Cyber Identity Security

Installation instructions

swisscom

August 2021
40003630 EN 8.2021

Thank you

for choosing our digital identity protection tool.

Cyber Identity Security protects against data theft and safeguards your digital identity against cyber attacks.

The product monitors personal e-mail addresses in the network around the clock. If there is any misuse, all other linked data, such as user names, passwords or credit card numbers, are displayed so they can be quickly changed or blocked.

Up to 10 e-mail addresses can be stored. You are immediately alerted if the stored data is affected by data theft and automatically receive the request to change the password or block the credit card.

With the help of the password manager, all passwords can be stored in a secure location, so you only need to remember one master password.

Scope of service

- Protects against data theft and safeguards digital identity against cyber attacks.
- Immediate warning in the event of misuse of e-mails and linked data, such as passwords or credit card numbers
- Instructions on what to do to prevent damage
- Password manager – your secure storage place for all passwords and credit card numbers

Supported platforms

- Windows 7 (SP1), Windows 8.1, Windows 10
- macOS X 10.14 (Mojave) or later
- Android 6.0 or later
- iOS 13.0 or later

Please make sure that all devices on which you wish to use Cyber Identity Security fulfil the system requirements.

swisscom

Installation process

1. Installing Cyber Identity Security on a device

2. Creating master password and recovery code

3. Entering e-mail addresses

4. Entering passwords and credit card numbers

5. Installing Cyber Identity Security on additional devices

6. Synchronising devices

7. Deinstalling Cyber Identity Security

swisscom

1. Installing Cyber Identity Security on a device

To install Cyber Identity Security, log into the device as administrator and proceed as described below.

Install app – step by step:

1. After placing the order, you will receive a welcome e-mail from us
2. Click the blue 'Download' button in the e-mail
3. Follow the directions and install the app on your device

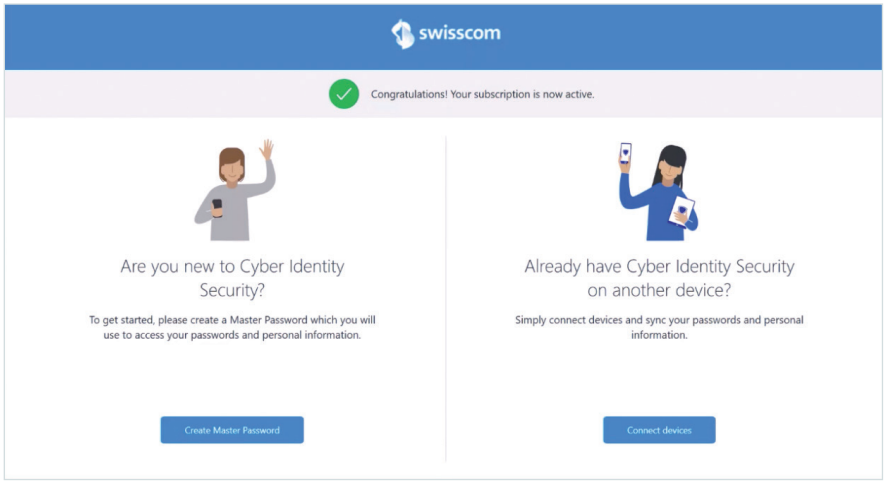
If you additionally ordered our Internet Security anti-virus protection, you must also install this separate app.

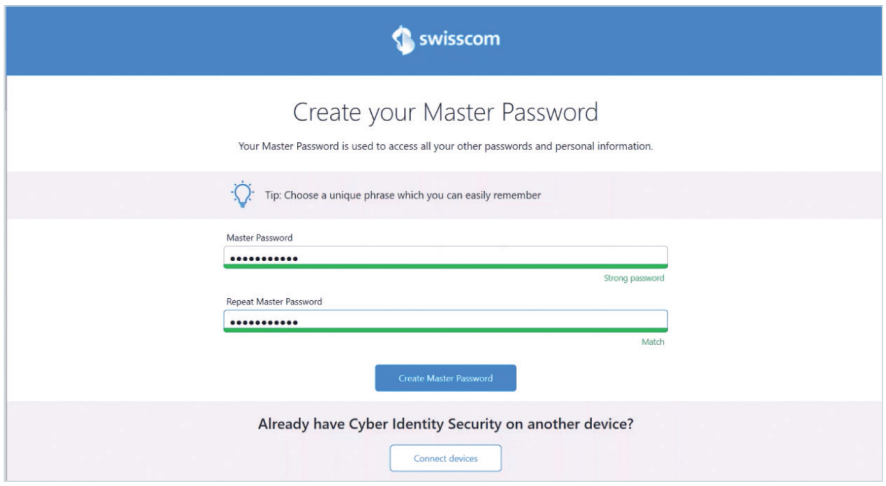
Please read the Internet Security installation instructions, which can be downloaded at swisscom.ch/securitypackage.

