SAASPASS

Start Guide For Personal Users

TEN QUICK STEPS FOR GETTING STARTED

SAASPASS is a powerful identity product used by both companies and personal users. There are many features included within the product that can be used to enhance your security and convenience at work as well as at home.

1. Download and install *SAASPASS* from your mobile app store (Apple Store, Google Play Store, etc.) or from https://saaspass.com/downloads.html.
2. Open the app and create a PIN.
3. Click GET STARTED and read the short in-app tutorial.
4. Add a recovery number by either:
   a) clicking on the red alert message at the top of the screen,
   b) selecting MOBILE NUMBER in the menu, or
   c) from the settings, which is the gear icon at the top right side of your screen, choose recovery.
5. Enter your mobile number and click ADD.
6. Once received by SMS text message, add the verification code and click CONFIRM.
7. Now provide your *SAASPASS* ID to your company admin to complete the onboarding process. Your admin may either ask you for your *SAASPASS* ID (listed at the top of the menu in your app) or email you a verification link prompting you to click on it and thus confirm your *SAASPASS* ID.
8. A section called COMPANY APPLICATIONS should appear in your *SAASPASS* app after you are on-boarded by your admin, and you will now have access to any application listed there.
9. Usually, your admin will install the Desktop Client onto your computer, after which a tiny *SAASPASS* orca logo will appear at the top of your screen. This is your SINGLE SIGN-ON CONSOLE in which all of your applications are listed and can be accessed with a single click. Click on it, scan the barcode to login, then enter your computer's password. This Desktop Client can be installed by any of the following methods:
   a) Your admin distributes a push package to your computer through Active Directory.
   b) Your admin installs the client directly onto your computer (for computers without Active Directory) and then manually enters a key into your Single Sign-on Console.
   c) A third option, however, if your machine is a personal computer and you wish to add and manage computer protection yourself, is for you to download and install the desktop client from here: https://saaspass.com/downloads.html.
10. Download the Browser Extension at https://saaspass.com/downloads.html. Once installed, your browser will be able to autofill usernames, passwords, and authenticator codes for any of your company Shared Accounts as well as any of your personal apps and websites. Most browsers are fully-supported, but the extension works best with Google Chrome.

THE BASICS

WHAT IS *SAASPASS*?

SAASPASS is a security set of different products all bundled in one Identity and Access Management Platform. Once installed, your computer and any applications paired with your *SAASPASS* ID will be protected with multi-factor authentication. The SAASPASS app on your mobile device will be the “key” used to “unlock” your computer and your applications in a passwordless manner, and you will manage your account from the mobile app, from the Single Sign-on Console on your desktop, and also through the Web Portal or the *SAASPASS* browser extension.

SAASPASS ID

When you get started, a new unique *SAASPASS* ID or in short SPID is generated for you. This 9-digit number works as your unique identification number to which all your user accounts[1] are linked. Your smartphone, tablet, work computer and personal laptop can all be paired to your unique *SAASPASS* ID, and all of these devices can be synchronized online. The *SAASPASS* ID is owned by the individual user, is unique to the individual, is portable, and can be used for both work and personal use.

TYPES OF USERS

In *SAASPASS* there are three types of users: mobile app users, hard token users and SMS users. Only the mobile app can also be used for non-corporate personal use cases.

Mobile app users

Mobile app users are considered those users who downloaded the applications for their mobile phones, tablets, or all other wearable devices from the store.

By downloading the app on a single device, the user is getting their own unique SPID which will allow them to login into their computer, accessing the *SAASPASS* web portal together with the End-User panel and using the browser extension for easy login capabilities for their password manager and authenticators.

The unique *SAASPASS* ID is associated with the mobile app in the mobile device, but can also be cloned onto any device that supports iOS (iPhone, iPad, Apple Watch), Android (Android phones, Android tablets, Android Wear Watches, Kindle Fire, etc.), and BlackBerry. All cloned devices can be managed and synchronized online from the End-User Portal in Mobile Numbers & Device Management tabs.

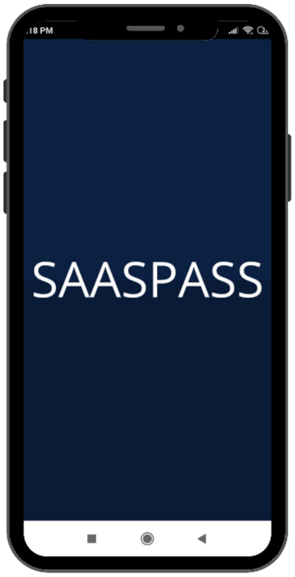
[1] At SAASPASS, we separate users from user accounts. Every user can own multiple user accounts, which can be used for different purposes. All those users accounts will be paired with the unique SPID of that user.

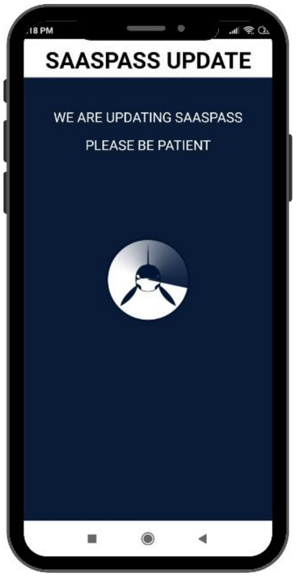
SETTING UP THE *SAASPASS* MOBILE APP AND A RECOVERY OPTION

Once you download the mobile app, you will be required to create a 4-digit PIN (can be changed in the future, or set another type of lock mechanism). You will need to click on the blue *Get Started* button at the top of the screen. After, read the short in-app tutorial and from the last page set the recovery number. If you skip that page, you can still set your recovery when you will move to the main screen of the either by:

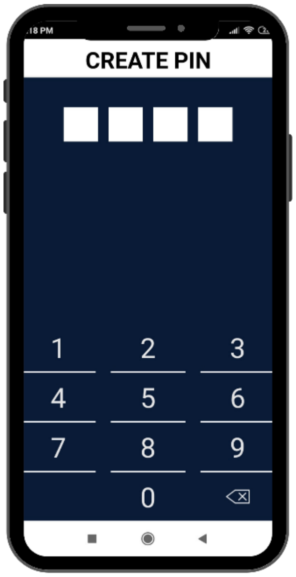
- clicking on the red alert message at the top of the screen,
- selecting MOBILE NUMBER in the menu, or
- from the settings, which is the gear icon at the top right side of your screen, choosing recovery.

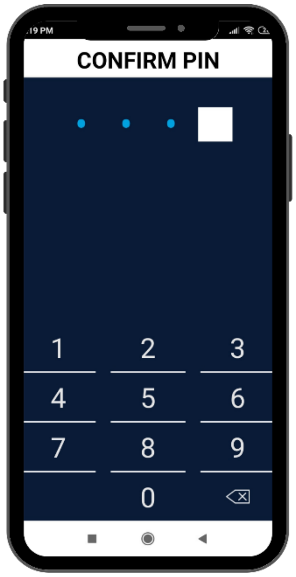
SAASPASS strongly recommends users to set their recovery number in their mobile app, no matter what use case be it personal, company or both types of user.

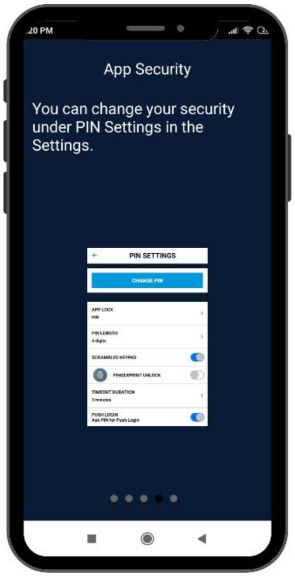

SAASPASS


SAASPASS UPDATE

WE ARE UPDATING SAASPASS
PLEASE BE PATIENT


CREATE PIN


CONFIRM PIN


App Security

You can change your security under PIN Settings in the Settings.

PIN SETTINGS

CHANGE PIN

APP LOCK
PIN

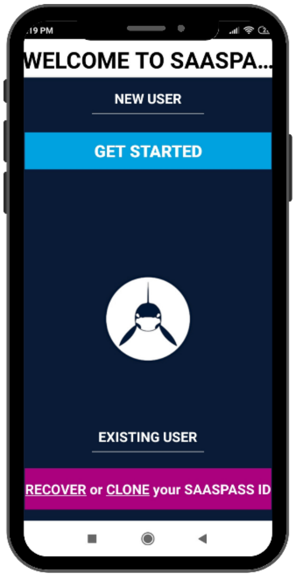
PIN LENGTH
4 digits

SCRAMBLED KEYPAD

FINGERPRINT UNLOCK

TIMEOUT DURATION
3 minutes

PUSH LOGIN
Ask PIN for Push Login

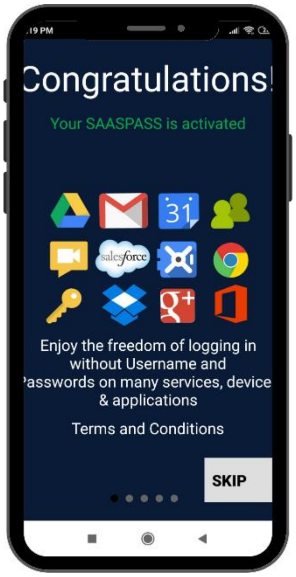

WELCOME TO SAASPA...

NEW USER

GET STARTED

EXISTING USER

RECOVER or CLONE your SAASPASS ID

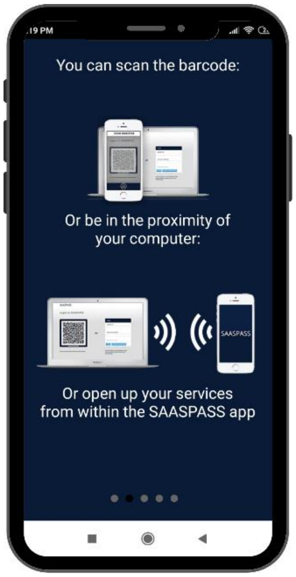

Congratulations!

Your SAASPASS is activated

Enjoy the freedom of logging in without Username and Passwords on many services, device & applications

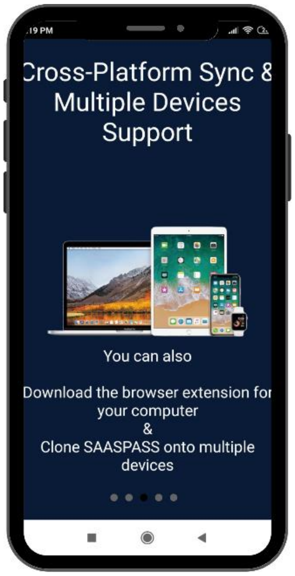
Terms and Conditions

SKIP


You can scan the barcode:

Or be in the proximity of your computer:

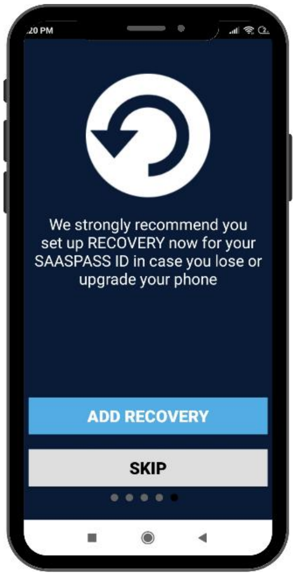
Or open up your services from within the SAASPASS app



Cross-Platform Sync & Multiple Devices Support

You can also

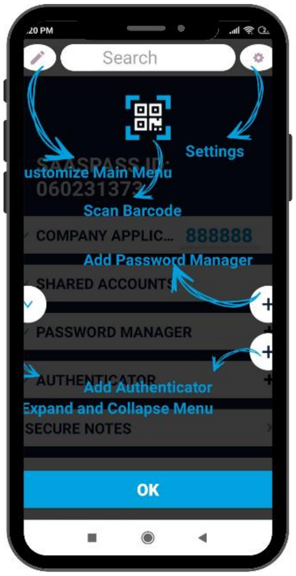
Download the browser extension for your computer
&
Clone SAASPASS onto multiple devices

