SecuriCloud

SecuriFire Remote Access
SecuriFire Mobile Control

Application-Information

Table of contents

1 SecuriFire

1.1 General information

Remote Connections to the SecuriFire fire alarm Control Panel can be established via SecuriCloud. This can currently be realized via the SecuriFire Studio, a VirtualMIC or a mobile operator application (SecuriFire MobileControl). The relevant settings are shown in this document.

Note
From the standard template R2.3.0 onwards, two different SecuriCloud users with different authorization are now configured in the remote settings. On the one hand, this is a user for remote access via SecuriFire Studio and VirtualMIC, and on the other hand a user for connection with the SecuriFire MobileControl App.

Warning: Country specific regulations for remote operation and configuration must be observed.
A pure readout of data from the control panel is basically possible at any time and without further precautions. For remote control via SecuriCloud (program changes, downloads, manipulations such as shutdowns, activations or similar on the system), the operator himself or a person instructed by him must be present on site to enable access. This person controls the operational readiness during and after completion of the work. It also ensures that any compensation measures are taken.

1.2 Requirements to connect to SecuriCloud

- The order form OF-220721 must be completed and available.
- A SecuriCloud router or the "alarmVPN" service on the transmission device must be present.
- In the customer network, access to the cloud from the SecuriFire fire alarm control panel must be enabled.

Settings in SecuriFire Studio:
From the standard template 2.3.0, users are already prepared for remote access.

Warning
As this is a security system, it is strongly recommended that the password is assigned specifically to the system. The security can be further increased if the username is also defined plant-specific.

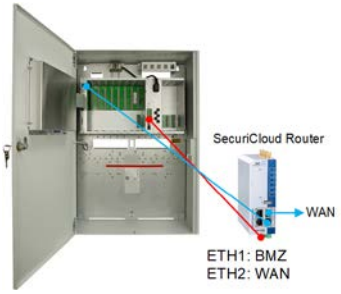
To set up a connection between SecuriFire and SecuriCloud, the following settings must be made.

- IP, subnet and gateway
- NTP settings
- Change passwords
- Set the display "Fire brigade alerted" correctly for the app

HW adjustments
Router NB1600

If a NET card is inserted, the NET card must be plugged in!

Router NB1601



If a NET card is inserted, the NET card must be plugged in!

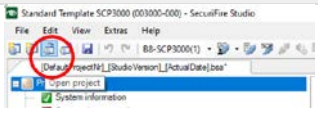
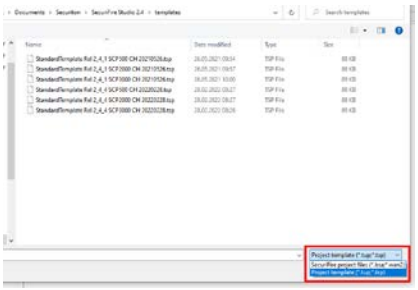
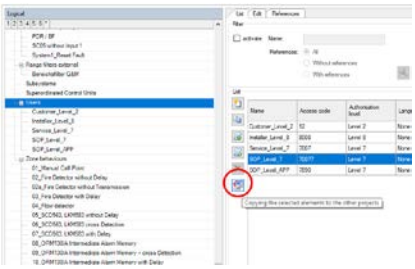
The SecuriFire - Remote services and SecuriFire - MobileControl are only available from Release 2.3.0. Therefore, the SecuriFire system must first be upgraded to at least Release 2.3.0.

1.3 Step-by-step instructions

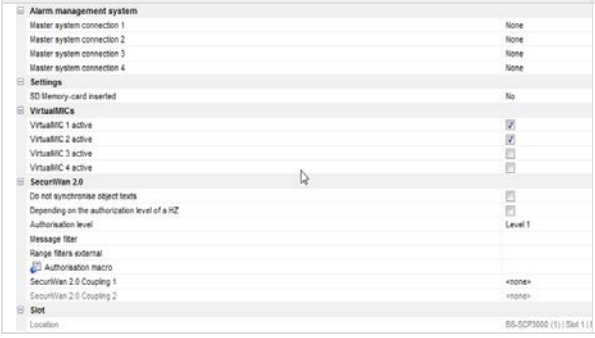
The step-by-step instructions are based on release 2.4.4 but are identical for all versions as of 2.3.0.
If the required users are not yet available in the project, they can be added from the respective template that is supplied with the installation.
We recommend to use the latest version whenever possible.

1. Upgrade all Control Panels and MIC 711 to the latest Release.
2. From the "StandardTemplate the following elements must be imported into the project.
3. User "SOP_Level_7"
4. User "SOP_Level_APP"
5. Authorisation macro "Authority SOP VMIC"
6. MIC Menus "MIC Menu_0002"
7. Boolean function "Authority Switch SOP VMIC

The easiest way to do this is to open the standard template mentioned above in addition to the project.

1. Open second project	**2. Switch to project templates and select the most recent template**	**3. The corresponding elements with the function "Copy the selected elements into the primary project".**
	 Expand the selection to open to the project templates. After this step, two projects are opened in SecuriFire Studio.	 The selected entries are imported into the customer project.

A second virtual MIC must be opened on the MCB card in the Control Panel where the SOP is activated. This virtual MIC is imported into the customer project.

Open a second VirtualMIC	Settings of the second VirtualMIC for Remote Access
	

1.4 IP Address, Subnet and Gateway

The settings can be seen on the SecuriCloud order form and must be adopted accordingly.

- **General settings (SecuriFire Studio)**

IP Range	192.168.192.X
Subnet Mask	255.255.255.0
Standard Gateway	192.168.192.254

Enter the IP address of the router/alarmVPN as the gateway.

General Settings

Network settings	
Settings individually per SCP/MIC711	☐
IP range	192.168.192
Subnet mask	255.255.255.0
Standard Gateway	192.168.192.254

Note
If "Settings individually per SCP/MIC711" is activated, these settings can be found under the individual Sub Control Panels.

1.5 NTP settings

As the delay and reconnaissance time is calculated using the time stamp, the times of SecuriCloud, SecuriFire and Smartphone must match. We achieve this by having the control panel automatically synchronize the time with SecuriCloud.

When using the SOP router, the forwarding of the NTP query via the IP of the router is not given. In this case, please use a public NTP service. (As an example: 1.se.pool.ntp.org / 2.se.pool.ntp.org)
In order for this address entry to work, the DNS name resolution must now be entered.

This setting can be made under "General settings".

- For the first server, we enter the router address.
- For the second server, we use the DNS server from Google.

General Settings

DNS server	
Use DNS	☑
DNS Server 1 IP address	192.168.192.254
DNS Server 2 IP address	8.8.8.8

Project / System Time

NTP- Network Time Protocol	
Use NTP	☑
NTP address	1.se.pool.ntp.org

1.6 Change password

The users and passwords for the templates had to be entered in advance. Changing usernames is optional, but for security reasons, the default passwords must be changed.