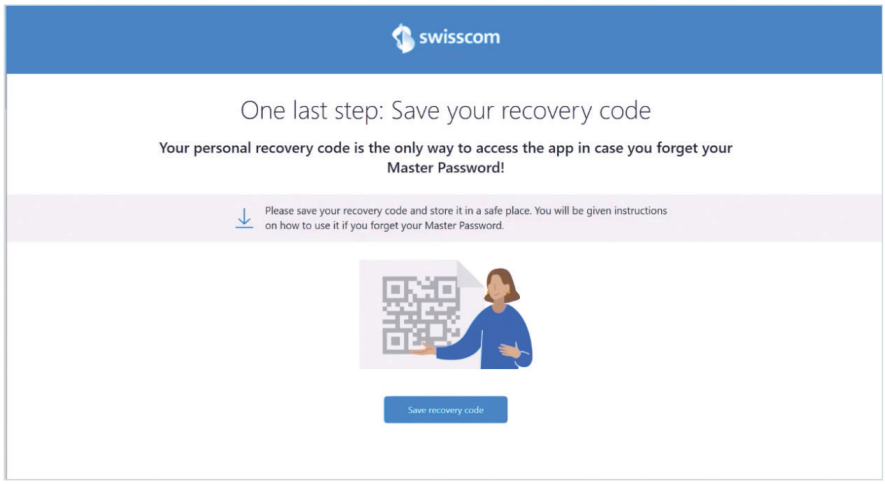
2. Creating master password and recovery code

In the future, you will only need to remember the master password you set. After installation, you are also asked if a recovery code should be generated. We urgently recommend that you generate one and save it on your device or print it out.

You can log in with this QR code if you forget the master password. We never store the master password or master encryption key. This data is encrypted on your device and we have no way of decrypting it.





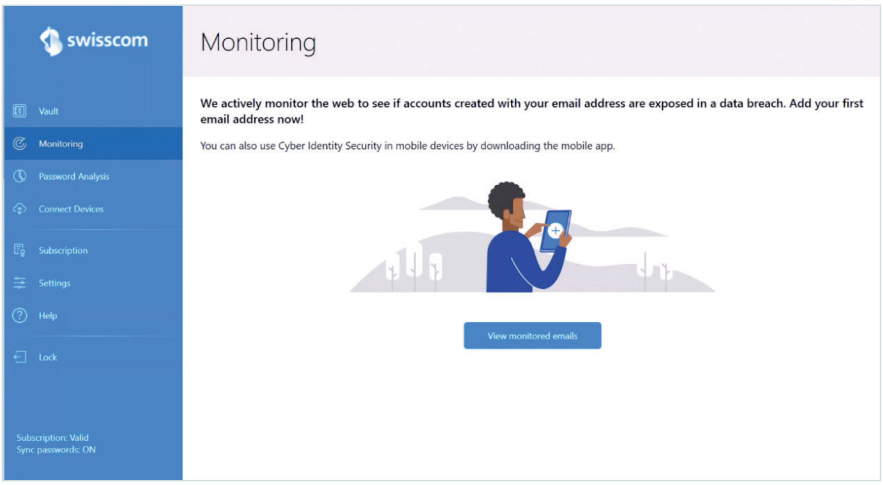


Please note that if you cancel your licences, you no longer have access to your stored data. It is therefore essential that you back up or note this data in advance.

3. Entering e-mail addresses

After the installation, you have the option of entering up to ten e-mail addresses. The e-mail addresses only have to be entered once even if you are using several devices.

1. Enter your first e-mail address directly into the app under 'Monitoring'.
2. After entering this information, you will, for security reasons, receive an e-mail to confirm the e-mail address entered (noreply@f-secure.com).
3. Your e-mail address will only be monitored after the confirmation (F-Secure web monitoring)
4. In the event of data misuse, you will be alerted in the app and can then proceed as advised.
5. Repeat steps 1–3 to enter additional e-mail addresses.