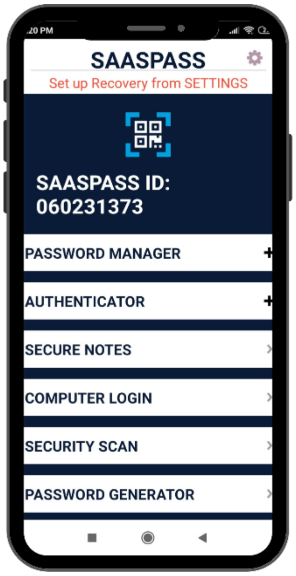


We strongly recommend you set up RECOVERY now for your SAASPASS ID in case you lose or upgrade your phone

ADD RECOVERY

SKIP





SAASPASS

Set up Recovery from SETTINGS

SAASPASS ID:
060231373

PASSWORD MANAGER +

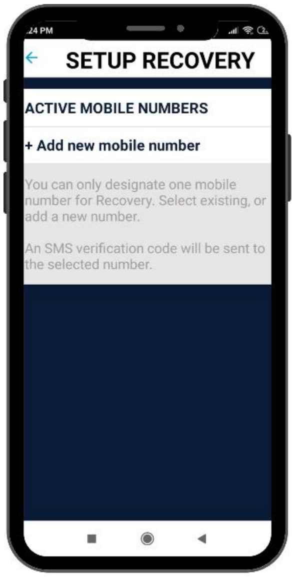
AUTHENTICATOR +

SECURE NOTES

COMPUTER LOGIN

SECURITY SCAN

PASSWORD GENERATOR



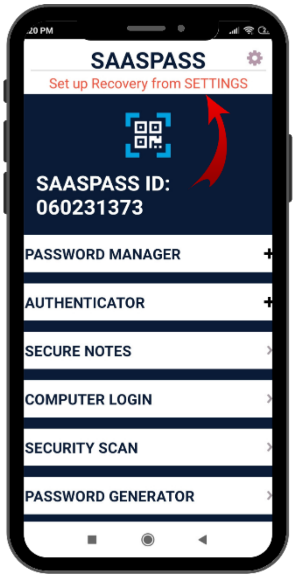
SETUP RECOVERY

ACTIVE MOBILE NUMBERS

+ Add new mobile number

You can only designate one mobile number for Recovery. Select existing, or add a new number.

An SMS verification code will be sent to the selected number.



SAASPASS

Set up Recovery from SETTINGS

SAASPASS ID:
060231373

PASSWORD MANAGER +

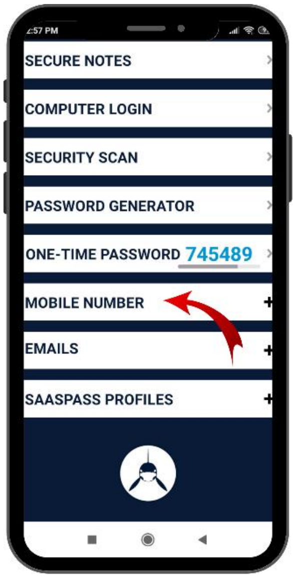
AUTHENTICATOR +

SECURE NOTES

COMPUTER LOGIN

SECURITY SCAN

PASSWORD GENERATOR



SECURE NOTES

COMPUTER LOGIN

SECURITY SCAN

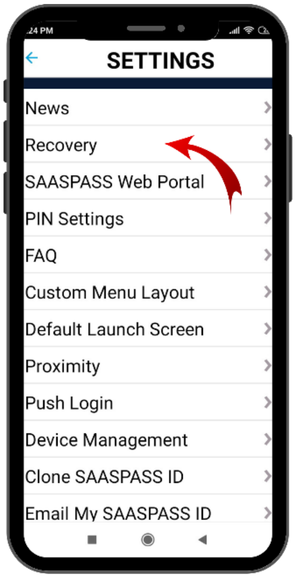
PASSWORD GENERATOR

ONE-TIME PASSWORD 745489

MOBILE NUMBER +

EMAILS +

SAASPASS PROFILES +



SETTINGS

News

Recovery

SAASPASS Web Portal

PIN Settings

FAQ

Custom Menu Layout

Default Launch Screen

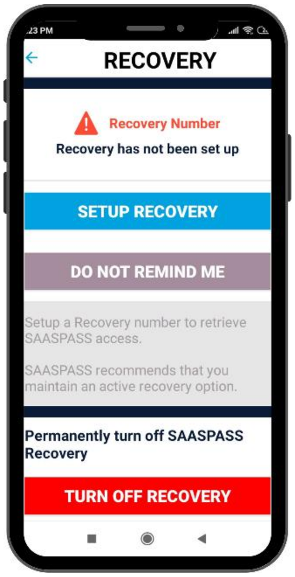
Proximity

Push Login

Device Management

Clone SAASPASS ID

Email My SAASPASS ID



RECOVERY

Recovery Number

Recovery has not been set up

SETUP RECOVERY

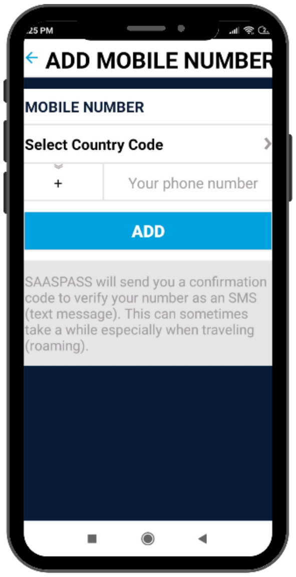
DO NOT REMIND ME

Setup a Recovery number to retrieve SAASPASS access.

SAASPASS recommends that you maintain an active recovery option.

Permanently turn off SAASPASS Recovery

TURN OFF RECOVERY



ADD MOBILE NUMBER

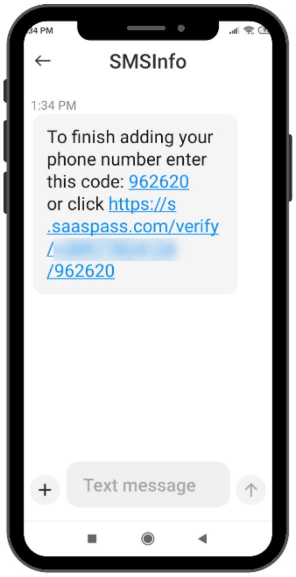
MOBILE NUMBER

Select Country Code

+ Your phone number

ADD

SAASPASS will send you a confirmation code to verify your number as an SMS (text message). This can sometimes take a while especially when traveling (roaming).

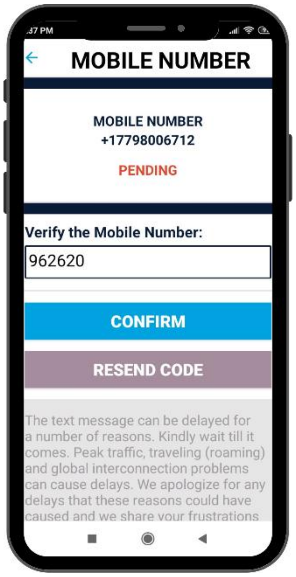


SMSInfo

1:34 PM

To finish adding your phone number enter this code: 962620 or click https://s.saaspass.com/verify/[redacted]/962620

Text message



MOBILE NUMBER

MOBILE NUMBER
+17798006712

PENDING

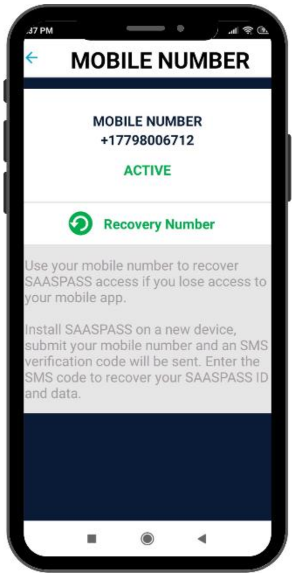
Verify the Mobile Number:

962620

CONFIRM

RESEND CODE

The text message can be delayed for a number of reasons. Kindly wait till it comes. Peak traffic, traveling (roaming) and global interconnection problems can cause delays. We apologize for any delays that these reasons could have caused and we share your frustrations



MOBILE NUMBER
+17798006712
ACTIVE

Use your mobile number to recover SAASPASS access if you lose access to your mobile app.

Install SAASPASS on a new device, submit your mobile number and an SMS verification code will be sent. Enter the SMS code to recover your SAASPASS ID and data.

Once the recovery number is set, from the Settings icon at the top right corner of your screen, choose the option Recovery and from there you can:

- Change the time period of 20 hours' delay for you to receive the verification code (a delay on the SMS delivery increases the security of your recovery, allowing you to contact your mobile carrier to avoid possible attacks).
- Add a customized recovery question and answer (right after the verification code is sent and populate, you will be asked for the security answer).
- Remove the active recovery option.
- Permanently turn off the recovery option (this action is irrevocable, once is done, you will never be able to set up recovery again and is only advised if you are 100% sure).

You can find more information at the Recovery Security section.

WHAT IF MY PHONE IS LOST OR DISABLED?

There are several methods for dealing with a lost or disabled mobile device, but the most important recommendation we make is to add a recovery phone number during setup. Mind that you can disable your *SAASPASS* mobile app even with 4 incorrect PIN entries in the app.

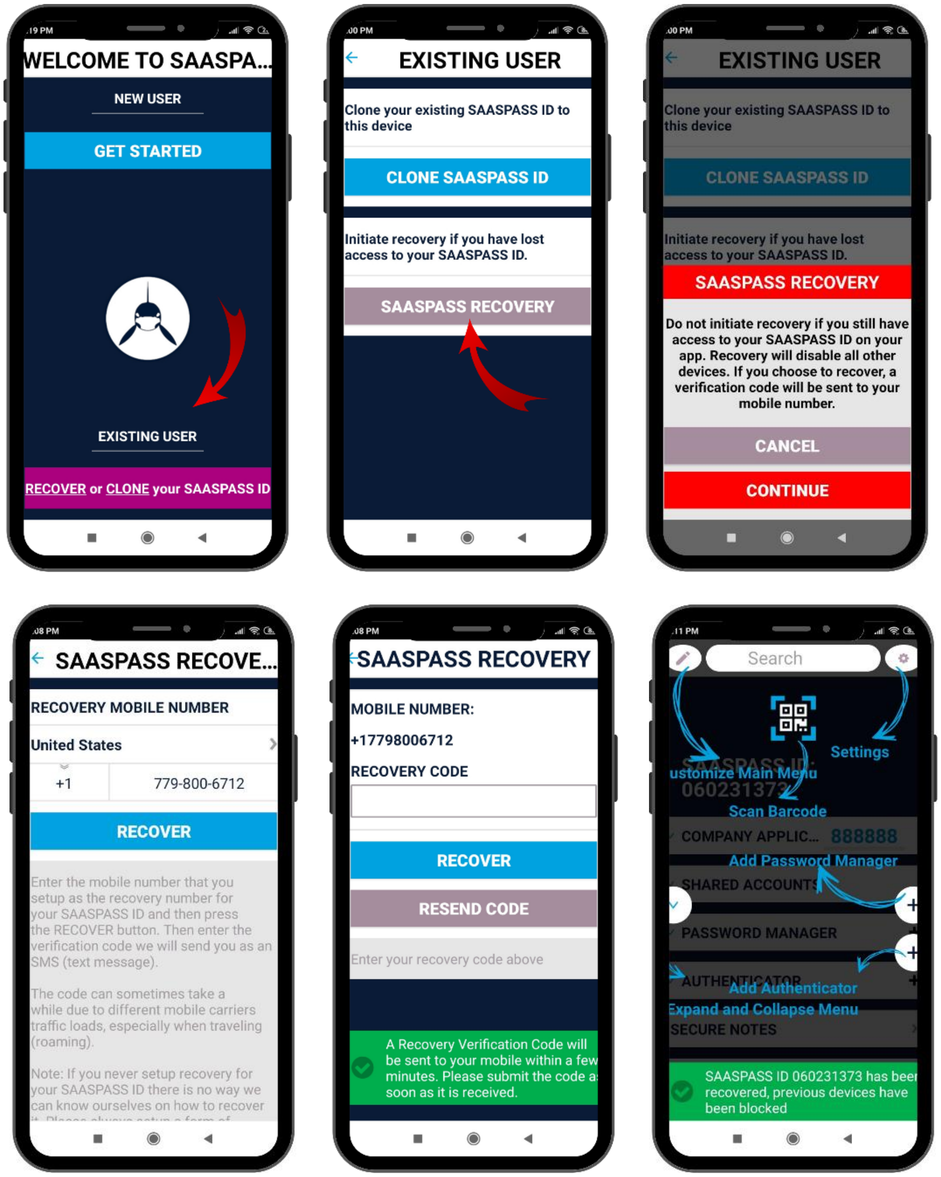
Lost or Disabled Mobile Device

There are multiple ways to recover your account in case of a lost or disabled mobile device:

SAASPASS Recovery

The easiest method to restore your account in the case of a lost or disabled mobile device is to initiate a *SAASPASS* Recovery. After you obtain a new device, and re-activate your original mobile number onto it, simply download a new *SAASPASS* app and select the purple button which says: "*Recovery or Clone your SAASPASS ID"* under EXISTING USER. After, choose the *SAASPASS* recovery option and enter your recovery number. A verification code will be sent by SMS to the number, and upon confirmation, your original account will be restored onto your new device. When you initiate a Recovery, your *SAASPASS* account will only be restored on the mobile device on which you are running the Recovery. If there is a *SAASPASS* mobile app associated with your *SAASPASS* ID installed or cloned onto any other device, that *SAASPASS* app will immediately clear and reset.

If you did not pair your account with a mobile number during initial setup, we strongly recommend you to do so now, otherwise this method of restoring your account will not be possible. Go to the MOBILE NUMBER section in your *SAASPASS* mobile app and add a mobile number there if you do not see one listed.



Clone your existing SAASPASS ID to this device

Initiate recovery if you have lost access to your SAASPASS ID.

Do not initiate recovery if you still have access to your SAASPASS ID on your app. Recovery will disable all other devices. If you choose to recover, a verification code will be sent to your mobile number.

Enter the mobile number that you setup as the recovery number for your SAASPASS ID and then press the RECOVER button. Then enter the verification code we will send you as an SMS (text message).

The code can sometimes take a while due to different mobile carriers traffic loads, especially when traveling (roaming).

Note: If you never setup recovery for your SAASPASS ID there is no way we can know ourselves on how to recover

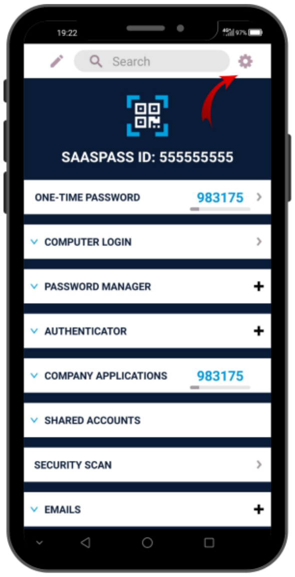
Enter your recovery code above

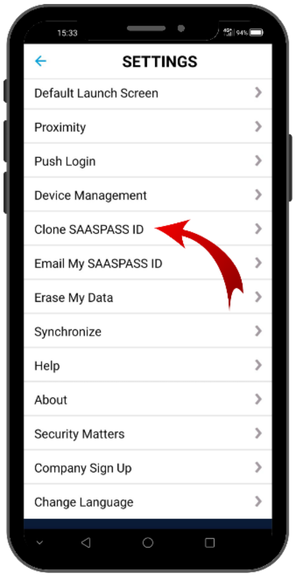
A Recovery Verification Code will be sent to your mobile within a few minutes. Please submit the code a soon as it is received.

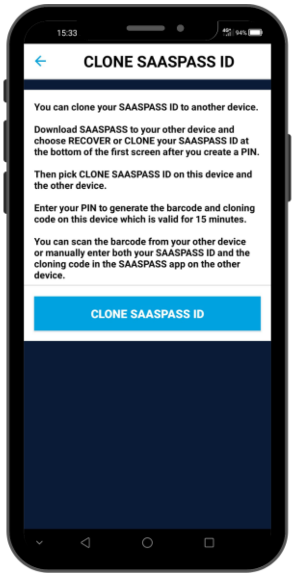
SAASPASS ID 060231373 has beer recovered, previous devices have been blocked

Cloning an Account

Cloning your *SAASPASS* account to a second device (or multiple devices) is another way to back up your *SAASPASS* account. Using this method, it is not necessary to have a recovery number. If you lose your primary device, the account remains on the cloned device(s) from which the account on the primary device can simply be removed. If you run a recovery, the *SAASPASS* account is automatically deleted from any other devices. To clone your *SAASPASS* ID onto another device go to SETTINGS on the original device. Pick CLONE *SAASPASS* ID and then enter your PIN or Pattern or Touch ID. This will produce a cloning code and a barcode that can be scanned. Download a brand new *SAASPASS* app onto the target device and after activating it, choose the CLONE option at the bottom right. Manually enter or scan the cloning code on your original *SAASPASS* app.







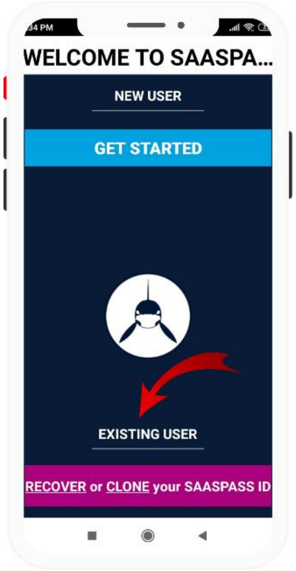
You can clone your SAASPASS ID to another device.

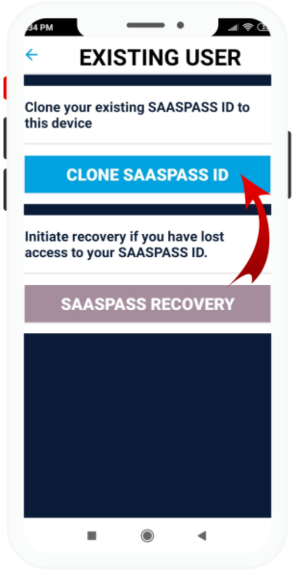
Download SAASPASS to your other device and choose RECOVER or CLONE your SAASPASS ID at the bottom of the first screen after you create a PIN.

Then pick CLONE SAASPASS ID on this device and the other device.

Enter your PIN to generate the barcode and cloning code on this device which is valid for 15 minutes.

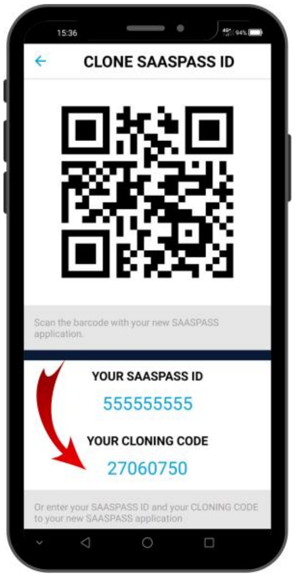
You can scan the barcode from your other device or manually enter both your SAASPASS ID and the cloning code in the SAASPASS app on the other device.





Clone your existing SAASPASS ID to this device

Initiate recovery if you have lost access to your SAASPASS ID.

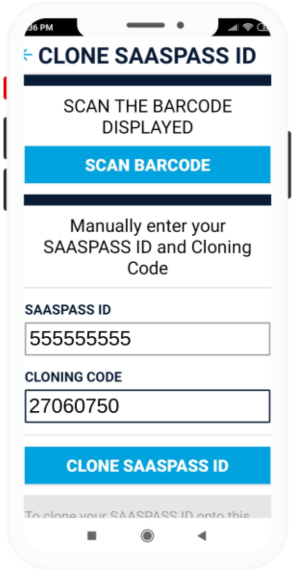


Scan the barcode with your new SAASPASS application.

YOUR SAASPASS ID
555555555

YOUR CLONING CODE
27060750

Or enter your SAASPASS ID and your CLONING CODE to your new SAASPASS application

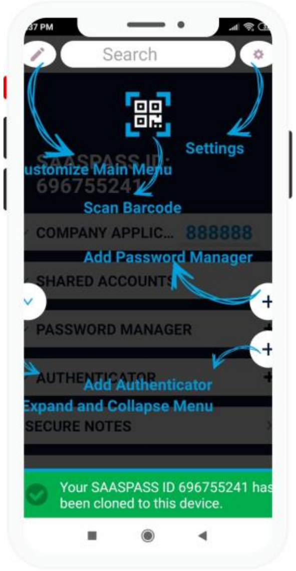

CLONE SAASPASS ID
SCAN THE BARCODE DISPLAYED
SCAN BARCODE

Manually enter your SAASPASS ID and Cloning Code

SAASPASS ID: 555555555

CLONING CODE: 27060750

CLONE SAASPASS ID
To clone your SAASPASS ID onto this



Your SAASPASS ID 696755241 has been cloned to this device.

Unrecoverable Accounts and Starting Over

Lastly, if your mobile device is permanently lost or disabled, and you're unable to run a recovery and you have no cloned devices, then you will need to download a fresh *SAASPASS* app to a new device and start over. You will need to re-setup all of the personal apps that you had paired with your account. For the personal password managers, usernames and passwords will need to be re-entered into the new *SAASPASS* app. But for personal authenticators, you will need to contact the account provider for each account (i.e. Facebook, Amazon, Gmail, etc.) to restore access. Due to this reason, *SAASPASS* strongly recommends setting up a recovery number.

Recovery Security

A critical weakness of many security products or features is often the recovery process. Recovery can create a backdoor that leaves the solution as a whole vulnerable to attack. *SAASPASS* has devised a number of measures to keep our recovery process from being the weak link in the chain: When a Recovery is initiated on a device, the *SAASPASS* account is always automatically deleted from all other devices.

- Because of the risk of interception when your verification code is sent by SMS during *SAASPASS* Recovery, *SAASPASS* uses a dynamic one-time passcode for verification, so once used, it is no longer valid, even if it's intercepted.
- A 20-hour delay period can also be configured, starting from when you initiate Recovery to when the verification code is sent to you. In other words, if you lose your phone, and initiate the recovery process, the verification code will not be sent to your number for 20 hours to give you time to cancel your lost or stolen device and set up your mobile number on a new device through your mobile service provider.
- A customized recovery question and answer can be added as an additional layer of protection.
- Although *SAASPASS* recommends that users maintain an active Recovery option, for the most concerned users, the Recovery option can be removed completely, so that an account cannot be restored. If Recovery is removed, this is an irrevocable action and cannot be undone, and cloning would be the only way to back up your account.

Some of these added precautions make the recovery process less convenient, but users can decide on their own what level of security they require and can configure options to the Recovery process, as needed.

HOW DOES *SAASPASS* HANDLE MY PRIVACY AND DATA CONCERNS?

SAASPASS acts as a digital "gatekeeper" checking the validity of your credentials before allowing you to access each protected "gate." What's behind that gate is your business. *SAASPASS* cannot know or see any of the credentials you store in your *SAASPASS* app and these are all encrypted at military-grade standards. Also, your *SAASPASS* PIN code is encrypted and stored only on your device; *SAASPASS* has no access to it, nor to the one-time passcodes generated in your device. Without these dynamic one-time passcodes, even knowing and decrypting your usernames and passwords would be useless information. In short, there is no way for *SAASPASS* to access any accounts that you protect with *SAASPASS*.