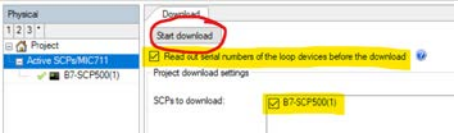
Users for Remote Access and Remote VirtualMic. The "Remote Access Password" must be changed. Optionally, the "Name" can also be adjusted. Both must match the SecuriCloud ServicePortal (Order Form) The Authorization settings under "RemoteAccess" are set so that this complies with the SES guidelines. Therefore, these may only be adjusted in special cases (Country specific regulation) In order for the VirtualMIC to function correctly, a VirtualMIC must be configured at the Control Panel where the connection to the SecuriCloud is made and the corresponding user must be enabled (this is already realized in the standard template on the first control panel).	
User for SecuriFire MobileControl The "Remote Access Password" must be changed. Optionally, the "Name" can also be adjusted. Both must match the SecuriCloud - ServicePortal.	

1.7 Set the display "Fire brigade alerted" correctly for the app

To ensure that the "Fire brigade alarmed" display is shown correctly on the app, the following must be observed:

The output which is assigned the lowest number as the transmission device activates the "Fire brigade alarmed" display in the SecuriFire MobileControl App.
In the standard template this is output 1 (Main Transmitter), this is also used for the display on the MIC.

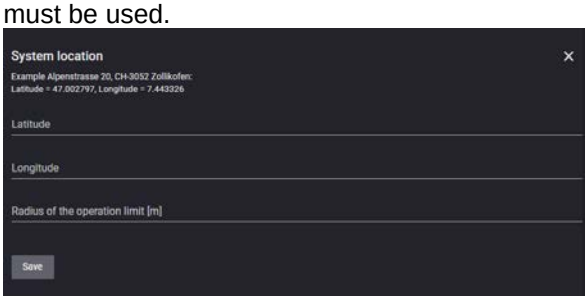
⚠ Essentiel ⚠
After creating the configuration or making any changes in the SecuriFire Studio, it is mandatory to download the project file including the serial number. The control centre from which the connection to the
SecuriCloud must be selected in the download list.
Only when this has been completed correctly can the app connect correctly.



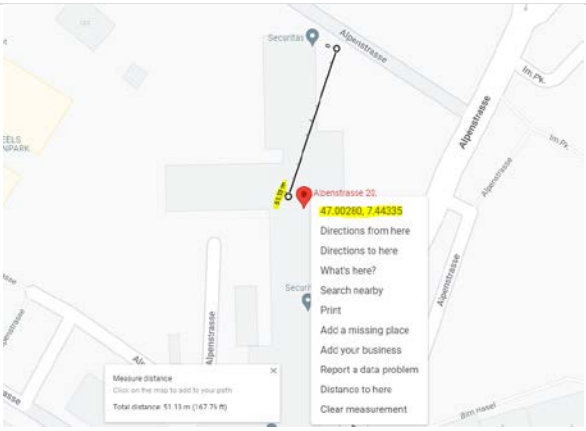
1.8 Protect customer installations

In the case of a SecuriFire system with App User, special care must be taken to ensure that recognized systems can only be operated remotely with a local authorization. The app contains a built-in GPS position check.

Operation only on site
With the coordinates of the fire alarm system, operation at the system location can be enabled. The coordinates can be read and transmitted via Google Maps using the functions "What is here?" and "Measure distance".
Hint:
To improve the accuracy of the GPS measurement inside the building, the smartphone's WLAN support must be used.



Transfer the latitude, longitude and radius coordinates to SecuriCloud (1 digit = latitude, 2 digits = longitude).



1.9 Notes

Connection costs
Costs may be incurred for connection via broadband Internet or mobile telephony.

Remote access is only possible to already configured control panels
The SecuriFire control panel must already be configured before it can be accessed via SecuriCloud.

The data throughput depends on the reception quality
Good mobile phone reception must be provided at the site to achieve fast data transmission for remote access.

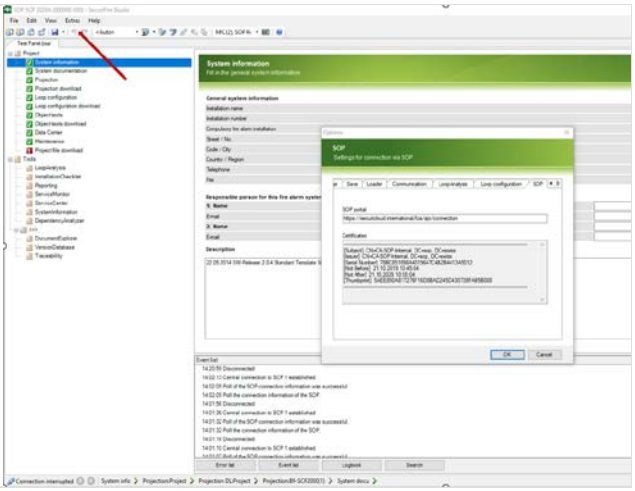
1.10 International Certificate

To be able to connect via Remote Access to a Control Panel the SOP Certificate must be valid inside the SecuriFire Studio

Check under:
Extras/Options/SOP the following entries

SOP portal link:
https://securicloud.international/fza/api/connection

Certificates:
[Subject] CN=CA-SOP-Internal, DC=sop, DC=swiss
[Issuer] CN=CA-SOP-Internal, DC=sop, DC=swiss
[Serial Number] 78BC851698A4319647C4B2B4413A5012
[Not Before] 21.10.2019 10:45:04
[Not After] 21.10.2029 10:55:04
[Thumbprint]
5AEE850A817276F16D8BAD245D430728FAB5B088



2 SecuriCloud

Establishing a connection to the control panel via SecuriCloud

2.1 General information

SecuriCloud enables remote access from the SecuriFire Studio to a SecuriFire fire alarm system without having to be on site at the system.

Note
As of the standard template, two different SOP users with different authorisations are now programmed in the remote settings. On the one hand there is a user for remote access via SecuriFire Studio and VirtualMIC, on the other hand there is a user for the connection with the SecuriFire - MobileControl App.

Warning
Critical situations may arise when using remote access.

While it is possible to read out data from the control panel at any time and without further precautions, remote control via SecuriCloud (program change, download, manipulations such as shutdowns, activations or similar on the system), the operator himself or a person instructed by him must be present on site to authorize access. This person checks the operational readiness during and after completion of the work. This person also ensures that any compensatory measures are taken.