Please note:
The e-mail addresses will only be monitored around the clock once they have been entered and confirmed.

4. Entering passwords and credit card numbers

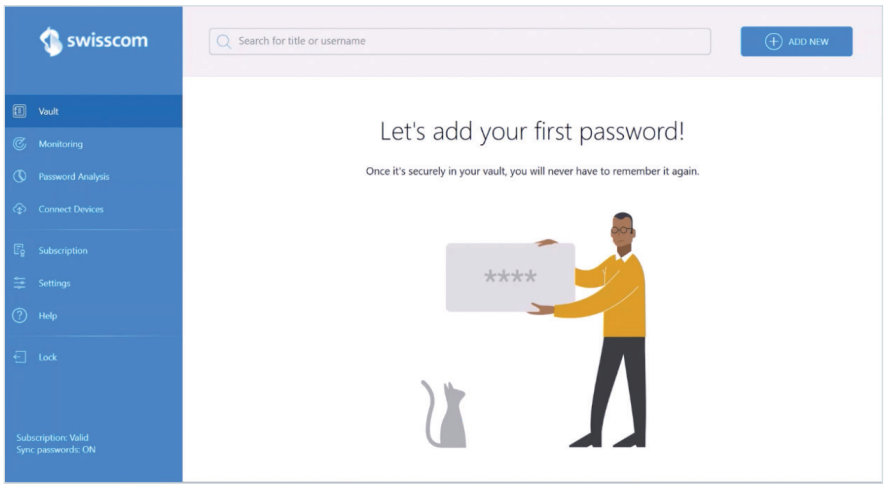
The password manager supports you with generating secure passwords or evaluating existing ones.

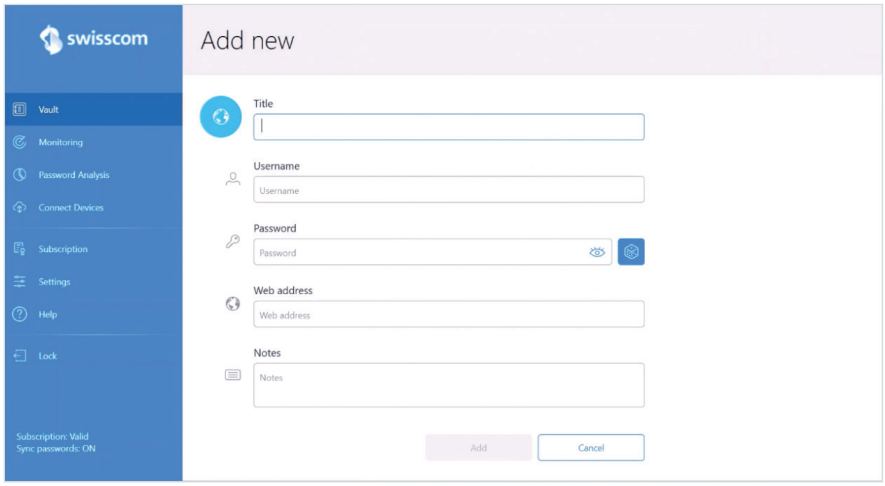
Protecting your passwords or credit card numbers

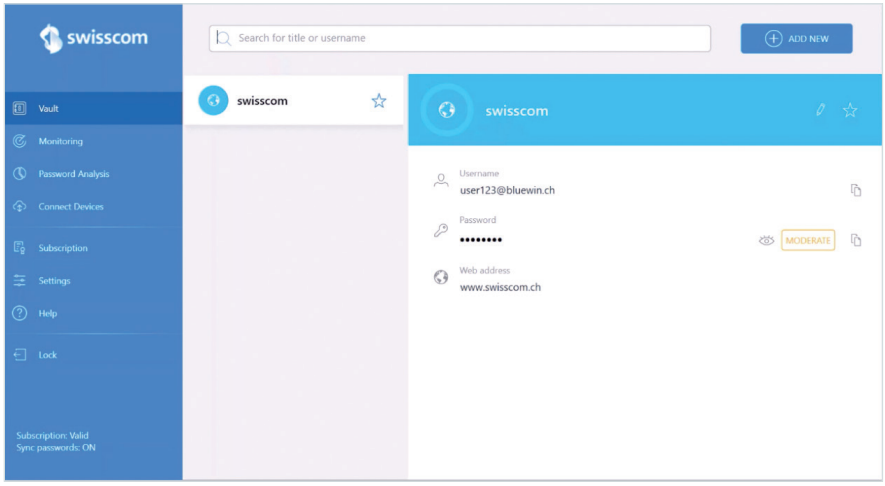
Passwords, login data and credit card numbers are stored centrally in the vault.