DEVICES SUPPORTED

SAASPASS works basically like a traditional lock and key system, where your “key” is your mobile phone or other *SAASPASS* enabled device, and the “lock” can be a computer, a smart lock, digital application, VPN, an IoT device, and so forth. Basically any device that runs iOS or Android or other mobile operating systems can operate as the “key” (Apple Watch, iPads, etc.) and any machine that runs OS’ such as Windows, Linux, and other supported protocols like SAML 2.0/Radius/OIDC/API can be the “lock” device. *SAASPASS* works seamlessly on iPhones, Android, Blackberry, and over 350 Java MIDP2 enabled mobile phones have been tested and certified through our extensive internal quality assurance process. We constantly test and certify new models as they become available. *SAASPASS* no longer supports Windows phones.

The Key - *SAASPASS* can be installed and/or cloned onto any device that supports:

- iOS (iPhone, iPad, Apple Watch, etc.)
- Android (Android phones, Android tablets, Android Wear Watches, Kindle Fire, etc.)
- BlackBerry
- Feature Phones (any device that supports J2ME)

The Lock - *SAASPASS* can be used to secure and authenticate to any device that supports:

- Windows
- Mac OS/OS X
- Linux
- Custom IoT OS, using our API (i.e. smart locks)

MULTI-FACTOR AUTHENTICATION (MFA)

Most experts agree that usernames and passwords are no longer adequate for verifying a user’s identity securely, and multi-factor authentication is now seen as a necessary security requirement for individuals and organizations. Multi-factor authentication (MFA), also known as “two-factor authentication” or ‘two-step verification” is the process of requiring two or more of the following factors to confirm your identity:

1. Knowledge: Something only you know.
2. Possession: Something only you have.
3. Inherence: Something only you are.

Simply adding a layer of MFA can dramatically reduce the risk and impact of a data breach or identity theft, but not every MFA solution is equal. For example, *SAASPASS* does not consider usernames and passwords as something only you know. Because they are inherently insecure, we assume everyone CAN know your username and password. So, our first factor begins with the PIN.. .

1. **Knowledge: Something only you know = *SAASPASS* PIN**

   The PIN used to unlock your *SAASPASS* mobile app is known only by you. *SAASPASS* goes above and beyond conventional best-practice for PINs by using our own custom-built keyboard, rather than relying on integration using the keyboard APIs built for the device's operating system, as all competing MFA solutions do. This means that other apps downloaded onto your device cannot gain access then "listen to" your PIN as it's being typed into your keypad. Also, the *SAASPASS* PIN is encrypted and stored only on your device. Even *SAASPASS* is unable to access it. Plus, *SAASPASS* PIN settings are configurable. The PIN keyboard can be scrambled, for example, so the order of the numbers on your keypad are randomly changed each time you open the app. Even someone standing behind you or watching the physical motions of your hands through a video camera would be unable to guess your PIN, in this case.

2. **Possession: Something only you have = Mobile Device + Dynamic passcodes**

   Your mobile device is something only you have in your possession, but more importantly, the dynamic one-time passcodes generated (out-of-band) within the device in the *SAASPASS* app are something only you have. Even if your phone is stolen, the dynamic codes are unable to be accessed without both unlocking the device (through a PIN or biometric - something only you know or something only you are) plus unlocking the *SAASPASS* app through an additional and separate PIN or biometric. Moreover, each passcode changes every 30 seconds, so even if obtained by a cybercriminal, the code would soon be useless if not used immediately.

3. **Inherence: Something only you are = Biometrics (fingerprint)**

   As a convenient alternative to the *SAASPASS* PIN, a fingerprint or other biometric--something you are--can be used to unlock the *SAASPASS* app under limited circumstances--only if the PIN was recently used to successfully unlock the app.

END-USER PORTAL

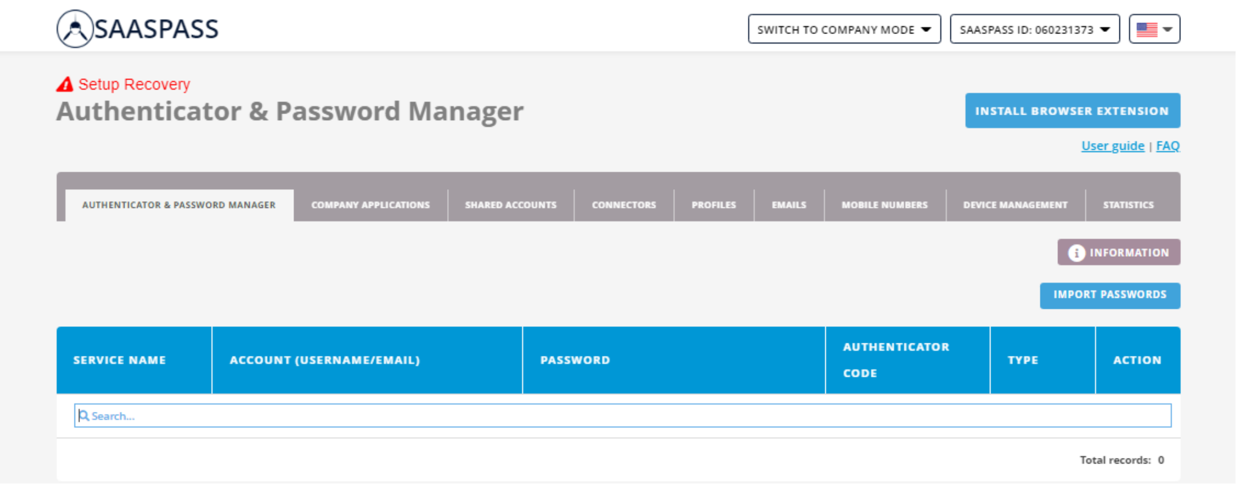
Every *SAASPASS* ID has access to their own End-User Portal and it doesn't matter if the SPID belongs to a company user or if it's a personal one. The End-User Portal is unique and personal to every user, no other SPID has access to it. Every time you log in to *SAASPASS* the first place that you are redirected to is the End-User Portal, from there, you can manage your personal credentials. In the following section, all capabilities and actions for personal users are explained in detail.

AUTHENTICATOR & PASSWORD MANAGER

In the Authentication & Password Manager tab, you are able to see all personal credentials that you imported or added from the mobile application. While using the Authenticators and Password Managers, we do recommend you to download and install the *SAASPASS* browser extension and let the browser extension auto-fill and auto-login into websites.

If you didn't set a recovery number into your mobile app, in the End-User Portal, there will always be a reminder for you to do so, until you set a recovery or turn off the reminder from your mobile app. Also, the Install Browser Extension button will be shown until you download the extension for the browser that you use.

You can download the extension directly from the End-User Portal or from the *SAASPASS* web site from the Download page.



Authenticator & Password Manager

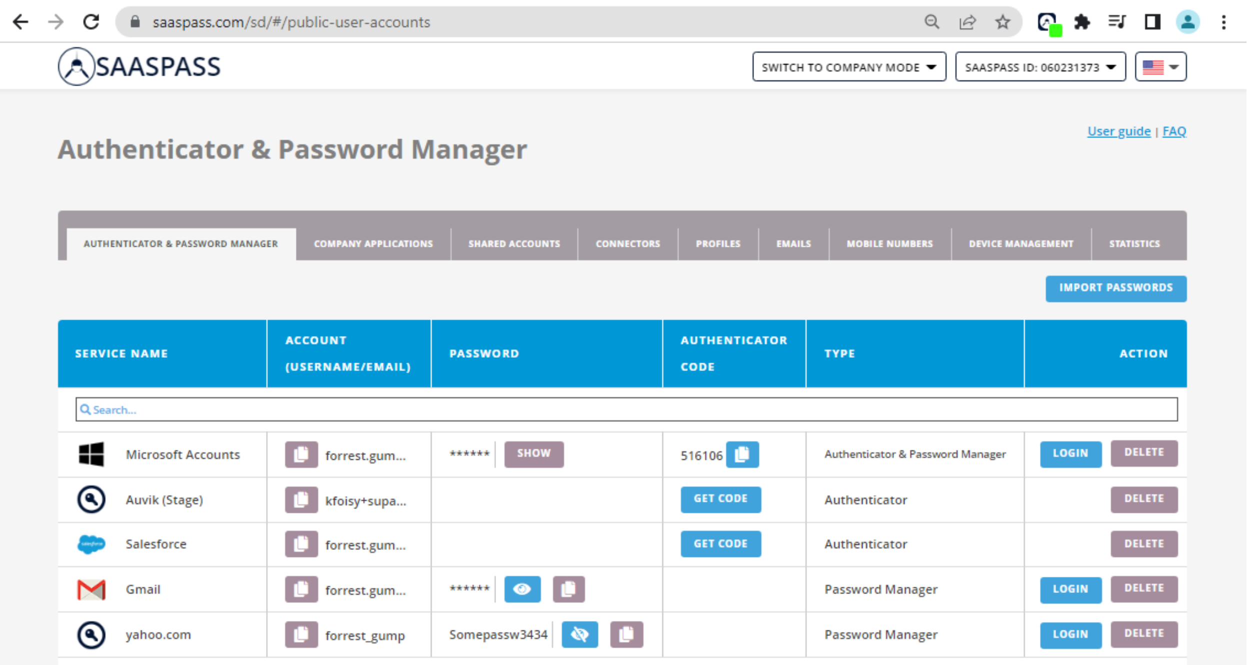
SERVICE NAME	ACCOUNT (USERNAME/EMAIL)	PASSWORD	AUTHENTICATOR CODE	TYPE	ACTION

Total records: 0

In the table with Authenticators and Password Managers you will be able to see:

- the Service name,
- the Account (username or the email),
- the Password which automatically is hidden and if you click on the *Show* button you will be able to see and copy it,
- if the credentials are from the type Authenticator by clicking on the *Get Code* button, the code will be shown from where you can copy and use it,
- the type of the service which can either be Authenticator, Password Manager or both,
- field with actions from where you can SSO login or delete the chosen credentials.

Once you set up a recovery number, download the browser extension and create or import your authenticators or password managers, the view will be similar to the picture below.