2.2 Requirements for establishing a connection via SecuriCloud

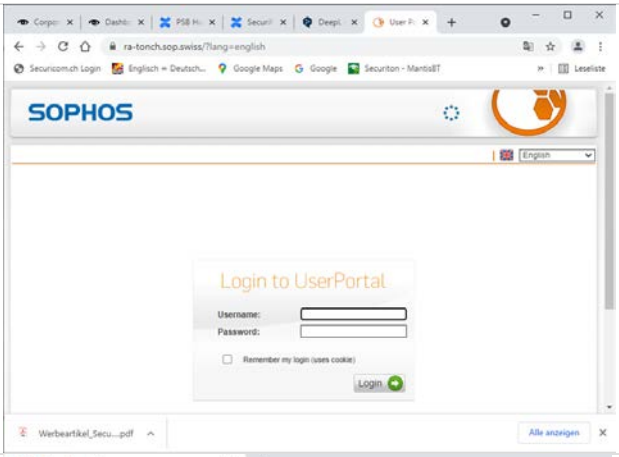
- At least one user with remote access must be configured on the SecuriFire system.
- The system must be connected to the Internet.
- The system must be registered in the SecuriCloud portal.
- The SecuriFire Studio user must be registered in the SecuriCloud portal.

2.3 Procedure

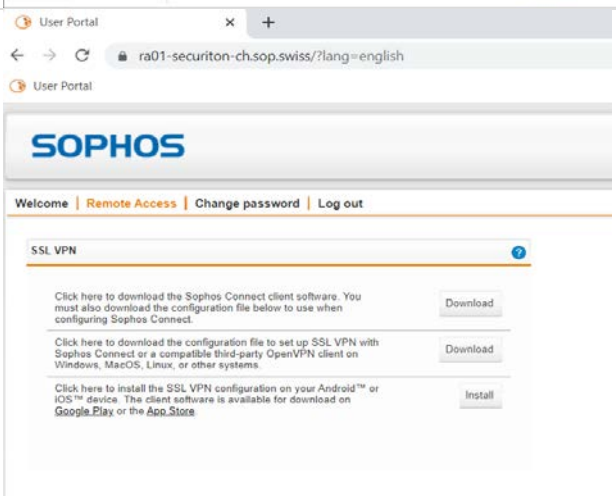
The following step-by-step instructions describe how to establish a connection via SecuriCloud to a SecuriFire control panel.

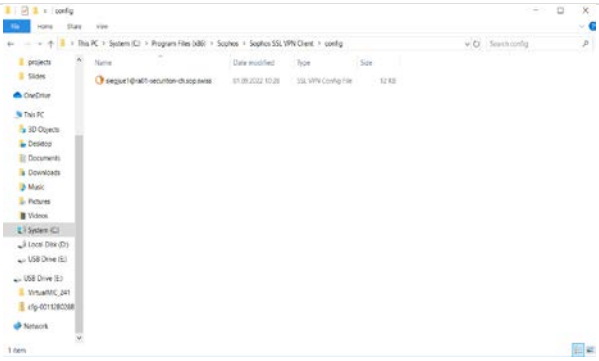
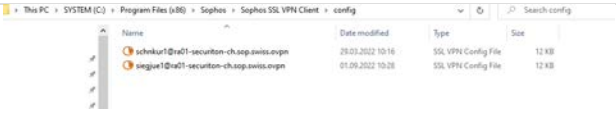
2.3.1 Set up Sophos SSL VPN Client

1. Login at https://ra01-securiton-ch.sop.swiss/
2. Change the password when logging in for the first time



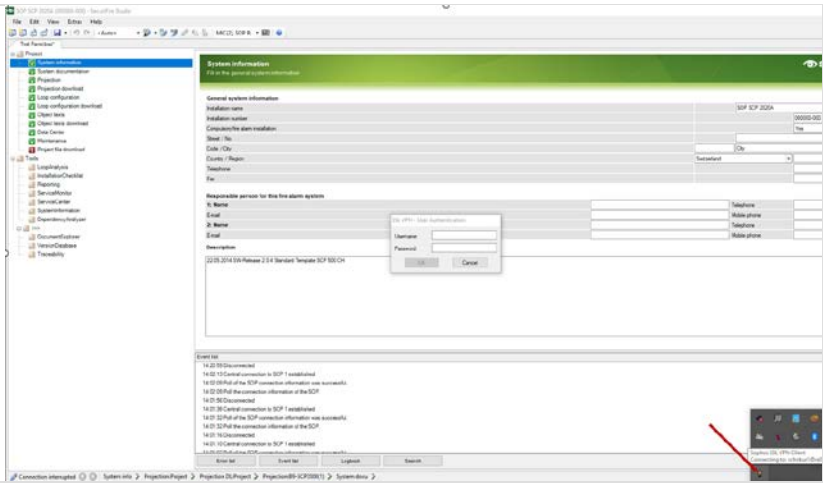
3. Download the Sophos Connect client
4. Download the Configuration file
5. Install the Sophos Connect Client



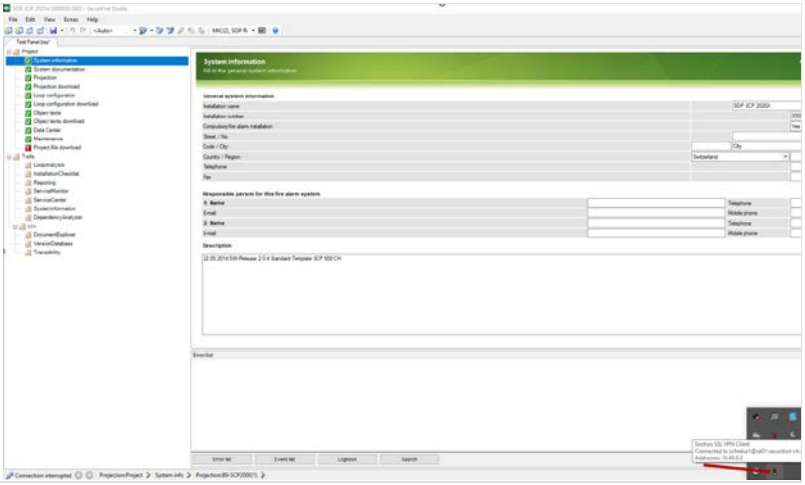
6. Copy the Configuration file into the Sophos SSL VPN Client Folder	
7. If two Sophos client User should have access on one Workstation copy both Configuration files into the Sophos SSL VPN Client Folder	