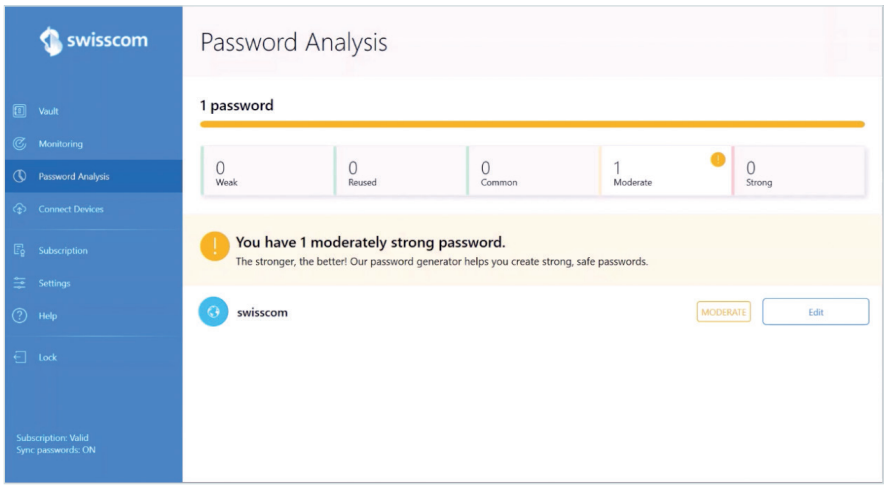
The synchronisation function means they can be retrieved on all devices with a master password. The password analysis enables you to check the passwords you use.

1. Enter your first password or your first credit card number in the vault and save it.
2. Repeat this procedure for additional passwords or credit card numbers. You can enter new passwords or credit card numbers at any time.
3. To synchronise the passwords or credit card numbers with additional devices, send the link by SMS/e-mail and follow the instructions to install the app.
4. Use your previously generated master password to log in.
   You can now synchronise the devices in the app (see point 6).


swisscom
Search for title or username
ADD NEW
Vault
Monitoring
Password Analysis
Connect Devices
Subscription
Settings
Help
Lock
Subscription: Valid
Sync passwords: ON
Let's add your first password!
Once it's securely in your vault, you will never have to remember it again.
****


swisscom
Add new
Vault
Monitoring
Password Analysis
Connect Devices
Subscription
Settings
Help
Lock
Subscription: Valid
Sync passwords: ON
Title
Username
Password
Web address
Notes
Add
Cancel


swisscom
Search for title or username
ADD NEW
Vault
Monitoring
Password Analysis
Connect Devices
Subscription
Settings
Help
Lock
Subscription: Valid
Sync passwords: ON
swisscom
swisscom
Username
user123@bluewin.ch
Password
MODERATE
Web address
www.swisscom.ch



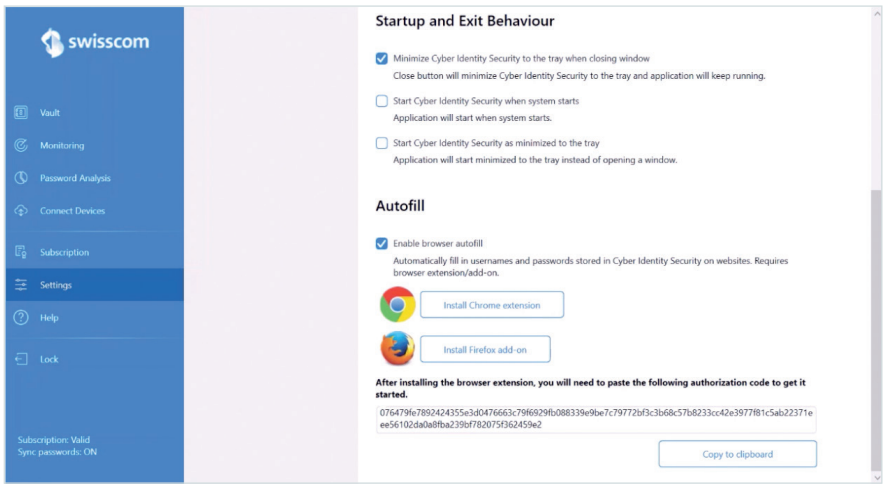
Share password manager with an additional user