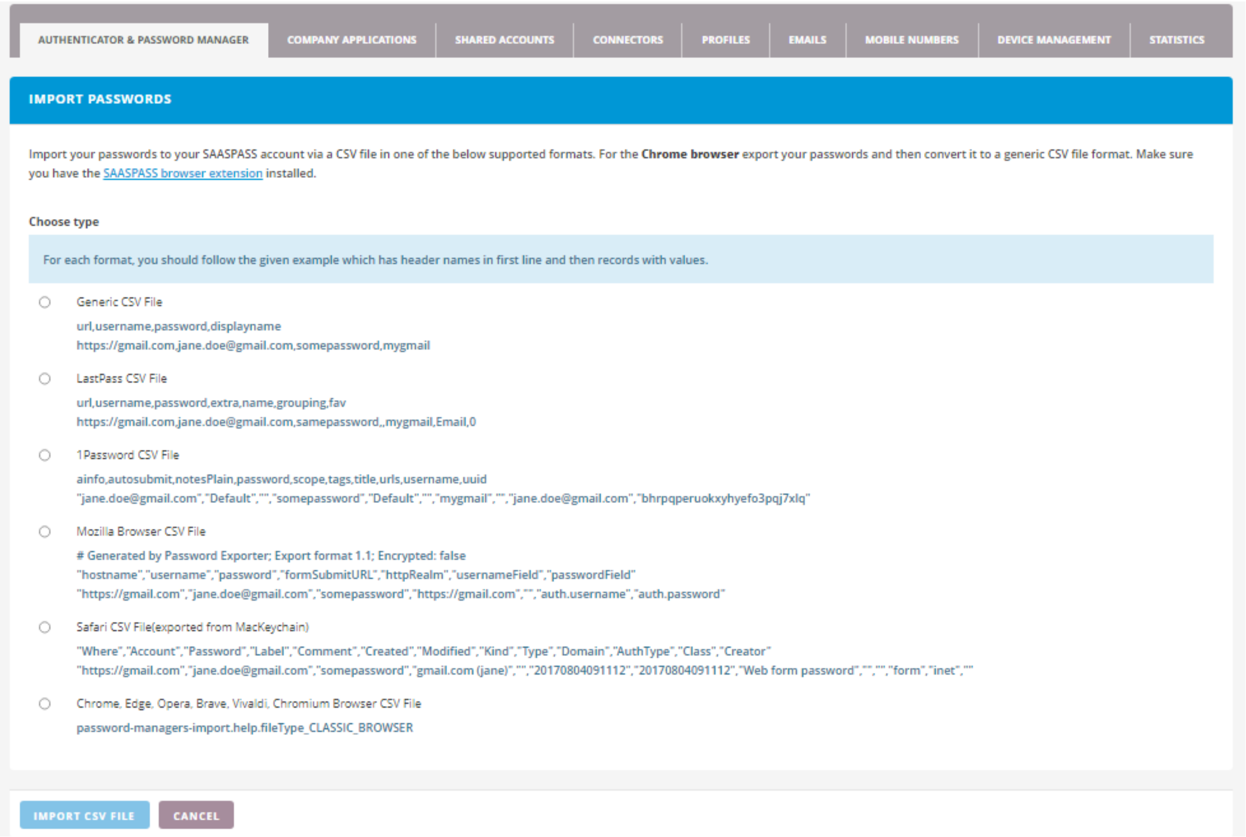
Authenticator & Password Manager

SERVICE NAME	ACCOUNT (USERNAME/EMAIL)	PASSWORD	AUTHENTICATOR CODE	TYPE	ACTION
Microsoft Accounts	forrest.gum...	****** SHOW	516106	Authenticator & Password Manager	LOGIN DELETE
Auvik (Stage)	kfoisy+supa...		GET CODE	Authenticator	DELETE
Salesforce	forrest.gum...		GET CODE	Authenticator	DELETE
Gmail	forrest.gum...	******		Password Manager	LOGIN DELETE
yahoo.com	forrest_gump	Somepassw3434		Password Manager	LOGIN DELETE

Import Passwords

The Users are allowed to import their personal Passwords Managers by CSV file. The maximum allowed amount of personal credentials is 500, the same is applied to the maximum number of rows per CSV file. By clicking on the *Import Passwords* button, you will be redirected to a page from where you can choose one of the supported formats. For each format, you should follow the given example which has header names in the first line and then records with values.

url,username,password,displayname
https://gmail.com,jane.doe@gmail.com,somepassword,mygmail
https://login.salesforce.com/, forrest.gump@popcornfly.com,Forres.GumP2022,Salesforce



IMPORT PASSWORDS

Import your passwords to your SAASPASS account via a CSV file in one of the below supported formats. For the **Chrome browser** export your passwords and then convert it to a generic CSV file format. Make sure you have the SAASPASS browser extension installed.

Choose type

For each format, you should follow the given example which has header names in first line and then records with values.

○ Generic CSV File

url,username,password,displayname
https://gmail.com,jane.doe@gmail.com,somepassword,mygmail

○ LastPass CSV File

url,username,password,extra,name,grouping,fav
https://gmail.com,jane.doe@gmail.com,samepassword,,mygmail,Email,0

○ 1Password CSV File

ainfo,autosubmit,notesPlain,password,scope,tags,title,urls,username,uuid
"jane.doe@gmail.com","Default","","somepassword","Default","","mygmail","","jane.doe@gmail.com","bhrpqperuokxyhyefo3pqj7xlq"

○ Mozilla Browser CSV File

Generated by Password Exporter; Export format 1.1; Encrypted: false
"hostname","username","password","formSubmitURL","httpRealm","usernameField","passwordField"
"https://gmail.com","jane.doe@gmail.com","somepassword","https://gmail.com","","auth.username","auth.password"

○ Safari CSV File(exported from MacKeychain)

"Where","Account","Password","Label","Comment","Created","Modified","Kind","Type","Domain","AuthType","Class","Creator"
"https://gmail.com","jane.doe@gmail.com","somepassword","gmail.com (jane)","","20170804091112","20170804091112","Web form password","","","form","inet",""

○ Chrome, Edge, Opera, Brave, Vivaldi, Chromium Browser CSV File

password-managers-import.help.fileType_CLASSIC_BROWSER

COMPANY APPLICATIONS

This section is only available for company users and will remain empty until your company starts using *SAASPASS* as an identity and access management tool for securing the corporate network.

SHARED ACCOUNTS

This section is only available for company users and will remain empty until your company starts using *SAASPASS* as an identity and access management tool for securing and sharing the corporate credentials.

CONNECTORS

Installing the Computer Connector is necessary for adding Computer Login Protection and also includes a desktop client called the Single Sign-On Console (Desktop Client). The Single Sign-On (SSO) Console is a drop-down menu on your desktop that you use for one-click access to each of your websites and applications. In order for the client to work and to be useful, you will need to download the browser extension.

WARNING: If your Computer is a domain bound/Active Directory Company computer, please do not install the personal protection, for AD bound machines it is necessary that you are a company user. Also if you have a Microsoft ID on Windows 10 do not download it as it currently does not support it. If you do proceed, you risk being locked out.

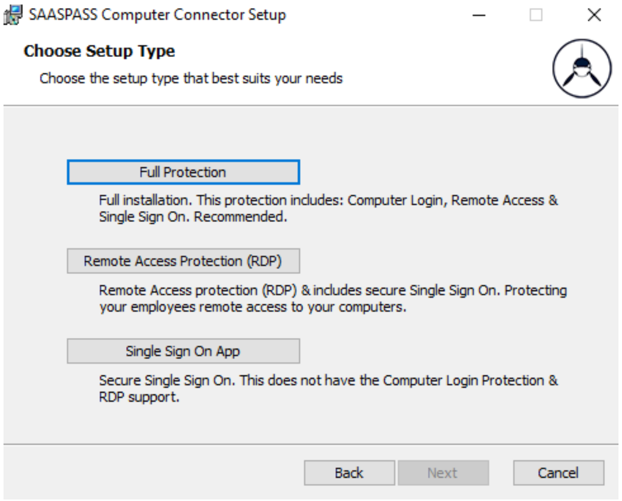
Before installation, ensure that your firewalls or VPNs will not interfere with *SAASPASS* connections. Some Antivirus programs (such as Avast) may treat *SAASPASS* as a threat and may not allow the full installation of *SAASPASS* Computer Connector. In such cases we strongly recommend adding an exception for *SAASPASS* Computer Connector in your Antivirus program.

Installing the Computer Connector is necessary for adding Computer Login Protection and also includes a desktop client called the Single Sign-On Console. SSO Console (Desktop Client) The Single Sign-On (SSO) Console is a drop-down menu on your desktop that you use for one-click access to each of your websites and applications. It is a desktop client installed onto your computer when you download the Computer Connector.

The Computer Protection can be used in offline mode as well. In order to use the offline mode, it is required that the user login with OTP while an internet connection is available for the first time and after, the user can use the offline mode of authentication with a one-time password.

Installation process

Go to the End-User Portal or to the *SAASPASS* web site where there is the Download page and download the matching version. Open the package and follow the installation wizard, when you will need to choose the setup type, we recommend choosing the Full Protection option. After the installation process is done, open the desktop app *SAASPASS* Computer Connector and log in by scanning the barcode or manually with your SPID and one-time password (OTP) that you will find in your *SAASPASS* mobile app (we do recommend the first login to be login with your *SAASPASS* ID and One-Time password).


SAASPASS Computer Connector Setup

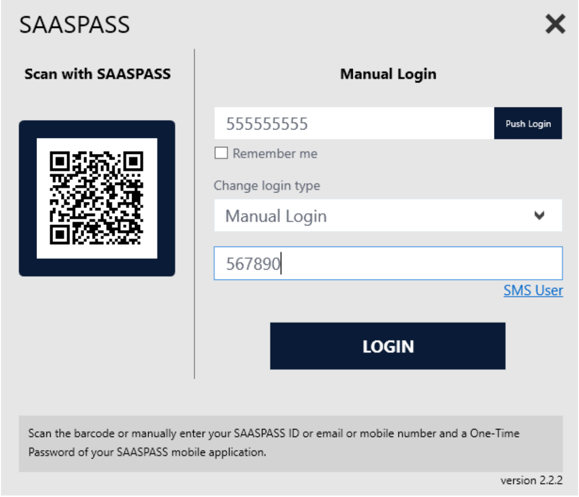
Choose Setup Type

Choose the setup type that best suits your needs

Full installation. This protection includes: Computer Login, Remote Access & Single Sign On. Recommended.

Remote Access protection (RDP) & includes secure Single Sign On. Protecting your employees remote access to your computers.

Secure Single Sign On. This does not have the Computer Login Protection & RDP support.


SAASPASS

555555555

□ Remember me

Change login type: Manual Login

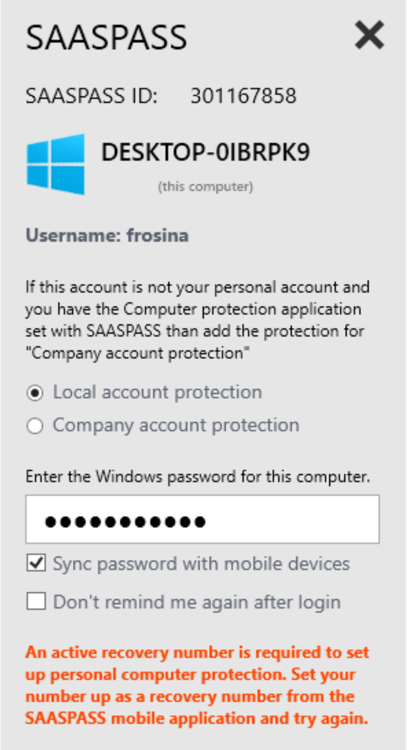
567890

Scan the barcode or manually enter your SAASPASS ID or email or mobile number and a One-Time Password of your SAASPASS mobile application.

version 2.2.2

Next, from the opened form, choose Local account protection, fill in the Windows password for the computer and check the box for password synchronization with the *SAASPASS* mobile app. After doing that click on the Activate button and then the Finish button.

IMPORTANT: You will not be able to set the Computer Protection without having an active recovery number set!!!


SAASPASS

SAASPASS ID: 301167858

DESKTOP-0IBRPK9

(this computer)

Username: frosina

If this account is not your personal account and you have the Computer protection application set with SAASPASS than add the protection for "Company account protection"

● Local account protection

○ Company account protection

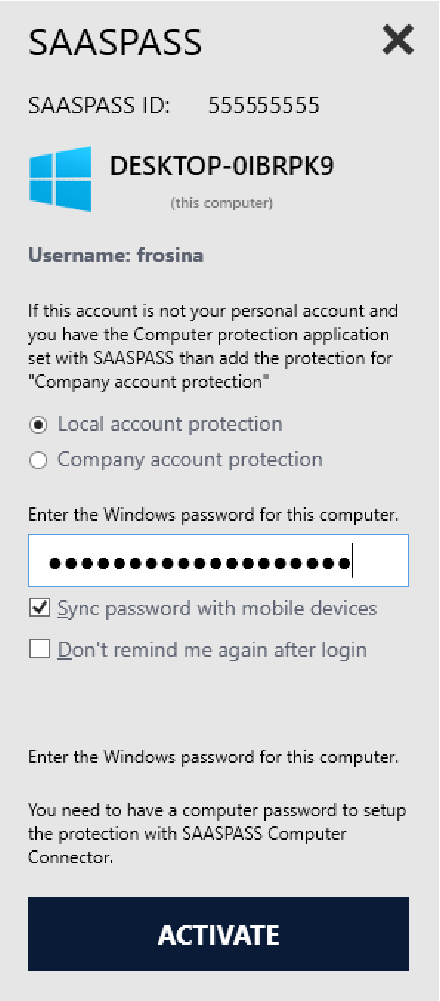
Enter the Windows password for this computer.

