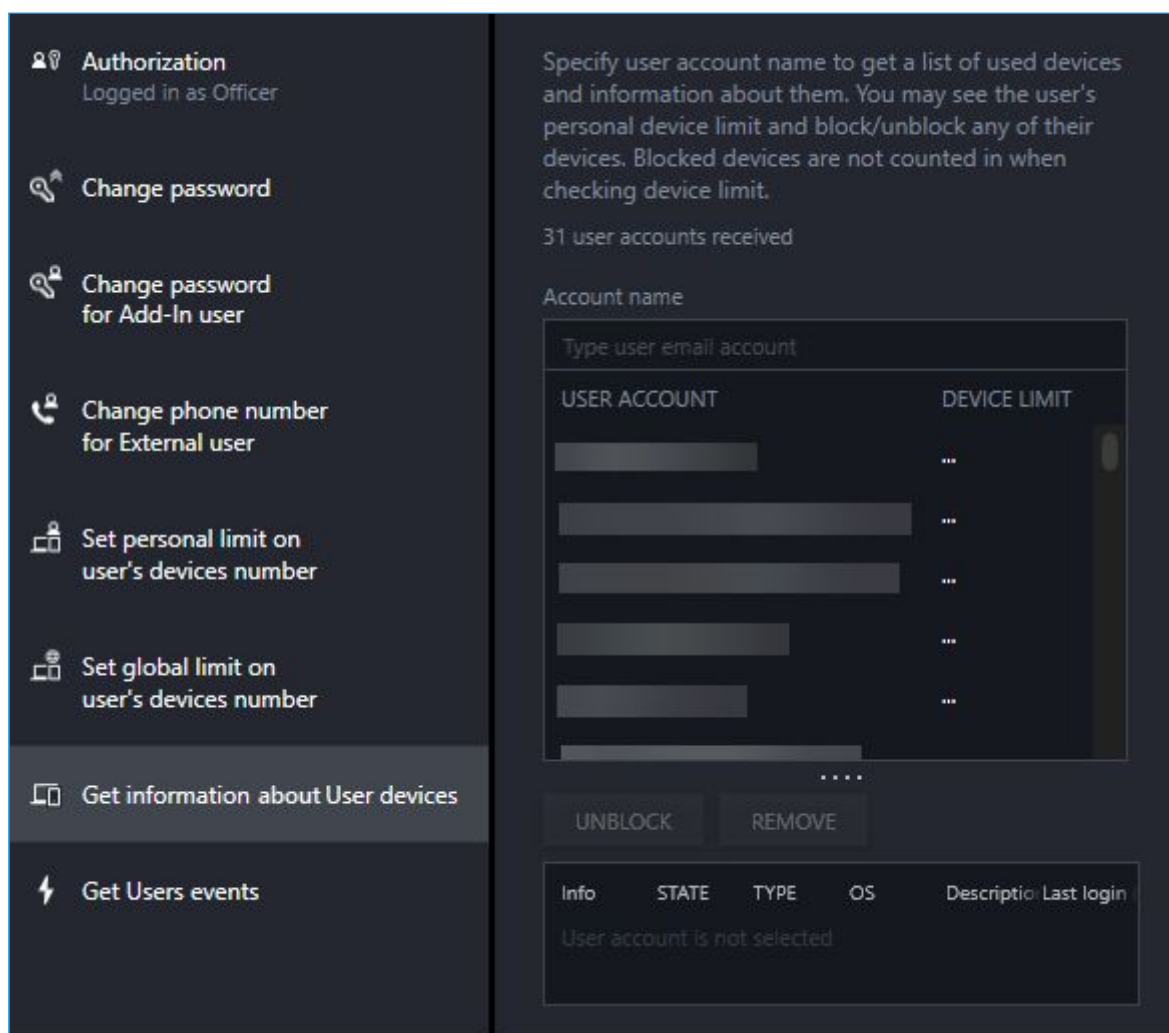


Fig. 6.6 Getting information about user devices

6.7 Getting information about user events

The security officer can request different information about user events within a certain period of time: by months, weeks or days.