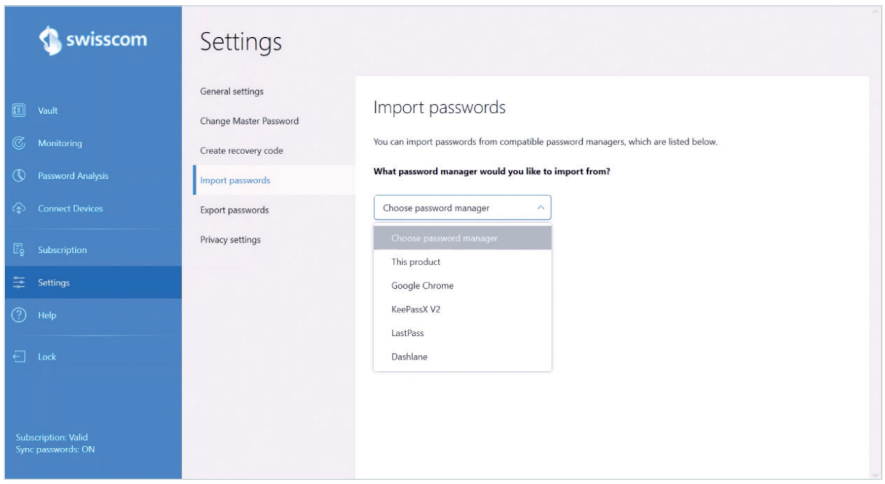
You can also share the password function with an additional user. To do this, send a licence to the relevant e-mail address.

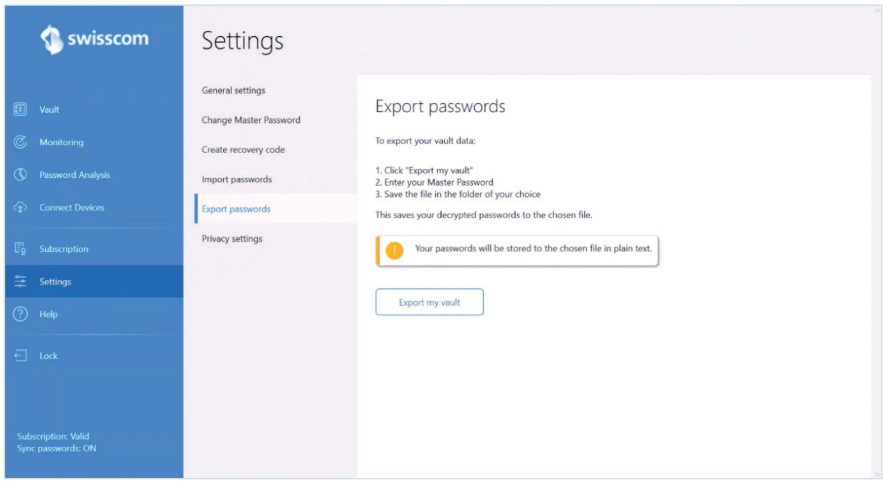
To use the password manager independently, a separate master password has to be generated on the additional device.
This now applies only for this device.
You cannot see the passwords of other users.

Already using a free password manager in your browser?