●●●●●●●●●●●

☑ Sync password with mobile devices

□ Don't remind me again after login

An active recovery number is required to set up personal computer protection. Set your number up as a recovery number from the SAASPASS mobile application and try again.



SAASPASS ✕

SAASPASS ID: 555555555

DESKTOP-0IBRPK9

(this computer)

Username: frosina

If this account is not your personal account and you have the Computer protection application set with SAASPASS than add the protection for "Company account protection"

● Local account protection

○ Company account protection

Enter the Windows password for this computer.

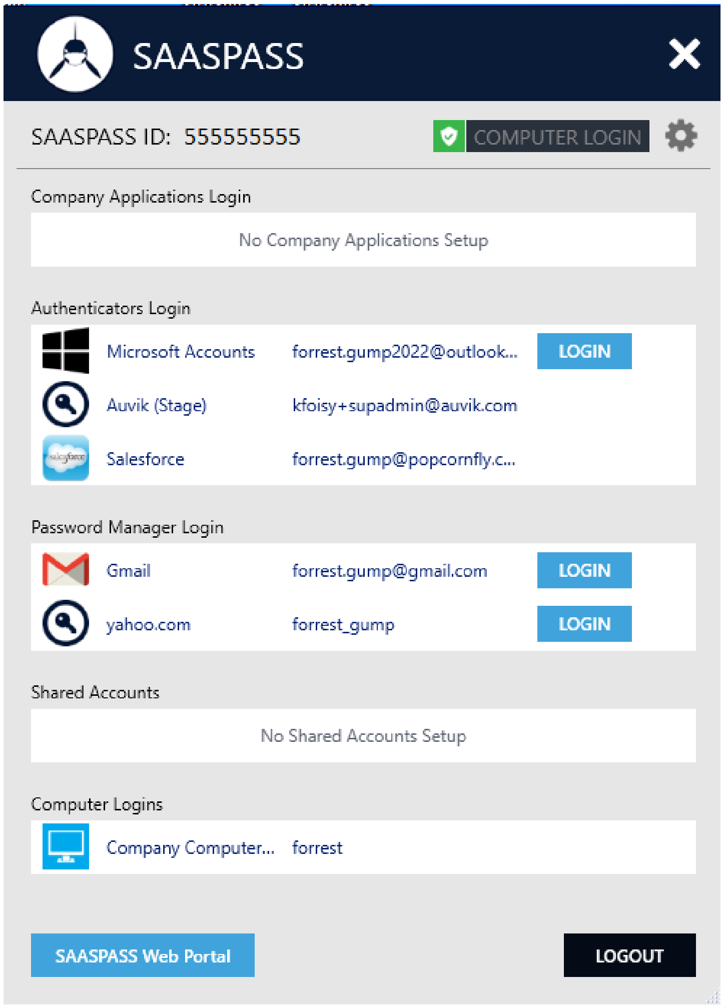
••••••••••••••••••••

☑ Sync password with mobile devices

□ Don't remind me again after login

Enter the Windows password for this computer.

You need to have a computer password to setup the protection with SAASPASS Computer Connector.



SAASPASS ✕

SAASPASS ID: 555555555 COMPUTER LOGIN

Company Applications Login

No Company Applications Setup

Authenticators Login

Microsoft Accounts	forrest.gump2022@outlook...	LOGIN
Auvik (Stage)	kfoisy+supadmin@auvik.com	
Salesforce	forrest.gump@popcornfly.c...	

Password Manager Login

Gmail	forrest.gump@gmail.com	LOGIN
yahoo.com	forrest_gump	LOGIN

Shared Accounts

No Shared Accounts Setup

Computer Logins

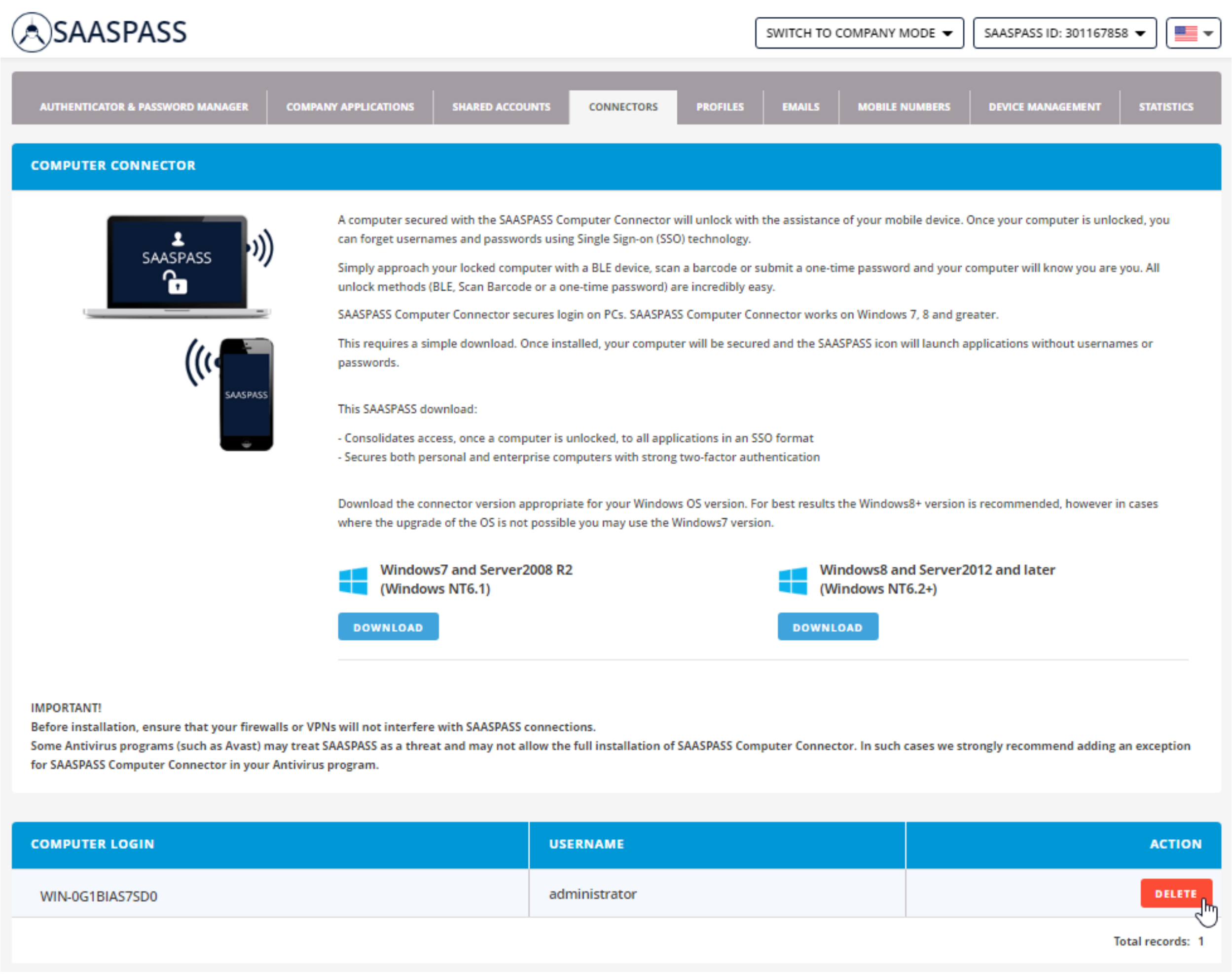
Company Computer...	forrest

After, you will be able to see the SSO console, from where you can directly login into your saved Password Managers, Authenticators and *SAASPASS* web portal. After installing and setting the Desktop client, we do recommend you to restart your machine. After the restart you will be prompted with the *SAASPASS* login options. From your mobile, you have the option for remote lock and unlock your machine.

If by any reason, you are not able to enter into your machine, then from the Connectors tab you can delete the protection and be able to login. Before taking this action be sure that your internet connection is good and you try all the methods for login: OTP, scanning the barcode, push notification and remote unlock.

If you are about to delete Computer Protection, when you will click on the *Delete* button, a pop up window will show up where you will need to enter the One-Time Password from your *SAASPASS* mobile app.

After you enter into your machine, you will be need to uninstall the protection and set it up again.



COMPUTER CONNECTOR

A computer secured with the SAASPASS Computer Connector will unlock with the assistance of your mobile device. Once your computer is unlocked, you can forget usernames and passwords using Single Sign-on (SSO) technology.

Simply approach your locked computer with a BLE device, scan a barcode or submit a one-time password and your computer will know you are you. All unlock methods (BLE, Scan Barcode or a one-time password) are incredibly easy.

SAASPASS Computer Connector secures login on PCs. SAASPASS Computer Connector works on Windows 7, 8 and greater.

This requires a simple download. Once installed, your computer will be secured and the SAASPASS icon will launch applications without usernames or passwords.

This SAASPASS download:

- Consolidates access, once a computer is unlocked, to all applications in an SSO format
- Secures both personal and enterprise computers with strong two-factor authentication

Download the connector version appropriate for your Windows OS version. For best results the Windows8+ version is recommended, however in cases where the upgrade of the OS is not possible you may use the Windows7 version.

Windows7 and Server2008 R2
(Windows NT6.1)

DOWNLOAD

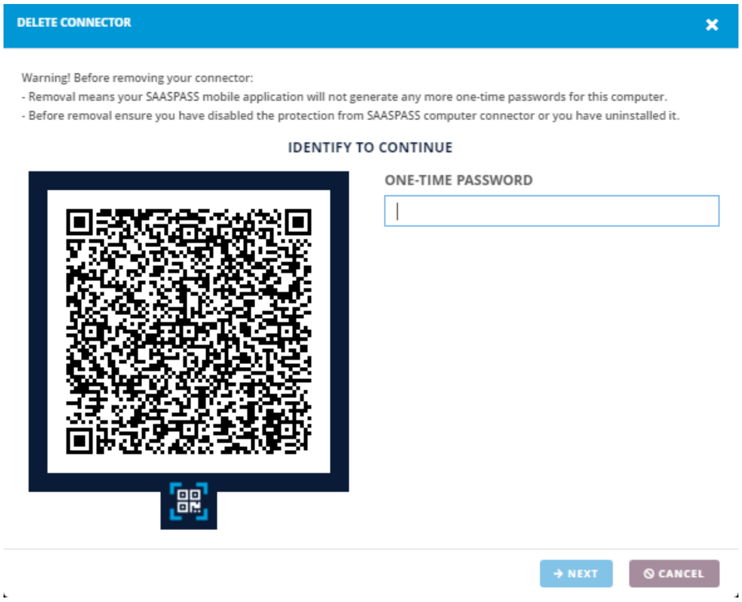
Windows8 and Server2012 and later
(Windows NT6.2+)

DOWNLOAD

IMPORTANT!
Before installation, ensure that your firewalls or VPNs will not interfere with SAASPASS connections.
Some Antivirus programs (such as Avast) may treat SAASPASS as a threat and may not allow the full installation of SAASPASS Computer Connector. In such cases we strongly recommend adding an exception for SAASPASS Computer Connector in your Antivirus program.

COMPUTER LOGIN	USERNAME	ACTION
WIN-0G1BIAS7SD0	administrator	DELETE

Total records: 1



DELETE CONNECTOR

Warning! Before removing your connector:
- Removal means your SAASPASS mobile application will not generate any more one-time passwords for this computer.
- Before removal ensure you have disabled the protection from SAASPASS computer connector or you have uninstalled it.