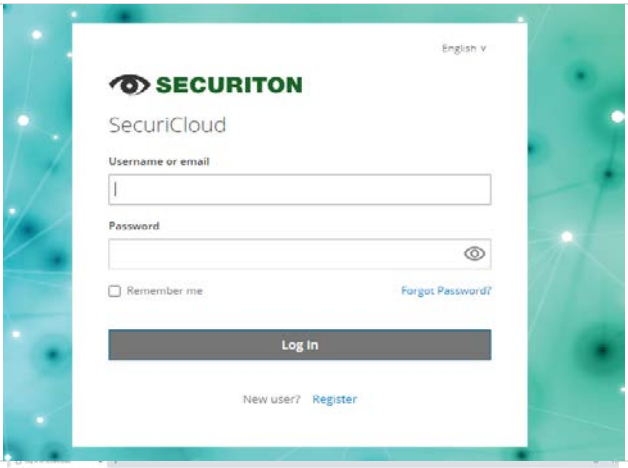
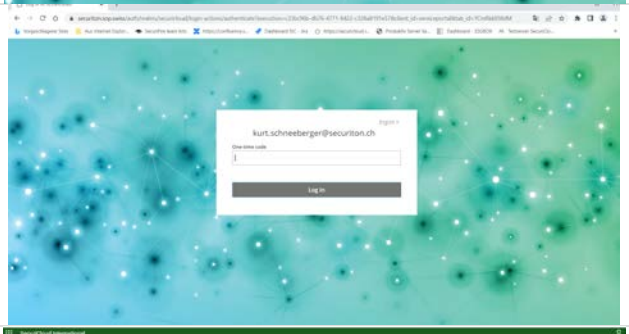
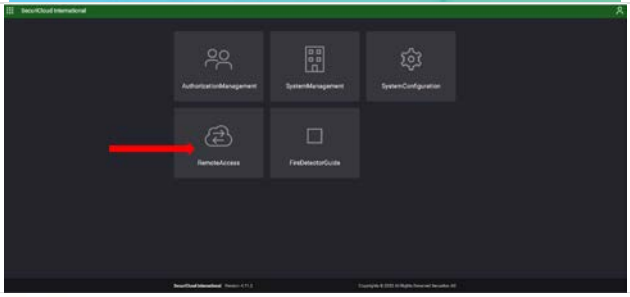
2.3.2 Connecting to SecuriCloud

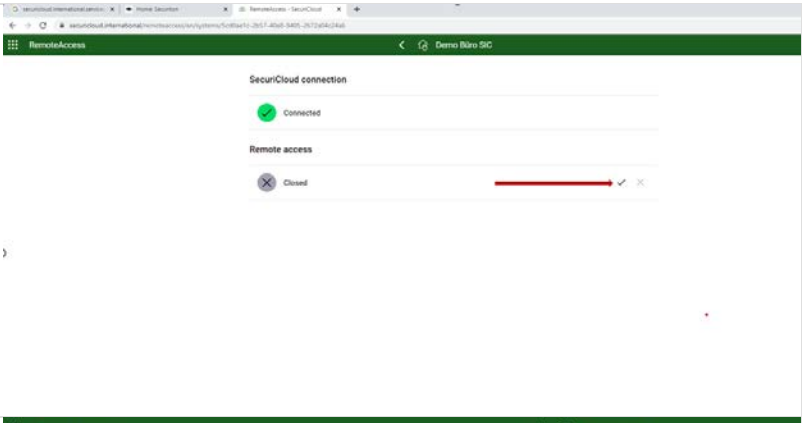
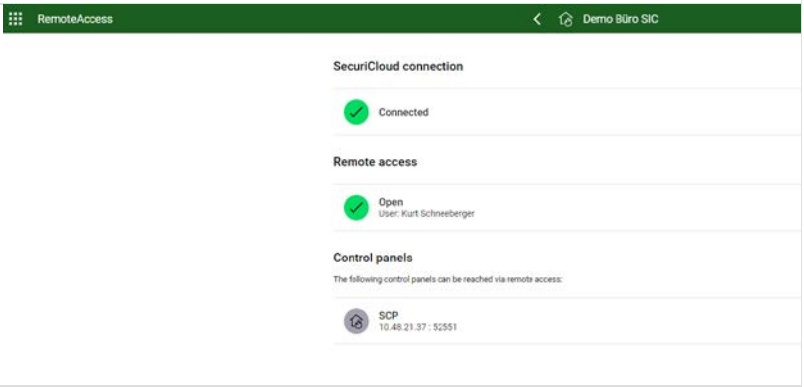
3. Establish a Sophos VPN Client Connection with your personal credentials Username and Password.



4. As soon the Traffic light symbol switches to green the VPN connection is established.



5. Enter username and password in the login form of the " SecuriCloud Portal " https://securicloud.international/serviceportal	
6. Enter one-time code from Google Authenticator.	
7. Clicking the "RemoteAccess" button.	
8. Selection of the desired system. (red arrow) The selection can be narrowed down with keywords for the object. (blue arrow)	

9. Clicking the tick on the right side activates the RemoteAccess.	
10. Remote Access activated	

Once the connection to the SecuriCloud has been established, these procedures are possible via SecuriFire Studio:

- **<Upload project file>**
  A connection is established with the SecuriFire system via SecuriCloud.
  The project file stored on the system is uploaded to the computer and opened.
  The connection to the SecuriFire system is terminated again.

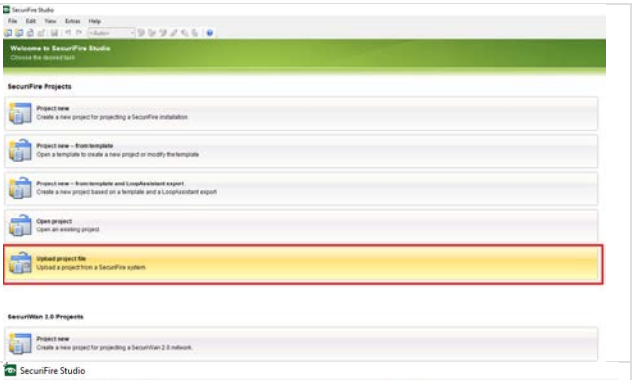
- **<Project file exists on PC>**
  The project file stored locally on the computer is opened.
  A connection is established with the SecuriFire system via SecuriCloud.

If the project file of the system in question is not known or it is uncertain whether the valid version of the project planning is really available on the computer, the first procedure is used.

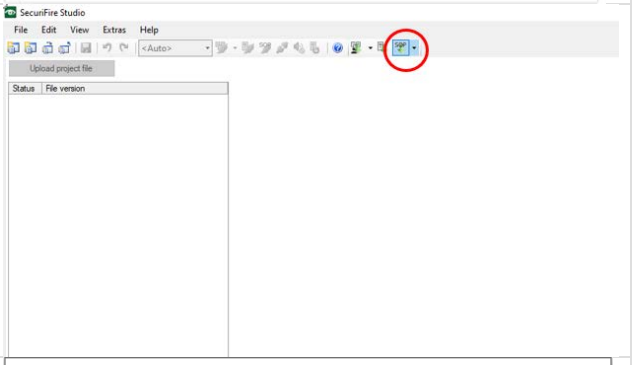
If the project file of the system in question is known and the valid version of the project planning is available on the computer, the second procedure is used.

2.3.3 Establish connection to system for <project file upload>.

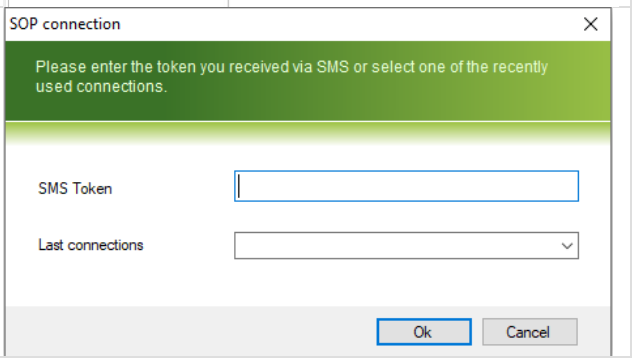
1. Launch SecuriFire Studio ≥ 2.4.1
2. Click on the "Upload project file" button.