Under 'Settings', you will find specific instructions on how to import passwords etc.




swisscom
Settings
Vault
Monitoring
Password Analysis
Connect Devices
Subscription
Settings
Help
Lock
Subscription: Valid
Sync passwords: ON
General settings
Change Master Password
Create recovery code
Import passwords
Export passwords
Privacy settings
Import passwords
You can import passwords from compatible password managers, which are listed below.
What password manager would you like to import from?
Choose password manager
Choose password manager
This product
Google Chrome
KeePassX V2
LastPass
Dashlane

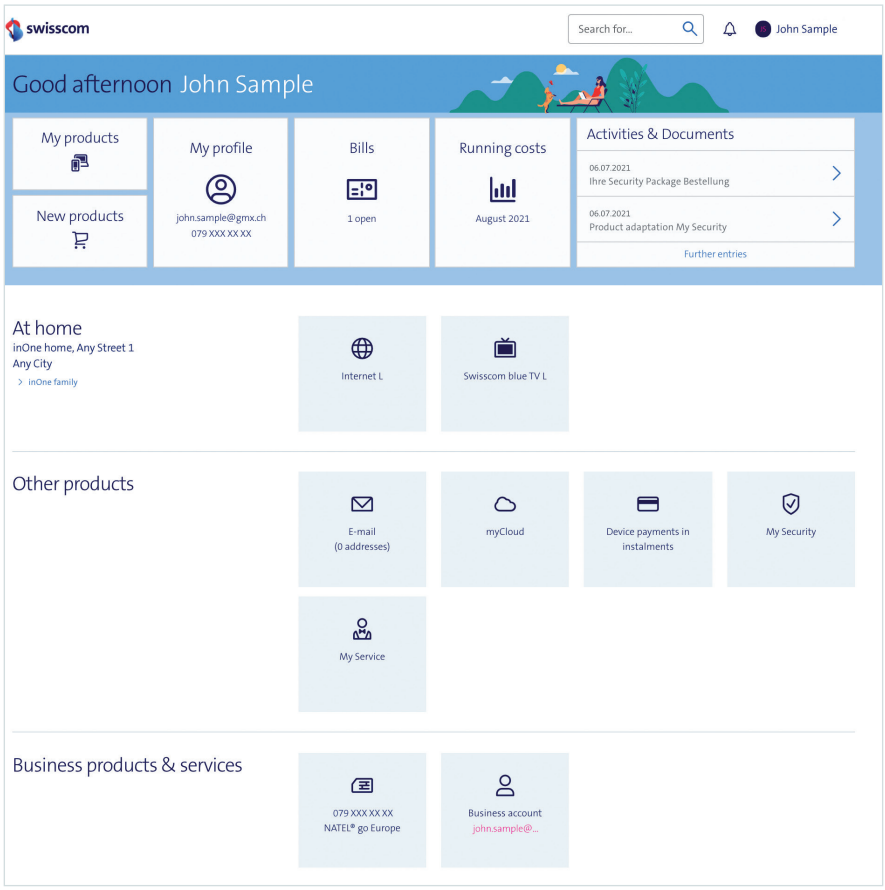

swisscom
Settings
Vault
Monitoring
Password Analysis
Connect Devices
Subscription
Settings
Help
Lock
Subscription: Valid
Sync passwords: ON
General settings
Change Master Password
Create recovery code
Import passwords
Export passwords
Privacy settings
Export passwords
To export your vault data:
1. Click "Export my vault"
2. Enter your Master Password
3. Save the file in the folder of your choice
This saves your decrypted passwords to the chosen file.
Your passwords will be stored to the chosen file in plain text.
Export my vault

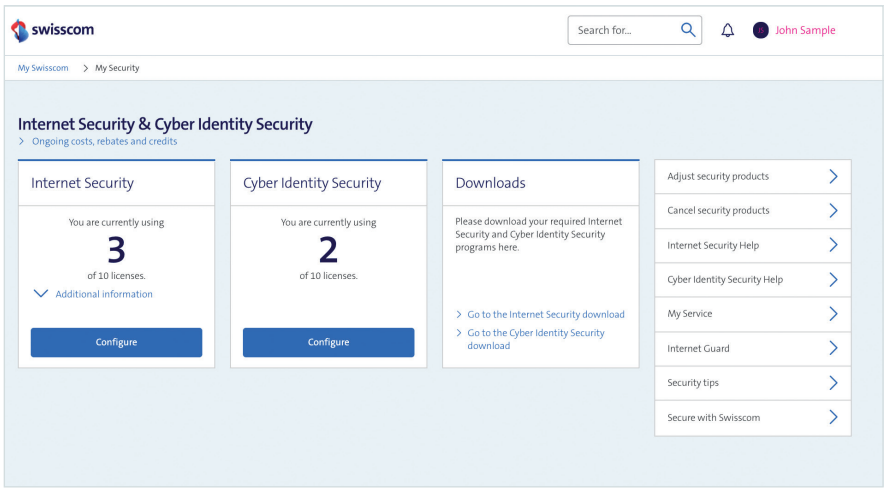
5. Installing Cyber Identity Security on additional devices

1. Use your Swisscom login in My Swisscom to log into the device on which you would like to install Cyber Identity Security (unless you are already logged in).