The security officer can also monitor user activity by sorting the event by specific filters.

In addition to the time period, the application also has such filters as: Event name, Account, Device ID, Operating system and IP address.

To get information about user events (Fig. 6.7-1):

1. Start the application and log in as a **security officer**.
2. Go to the **Get User events** menu.
3. In the **Filter** section, in the **From** field, specify the beginning of the time period.
4. In the **Filter** section, in the **To** field specify, the end of the time period.
5. To sort the events by additional parameters, click **ADD FILTER CRITERION**.

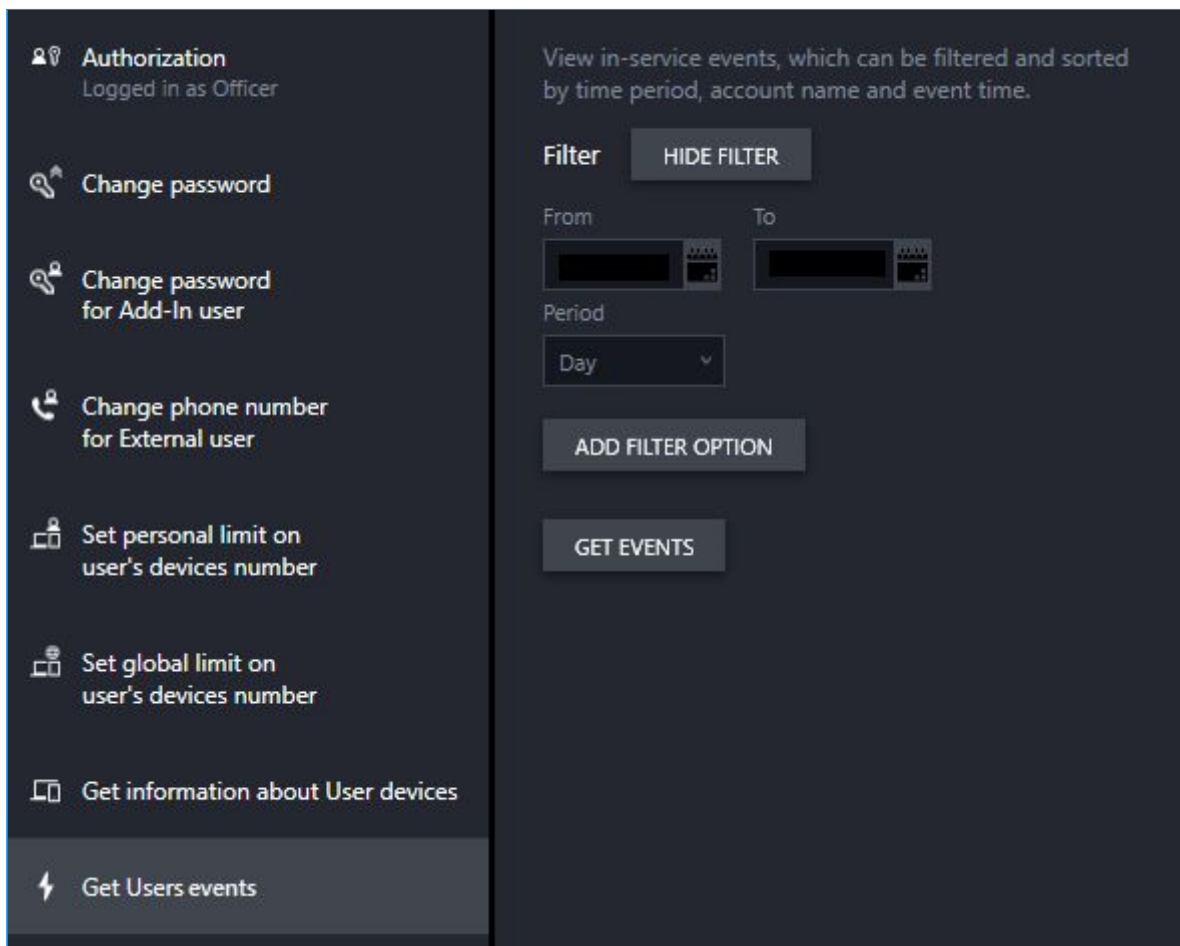


Figure 6.7-1 Getting information about user events

6. After setting the event sorting parameters, click **GET EVENTS** (Fig. 6.7-2).

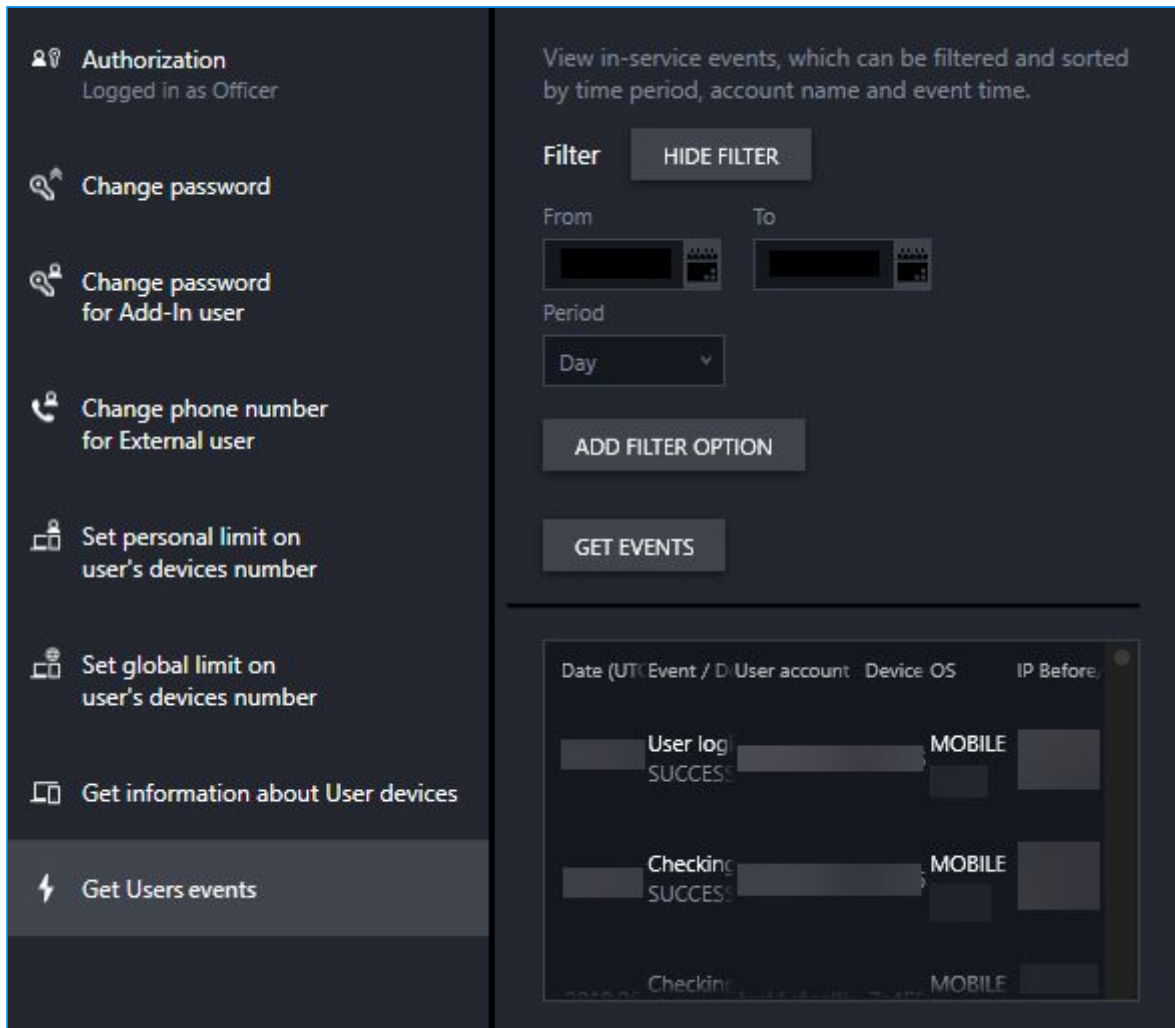


Figure 6.7-2 Getting information about user events

7. Logging out

To complete current session in the application (Fig. 7):