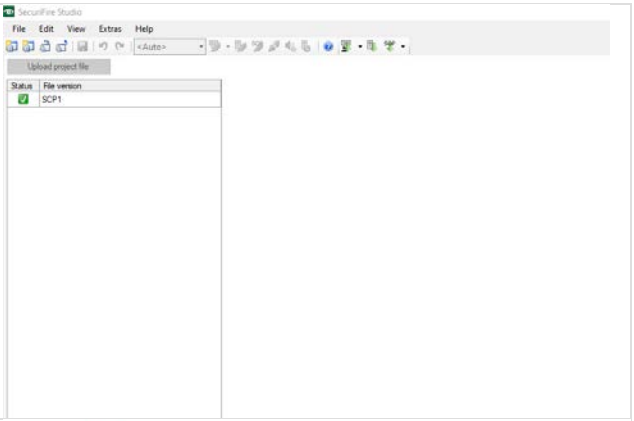
3. In the upload view, click on the icon "Search project file on SCP via SOP".



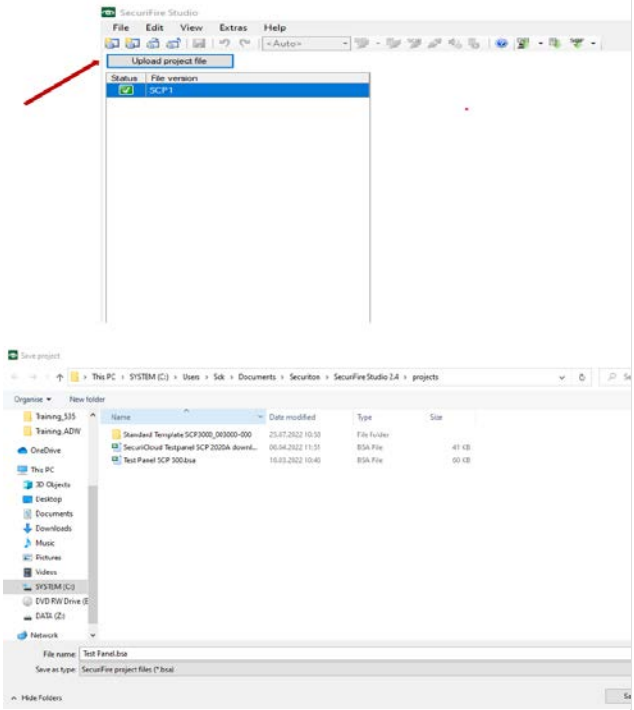
4. A dialogue for entering the SMS token appears. After entering the token, confirm with "Ok".



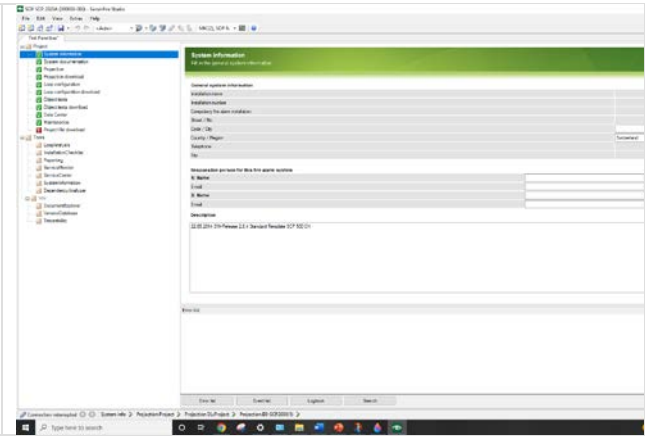
5. The connection information is queried by SecuriCloud. The network is then searched for SCPs and a connection is established to the system via SecuriCloud.



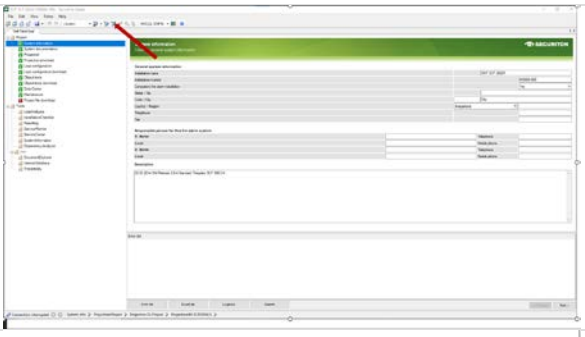
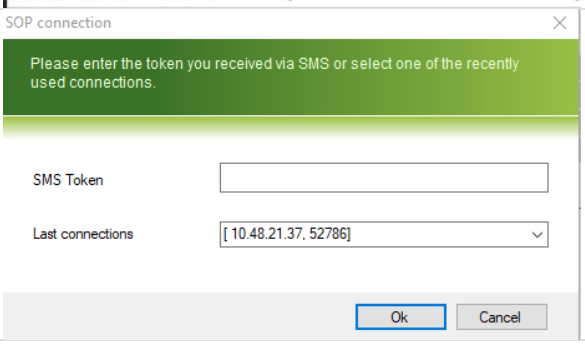
6. Afterwards, the projection can be uploaded, saved and opened as usual.

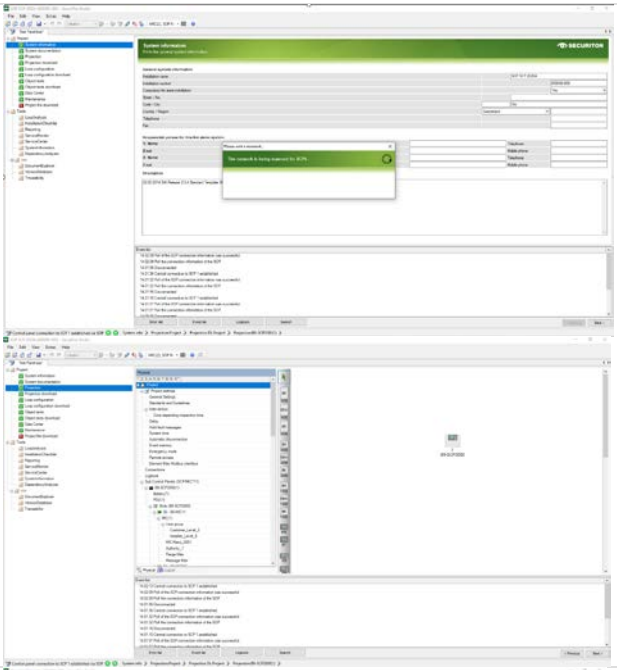
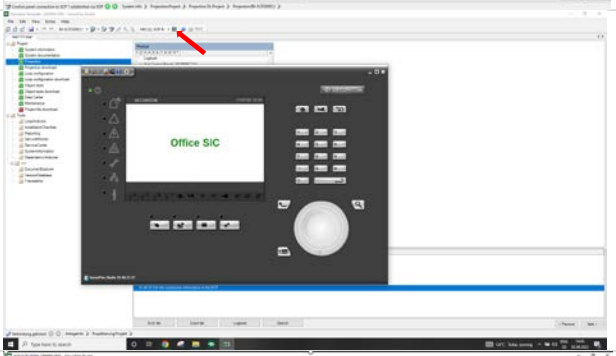
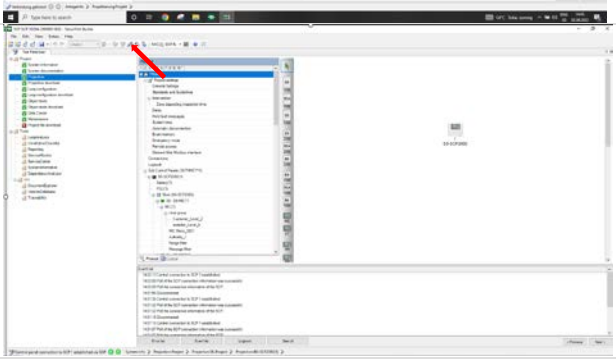