   Select 'My Security' and then, in the 'Downloads', select 'Go to Cyber Identity Security Download'.

   You can install Cyber Identity Security on your devices from the Control Center (from our supplier F-Secure).





2. Check if the right platform (Windows/Mac or Android/iOS) was recognised for your device. Correct this if required.

3. Select 'Download' and follow the instructions of the installation assistant. Please note the following supplementary information, depending on your device type:

a. Windows Computer (PC)/Mac

Open the downloaded installation file and follow the instructions of the installation assistant.

b. Android

After naming the device, you are linked to the Play Store.
A relevant account in the Play Store is a prerequisite for installing the application.

c. iOS

After naming the device, you are linked to the App Store.
A relevant account in the App Store is a pre-requisite for installing the application.

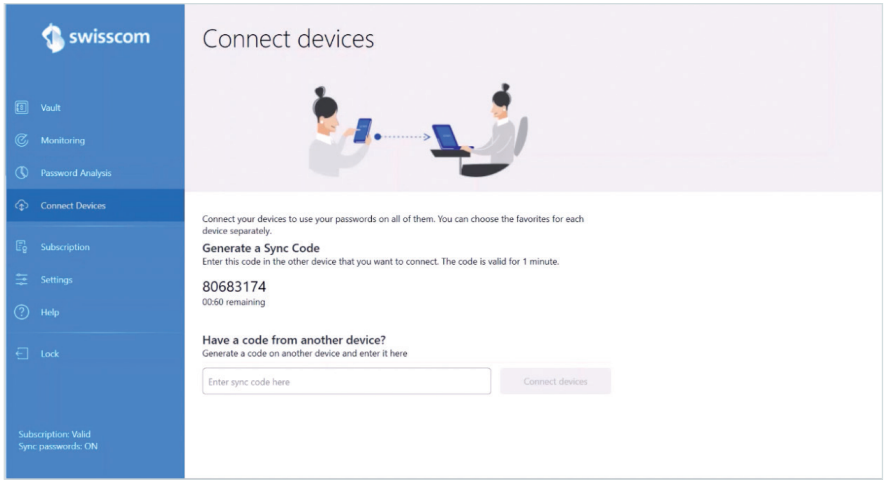
After installation and activation, Cyber Identity Security is automatically updated via the Internet. This completes the installation.

6. Synchronising devices

If you use several devices, you have to repeat the installation procedure each time.

The devices are then synchronised with each other. You do not have to enter the passwords again and can simply log into your accounts using an additional device.

Select 'Connect Devices' and follow the instructions.



7. Deinstalling Cyber Identity Security

Proceed as follows to remove Cyber Identity Security:

Windows 7 and 8.1

1. Windows 7: Access the 'Start' menu on your computer
2. Windows 8.1: Right click on an empty field in the tile view. Then select 'All apps'
3. Access the 'Control Panel'
4. Access 'Programs and Functions'
5. Select the entry for the respective program in the 'Deinstall or change program' window.
6. Access the 'Deinstall' function
7. Follow the instructions for the deinstallation program

Windows 10

1. Windows 10: Access the 'Start' menu on your computer
2. Access 'Settings'
3. Select 'Apps'
4. Execute program and then select 'Deinstall'
5. Follow the instructions for the deinstallation program

macOS X

1. Search for storage location of the program that you want to deinstall in the 'Finder' (e.g. under 'Locations'→'Programs').

2. a. Recommended: If the program comes with a deinstallation assistant, always use this to deinstall the program and follow the deinstallation assistant.

   b. If the program has no deinstallation assistant, drag the program you want to deinstall and the associated files and folders into the recycle bin. Store files temporarily in the recycle bin until you are certain that your Mac is still working without any problems.

Android

Open Google Play Store app, Tap the three-line menu and select 'My apps and games'.

Tap the Cyber Identity Security app. Tap on 'Deinstall'.

iOS

Place your finger on the Cyber Identity Security app for fast-action menu opening.

Tap on 'Remove app' and then on 'Delete app'.