1. Go to the **Authorization** menu.
2. In the Authorization menu, click **LOGOUT**.

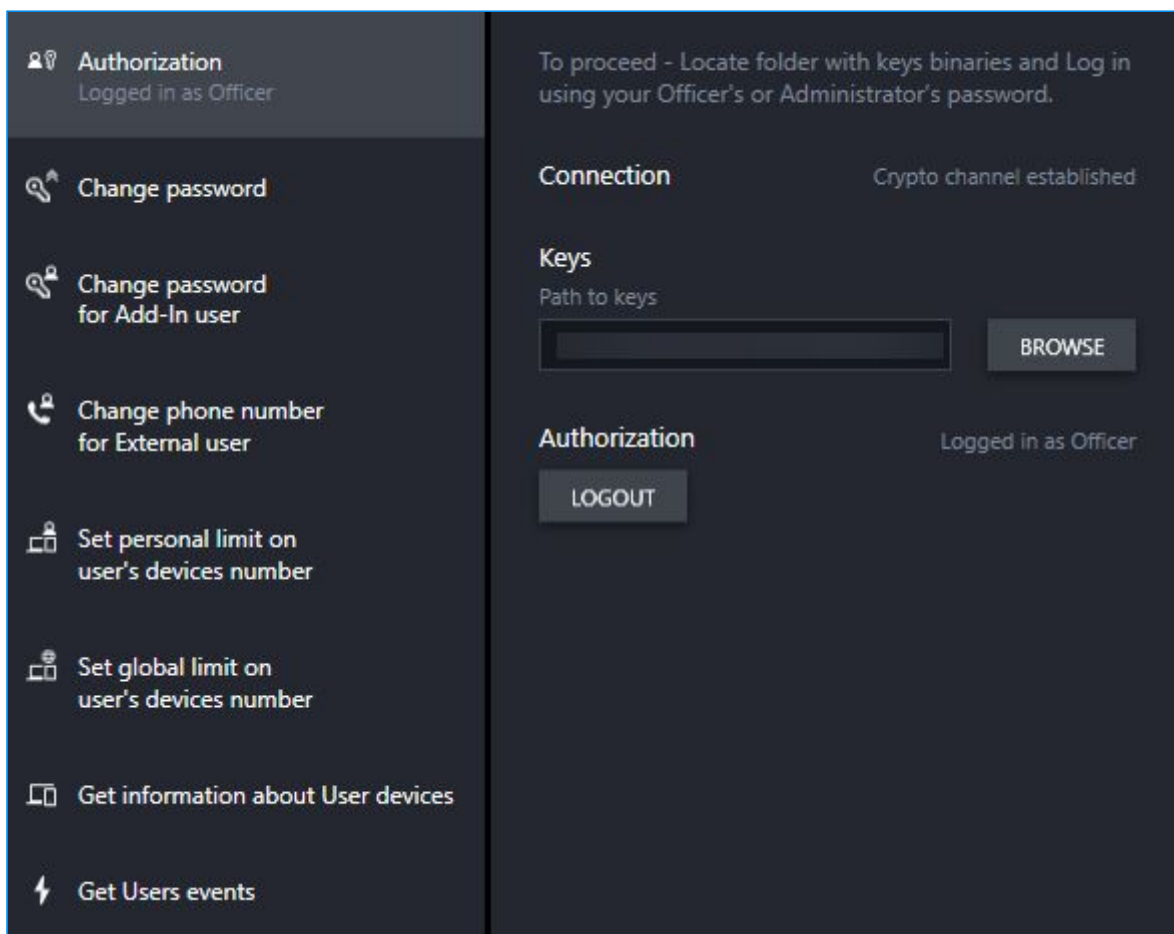


Fig. 7 Session completion