7. Now you can create a SecuriCloud connection to the system with the project planning open.
   The procedure is described in the subchapter "Establishing a connection to the system <project file available on PC>



2.3.4 Establish connection to system <project file available on PC>.

1. Start SecuriFire Studio ≥ 2.4.1 and open the project planning corresponding to the system. Click on the icon "Start Secure Online Platform Connection".	
2. A dialogue for entering the SMS token appears. After entering the token, confirm with "Ok".	

3. The connection information is queried by SecuriCloud. The network is then searched for SCPs and a connection is established to the system via SecuriCloud.	
4. The virtual MIC connection can be established just by clicking on the icon Virtual MIC. It requires the virtual MIC version ≥ 2.4.1	
5. After completion, log off to cleanly disconnect from the system: Click on the "Disconnect" icon	

2.5 SecuriCloud Token validity

Here you will find information on how access rights to a SecuriFire system via SecuriCloud are regulated with the token.

Information:

- **The token is Installation related.**
  The received token works "only" on the system selected in SecuriCloud.

- **The token is valid for 10 minutes.**
  Once the token has been sent, the SecuriFire must be dialled into within 10 minutes.

- **The token is valid for SecuriFire Studio and VirtualMIC.**
  The same token can be used for both programs, but the switchover must be made within 10 minutes.
  Simultaneous connection of SecuriFire Studio and VirtualMIC is not possible via remote access.

- **Disconnection after 1h inactivity.**
  If a connection is idle for one hour, the connection will be closed automatically. (Caution: both SecuriFire Studio and VirtualMIC generate data continuously).

- **One connection per system.**
  Only one connection can be established per system. If a technician has already established a connection to the central unit, this unit is blocked for others.
  If a colleague has forgotten to close the remote access on SecuriCloud, it can be closed. If there is no active connection (notebook SecuriFire)

- **Re-establish connection to the control center.**
  If a connection is re-established after the tool has been disconnected, this is only possible within the 10 minutes. A new token must then be requested.

2.6 Notes

Note
Connection costs
Costs may be incurred for the connection via broadband Internet or mobile phone.

Note
Remote access is only possible to control panels that have already been configured.
The SecuriFire control panel must already be configured before it can be accessed via SecuriCloud.

Note
The data throughput depends on the reception quality.
Ensure good mobile phone reception at the site to achieve fast data transmission for remote access.

2.7 References

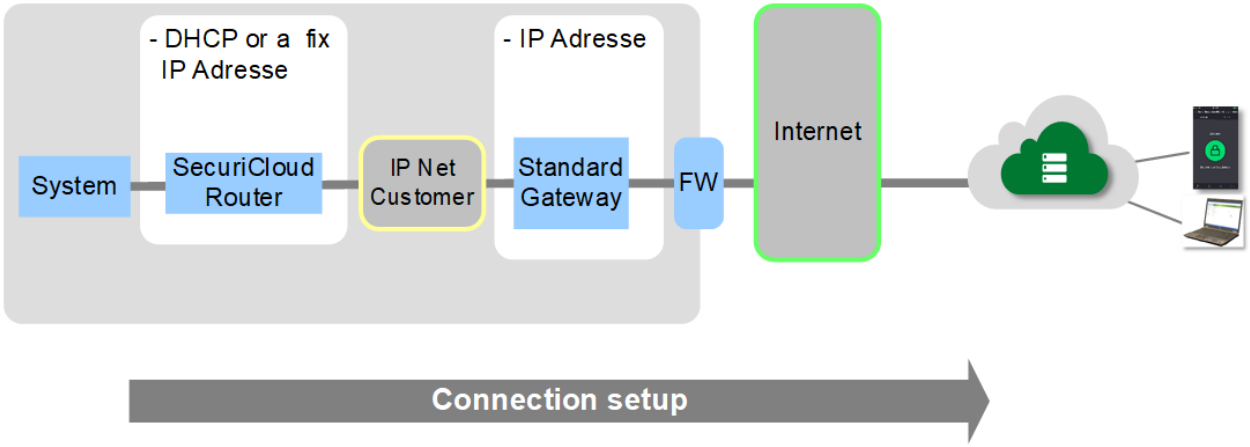
- SecuriFire Studio Manual T811093

3 IT-Connection Settings

3.1 General Information

In order for the device to be able to communicate with SecuriCloud, it is necessary to configure the IT environment accordingly. The following information must be recorded for this purpose.

3.2 Installation



3.3 Connection

- An Internet router (xDSL, Cable, etc.) is set up and operational at the SecuriCloud router location.
- The router or the house installation of the LAN has a free connection for the Ethernet cable of the SecuriCloud router. Securiton recommends that the device is connected as close as possible to the Internet router.
- The Ethernet port is designed for a data rate of 10BaseT or 100BaseT (autonegotiation)
- An Ethernet cable RJ45 (min. Cat. 5) has been laid from the router to the SecuriCloud router location and is ready for connection of the device. The maximum cable length is 100m.
- An Ethernet cable RJ45 (min. Cat. 5) has been installed from the router to the The Internet router is configured in such a way that the connection to the Internet is permanently maintained and that it automatically re-establishes the connection to the provider after an interruption.

3.4 IP adress

The device requires an internal IP address with a corresponding SubNet mask as well as the IP address of the standard gateway that is valid within the customer environment. These details can be obtained automatically by the SecuriCloud router via the DHCP service or must be entered manually:

The following information must be passed on to Securiton AG:

☐ Obtain IP addresses automatically (DHCP)

☐ Enter IP addresses manually: IP Address . . .

SubNet Mask . . .

IP Address Standard GW . . .