IDENTIFY TO CONTINUE

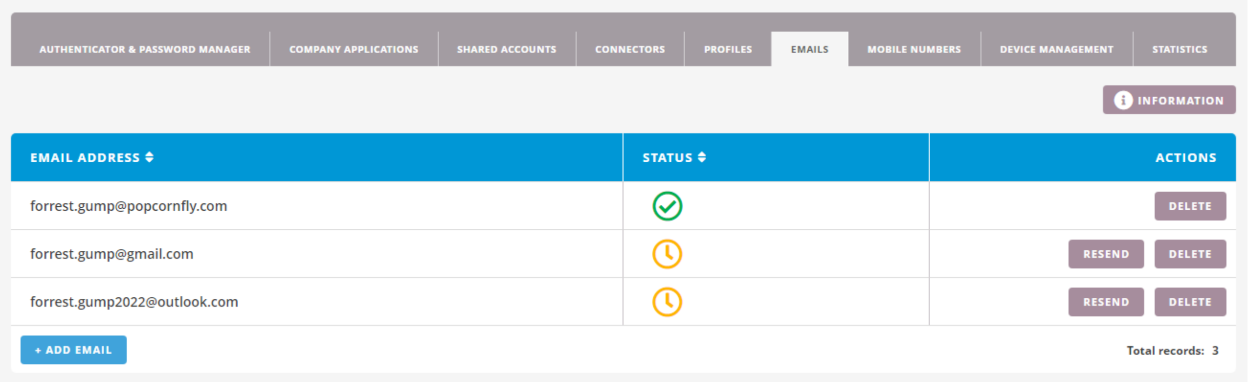
ONE-TIME PASSWORD

PROFILES

Profiles section is used only by Company users to register and login instantly to applications that support *SAASPASS*.

EMAILS

You can manage your personal emails from here. All emails must be verified by a verification link.

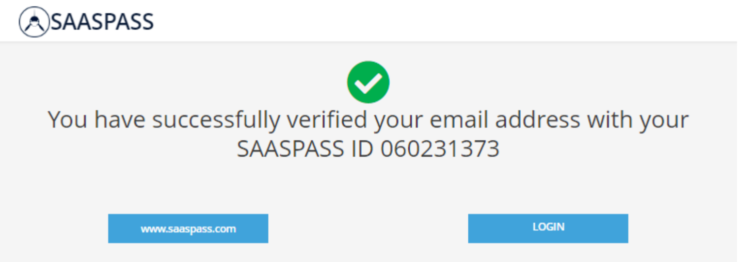


EMAIL ADDRESS ⇕	STATUS ⇕	ACTIONS
forrest.gump@popcornfly.com	✓	DELETE
forrest.gump@gmail.com	🕓	RESEND DELETE
forrest.gump2022@outlook.com	🕓	RESEND DELETE

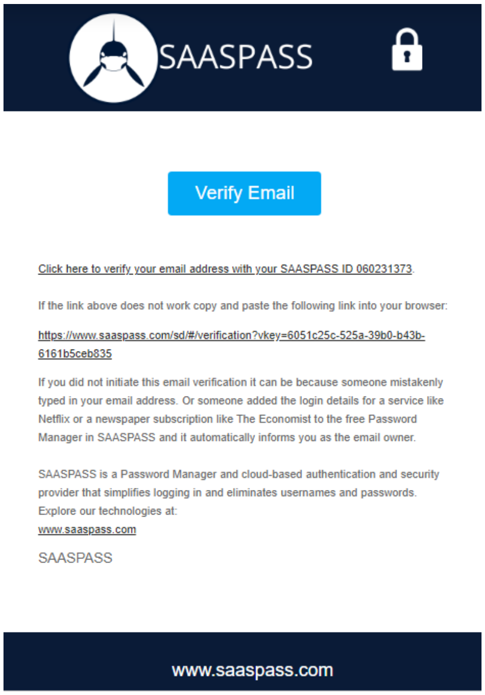
+ ADD EMAIL

Total records: 3

Whenever you add a new password manager with a different email then the existing ones, you will get an automated email for verification. You can also add new emails directly from the End-User portal and resend the verification link to those who are not verified yet.



You have successfully verified your email address with your SAASPASS ID 060231373



Click here to verify your email address with your SAASPASS ID 060231373.

If the link above does not work copy and paste the following link into your browser:

https://www.saaspass.com/sd/#/verification?vkey=6051c25c-525a-39b0-b43b-6161b5ceb835

If you did not initiate this email verification it can be because someone mistakenly typed in your email address. Or someone added the login details for a service like Netflix or a newspaper subscription like The Economist to the free Password Manager in SAASPASS and it automatically informs you as the email owner.

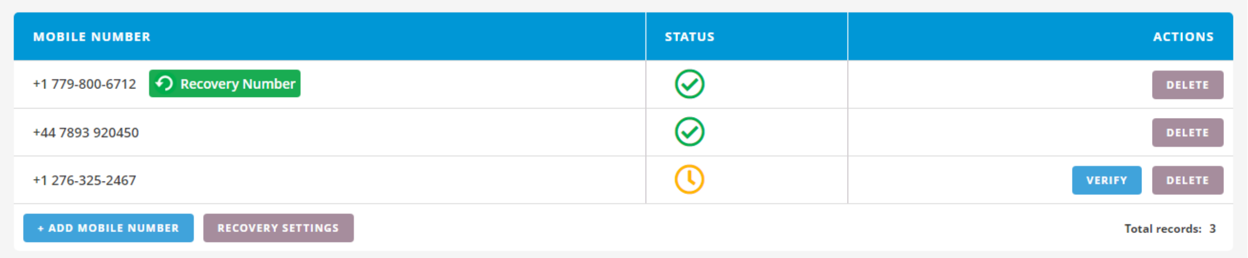
SAASPASS is a Password Manager and cloud-based authentication and security provider that simplifies logging in and eliminates usernames and passwords.
Explore our technologies at:
www.saaspass.com

SAASPASS

www.saaspass.com

MOBILE NUMBERS

In this section you can add a number or you can change your Recovery Settings.

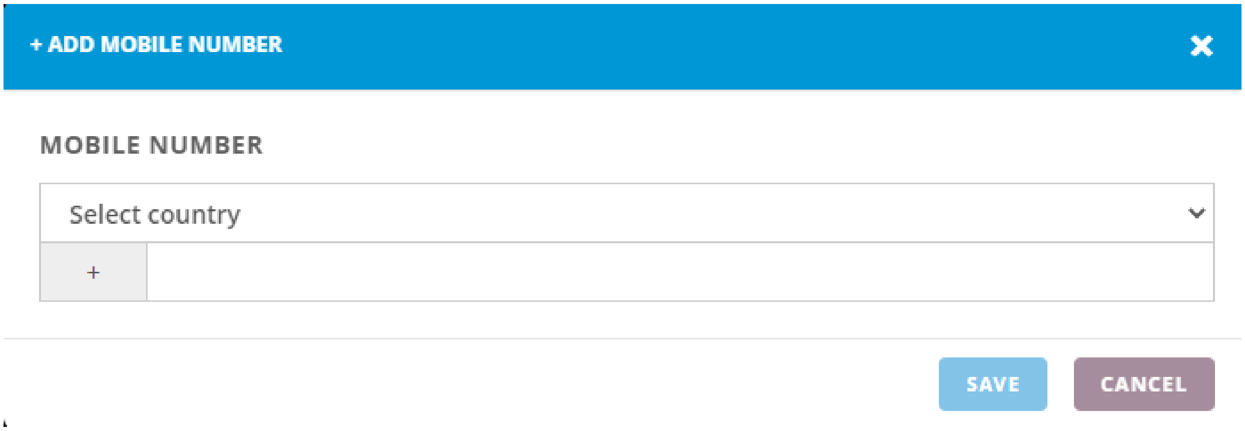


MOBILE NUMBER	STATUS	ACTIONS
+1 779-800-6712 Recovery Number	✓	DELETE
+44 7893 920450	✓	DELETE
+1 276-325-2467	🕓	VERIFY DELETE

+ ADD MOBILE NUMBER RECOVERY SETTINGS

Total records: 3

To add a number, you will need to click on the *Add Mobile Number* button and select the country and enter your mobile number. After, when you will receive the SMS code into your mobile enter the verification code in the dedicated field and click the *Verify* button.

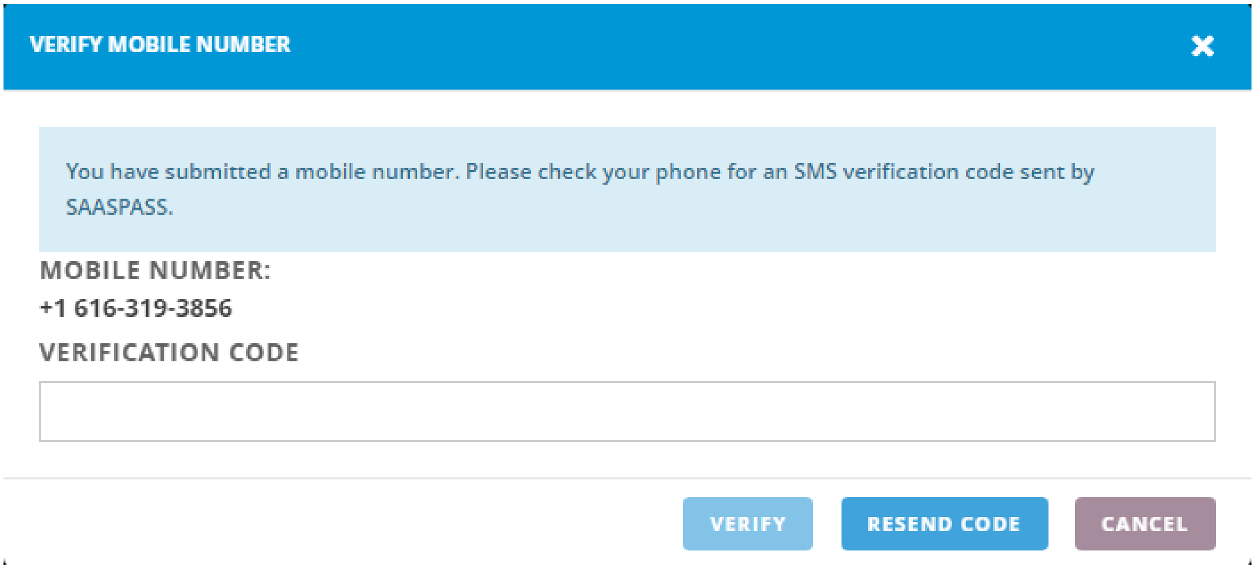


+ ADD MOBILE NUMBER

MOBILE NUMBER

Select country

+



VERIFY MOBILE NUMBER

You have submitted a mobile number. Please check your phone for an SMS verification code sent by SAASPASS.

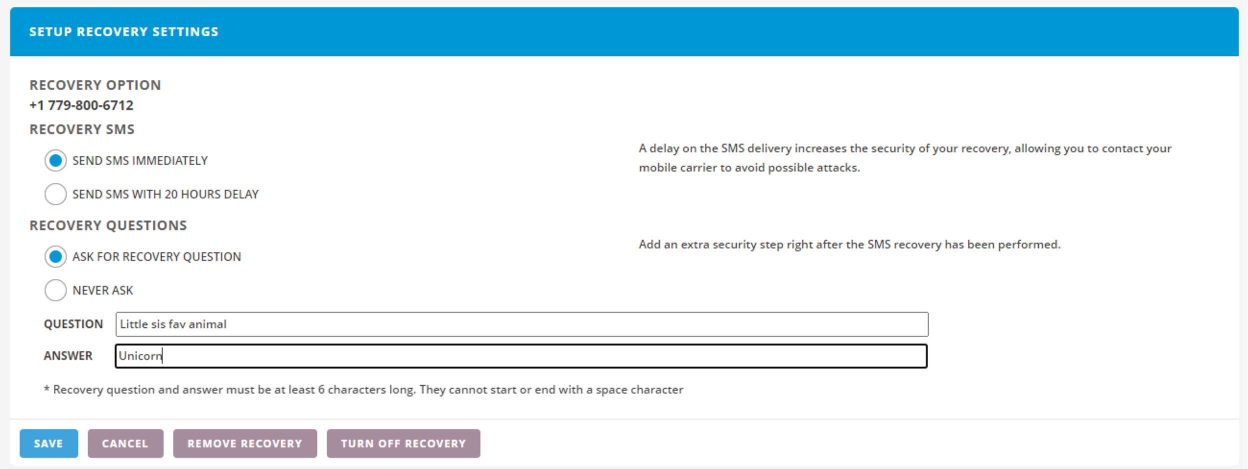
MOBILE NUMBER:
+1 616-319-3856

VERIFICATION CODE

Every number added can be verified by a SMS confirmation code and only one number can be your recovery number. The recovery number is marked with a green box. The verified number, in the status field, has a green check mark, and those numbers that need to be verified are marked with a yellow clock.