3.5 Ports

The device communicates with the SecuriCloud via specific IP ports. These must be enabled on any installed firewalls (FW) or proxies for communication with the outside world.

Function	Protocol	Port	Connection enabled
OpenVPN	TCP	443	☐ Yes
IPsec	UDP / ESP	500	☐ Yes
	UDP / ESP	4500	☐ Yes
	TCP (IKE)	10000	☐ Yes

3.6 IP designation addresses

The IP target addresses must be released in the customer network depending on the configuration of the customer environment. Since the destination addresses are different, they can be requested if necessary.

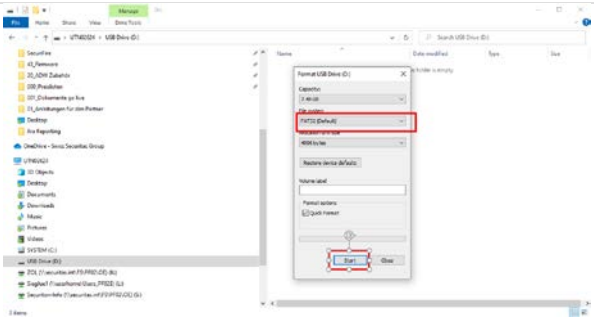
ra-tonch.sop.swiss 185.161.103.12

ra01-securiton-ch.sop.swiss 185.161.103.103

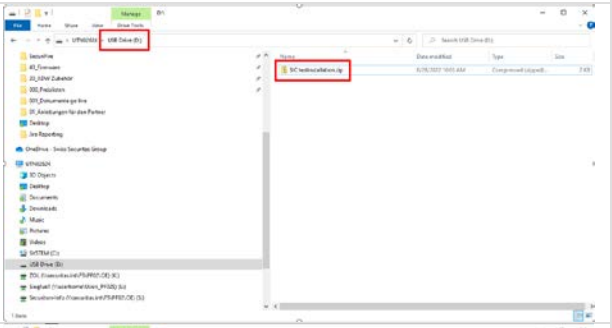
4 SecuriCloud Router

4.1 Memory-Bootstick

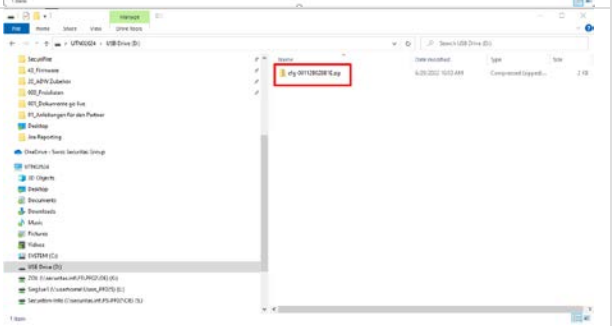
1. Format the memory stick (FAT32): Right click on the corresponding drive -> format -> select FAT32 -> Click start



2. Copy the ZIP file received from Securiton (must contain a .cfg file and the autorun key) onto the stick.



3. Rename the ZIP-file as follows:
   - Cfg-SERIALNUMBER-ROUTER.zip



   - The serialnumber can be found on the back of the SecuriCloud-router.
   - Example: cfg-00112B028B1E.zip

4.2 Factory-Reset

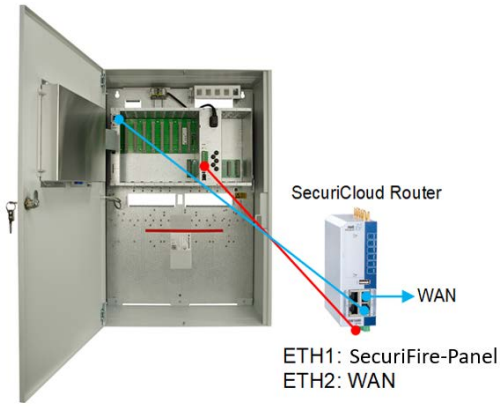
Instructions for uninstalling the configuration on the SecuriCloud router. 4. Press the reset button on the SecuriCloud router for at least 10 seconds.	
5. Factory reset is triggered. All LEDs light up briefly.	
6. The SecuriCloud router restarts (LED STAT) flashes.	
7. The SecuriCloud router is reset and is back in the factory default state. (STAT LED lights up constantly)	

4.3 Installation

8. Connect the SecuriCloud router to the power supply and wait until the STATUS LED is constantly green. 230V AC with power supply unit directly with 12V DC / 24V DC.	
9. Insert Memory-Bootstick stick into the router.	
10. Wait until configuration is installed: All LEDs flash green → Configuration is installed.	
11. Status LED is steady green again → Configuration has been installed. Bootstick can be removed and data on the stick can be deleted.	

12. The router can now be installed in the SecuriFire-Panel and connected to the WAN.

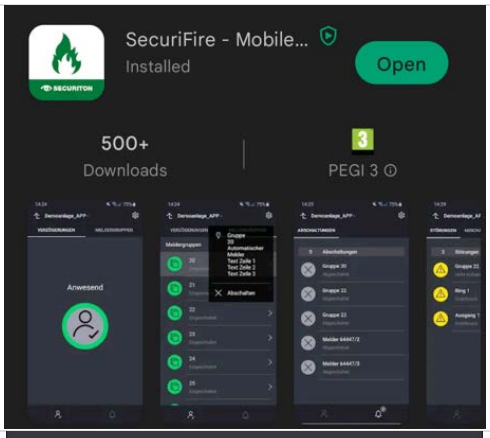
If a NET card is inserted, the NET card must be plugged in!



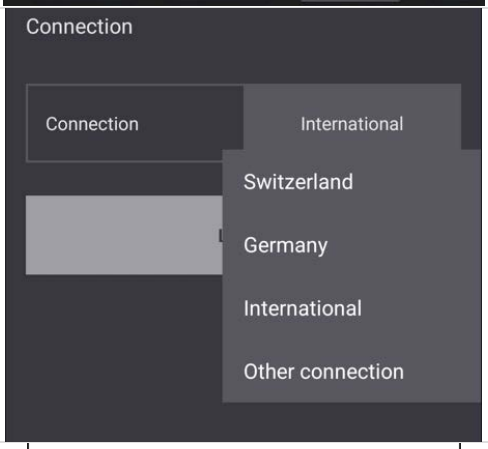
5 Mobile-Control-App

5.1 Android via Google Playstore

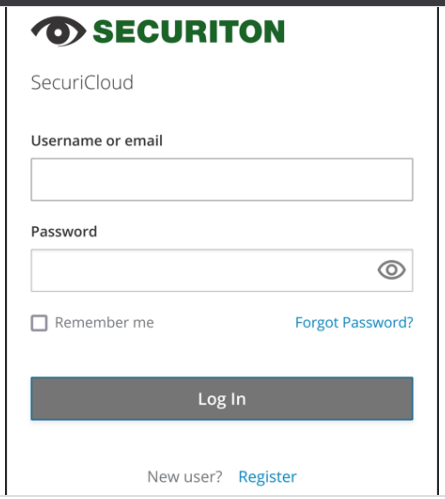
1. Download the SecuriFire-App from the Playstore and open the App.