If you have multiple verified numbers and if you delete the recovery number for of any reason, the number that you verified second in row, will automatically become a recovery number.

To edit the Recovery Settings, click on the *Recovery Settings* button. From there you can choose SMS recovery options from: 'Immediate Recovery SMS' or 'Delayed Recovery SMS' for recovery confirmation codes. Optionally, as an additional security factor to SMS recovery, you can define a security question and answer, to make your recovery process more secure.



SETUP RECOVERY SETTINGS

RECOVERY OPTION
+1 779-800-6712

RECOVERY SMS

● SEND SMS IMMEDIATELY

○ SEND SMS WITH 20 HOURS DELAY

A delay on the SMS delivery increases the security of your recovery, allowing you to contact your mobile carrier to avoid possible attacks.

RECOVERY QUESTIONS

● ASK FOR RECOVERY QUESTION

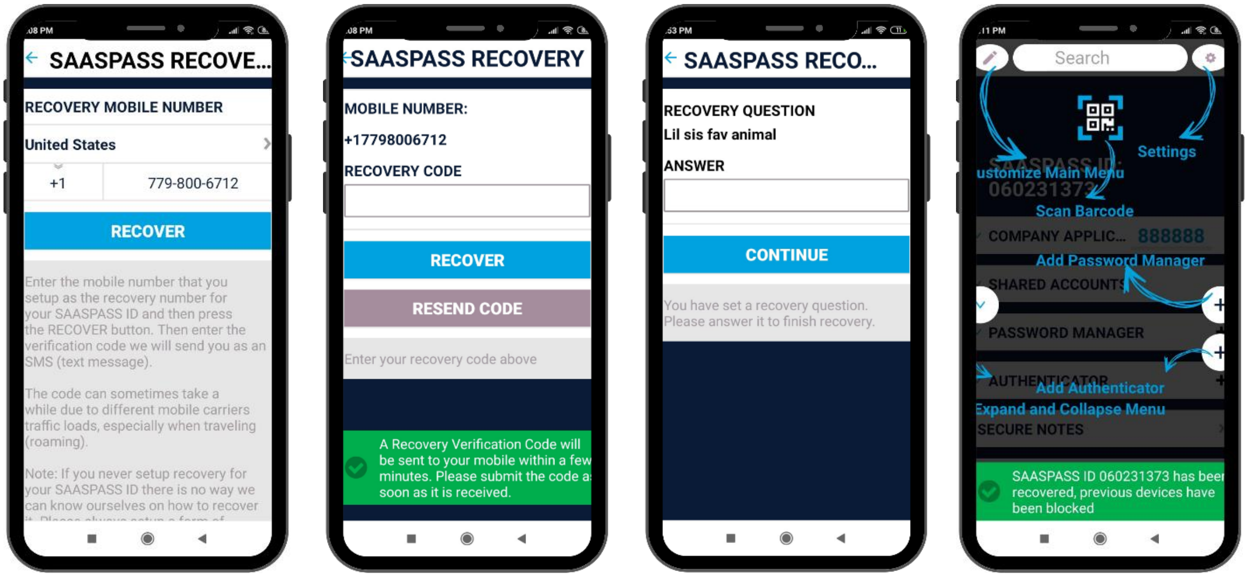
○ NEVER ASK

Add an extra security step right after the SMS recovery has been performed.

QUESTION	Little sis fav animal
ANSWER	Unicorn

* Recovery question and answer must be at least 6 characters long. They cannot start or end with a space character

If you set a recovery question, that means that when you will initiate a recovery and populate the recovery code that you will receive by SMS, you will be asked to answer the security question that you set previously. Until you didn't set the correct answer, you will not be able to proceed with the recovery.



RECOVERY MOBILE NUMBER

United States

+1 779-800-6712

Enter the mobile number that you setup as the recovery number for your SAASPASS ID and then press the RECOVER button. Then enter the verification code we will send you as an SMS (text message).

The code can sometimes take a while due to different mobile carriers traffic loads, especially when traveling (roaming).

Note: If you never setup recovery for your SAASPASS ID there is no way we can know ourselves on how to recover

MOBILE NUMBER:
+17798006712

RECOVERY CODE

Enter your recovery code above

A Recovery Verification Code will be sent to your mobile within a few minutes. Please submit the code a soon as it is received.

RECOVERY QUESTION
Lil sis fav animal

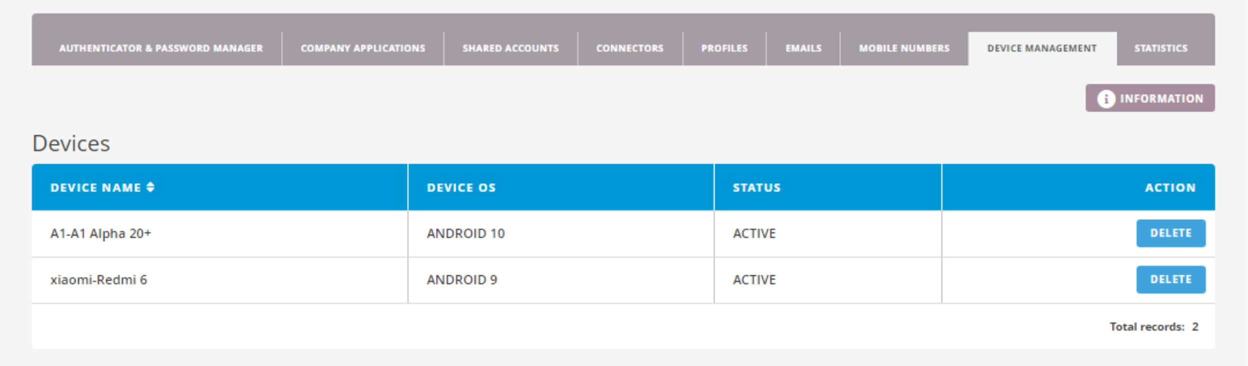
ANSWER

You have set a recovery question. Please answer it to finish recovery.

SAASPASS ID 060231373 has been recovered, previous devices have been blocked

DEVICE MANAGEMENT

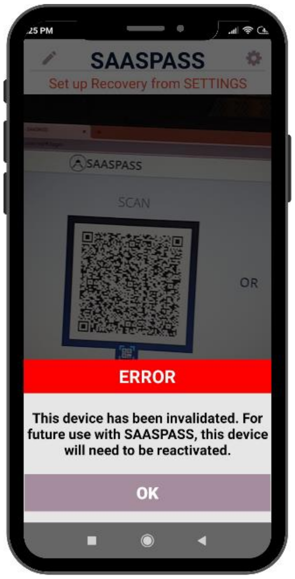
The same *SAASPASS* ID can be used across multiple devices. All active devices will be shown listed here. You can find out more about cloning *SAASPASS* in the Cloning an Account section.



Devices

DEVICE NAME ⬍	DEVICE OS	STATUS	ACTION
A1-A1 Alpha 20+	ANDROID 10	ACTIVE	DELETE
xiaomi-Redmi 6	ANDROID 9	ACTIVE	DELETE

Total records: 2



ERROR

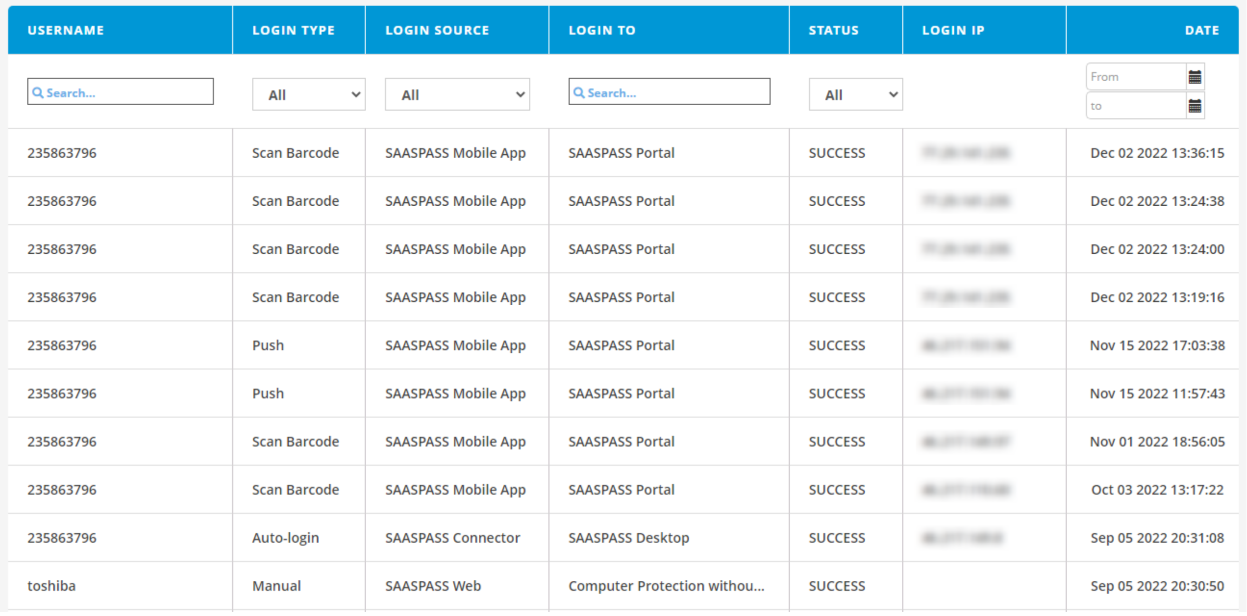
This device has been invalidated. For future use with SAASPASS, this device will need to be reactivated.

OK

If you delete a device that’s means that the *SAASPASS* mobile app will no longer be functional on that device. The application will remain to exist but if you try to use it, you will get a proper error message.

STATISTICS

In this section you can see your login activities.



USERNAME	LOGIN TYPE	LOGIN SOURCE	LOGIN TO	STATUS	LOGIN IP	DATE
Search...	All	All	Search...	All		From to
235863796	Scan Barcode	SAASPASS Mobile App	SAASPASS Portal	SUCCESS	[redacted]	Dec 02 2022 13:36:15
235863796	Scan Barcode	SAASPASS Mobile App	SAASPASS Portal	SUCCESS	[redacted]	Dec 02 2022 13:24:38
235863796	Scan Barcode	SAASPASS Mobile App	SAASPASS Portal	SUCCESS	[redacted]	Dec 02 2022 13:24:00
235863796	Scan Barcode	SAASPASS Mobile App	SAASPASS Portal	SUCCESS	[redacted]	Dec 02 2022 13:19:16
235863796	Push	SAASPASS Mobile App	SAASPASS Portal	SUCCESS	[redacted]	Nov 15 2022 17:03:38
235863796	Push	SAASPASS Mobile App	SAASPASS Portal	SUCCESS	[redacted]	Nov 15 2022 11:57:43
235863796	Scan Barcode	SAASPASS Mobile App	SAASPASS Portal	SUCCESS	[redacted]	Nov 01 2022 18:56:05
235863796	Scan Barcode	SAASPASS Mobile App	SAASPASS Portal	SUCCESS	[redacted]	Oct 03 2022 13:17:22
235863796	Auto-login	SAASPASS Connector	SAASPASS Desktop	SUCCESS	[redacted]	Sep 05 2022 20:31:08
toshiba	Manual	SAASPASS Web	Computer Protection withou...	SUCCESS		Sep 05 2022 20:30:50

For any questions, you can always contact us at:

support@saaspass.com