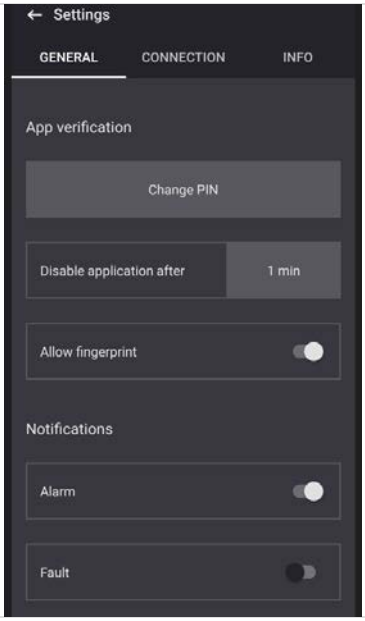
2. When selecting "Connection", make sure that "International" is selected.



3. You will be automatically redirected to the registration page.
Enter your username/e-mail and password.

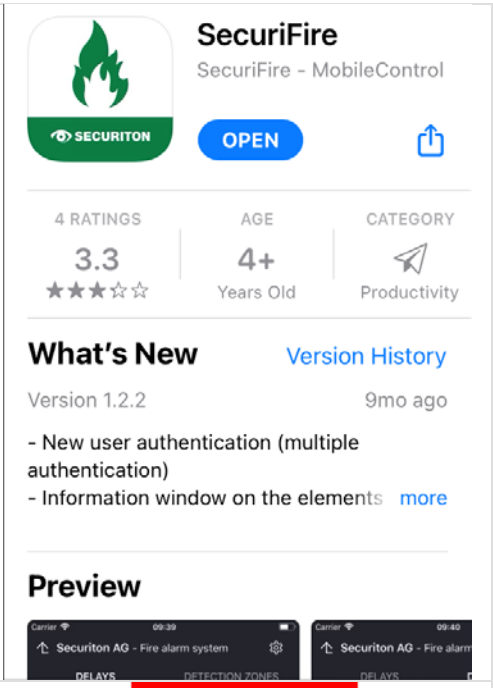


4. You are now connected via MobileControl.
   Under Settings/General you can make the following settings:
   - Change the PIN to open the App
   - Set disable time
   - Allow login via fingerprint
   - Define which notifications you want to receive



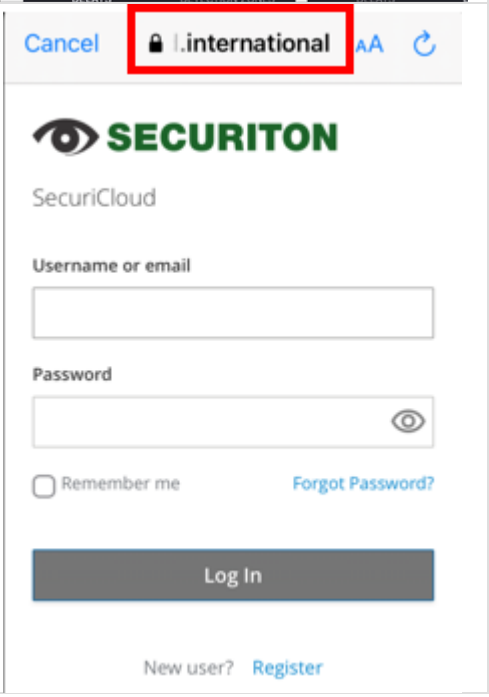
5.2 iPhone via App-Store

1. Download the SecuriFire-App from the App-store and open the App.



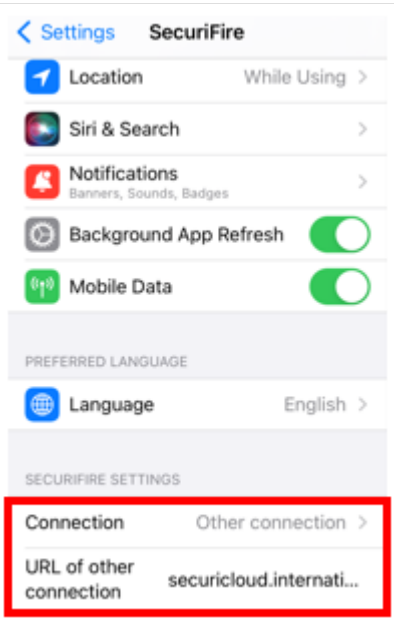
2. Log in with username/e-mail and password. Make sure that the connection is established to “securicloud.international”.

   If this is not the case, go to point 3.

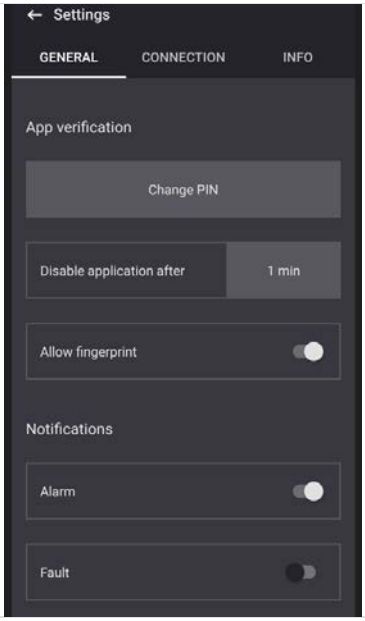


This step is only necessary if the connection is not established to "securicloud.international".

3. Go to Settings -> SecuriFire and make the following adjustments:
   Connection: Other connection
   URL of other connection: securicloud.international



4. You are now connected via MobileControl.
   Under Settings/General you can make the following settings:
   - Change the PIN to open the App
   - Set disable time
   - Allow login via fingerprint
   - Define which notifications you want to receive



6 Checklist

“Step by Step”-checklist to your SecuiCloud-solution:

ordered	Order item	received
☐ Yes	Order the SecuriCloud-router at Securiton Sales International.	☐ Yes
☐ Yes	The order-form *“SecuriCloud_SIC_OF_220721”* is filled out and sent to Securiton Sales International.	☐ Yes
☐ Yes	The VPN-program “SOPHOS CLIENT” sent from Securiton including the login data is installed and running.	☐ Yes
☐ Yes	Install the Google-Authenticator.	☐ Yes
☐ Yes	For MobileControl-users: Download the “SecuriFire”-App from the Appstore or Google-Play.	☐ Yes
☐ Yes	Register yourself on: https://securicloud.international/	☐ Yes
☐ Yes	Upgrade all Control Panels and MIC 711 to Release 2.3.0 or newer.	☐ Yes
☐ Yes	The changes in the SecuriFire-project are made according this document.	☐ Yes
☐ Yes	The router-file is loaded to the router and the router is ready to use.	☐ Yes
☐ Yes	Internet-connection for the router is up running and the VPN-connection is stable.	☐ Yes