SAASPASS

Start Guide For Company Users

Table of Contents

company user guide

company user guide

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, 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 confirm.
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. The same SPID can even be used by a user employed at multiple companies. Due to the fact that corporate and personal data operate in sandboxed silos, company admins can manage and configure user access to their own corporate network, but have no access to the employee's personal apps and services, or another employer's network. This allows a company to extend the security perimeter of their organization to the personal data of employees, without compromising the employee's privacy.

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-

[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.

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.

Hard Token users

Hard token users are those who use tokens to login into the *SAASPASS* web portal, secure application, or login into their computer. Hard Token users can be only company users. *SAASPASS* supports a number of physical hard/USB token solutions for companies, and those include: USB FIDO Tokens, USB (non-FIDO) Tokens, OATH TOTP Hard Tokens, OATH HOTP Hard Tokens.

SMS users

SAASPASS offers the ability to use SMS (text messaging) as two-factor authentication for the employees who do not have mobile phones that support the *SAASPASS* application. A dynamic password sent by SMS increases the security compared to static username/password credentials but is considerably less than dynamic passwords generated by the *SAASPASS* mobile application.

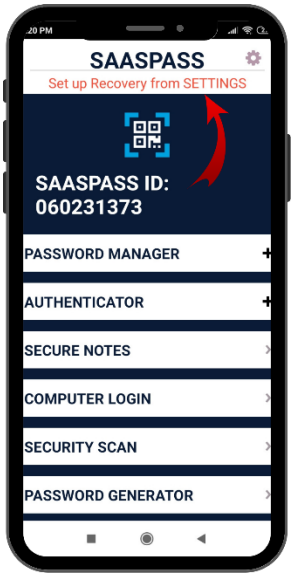
Setting up the SAASPASS mobile app and a recovery option

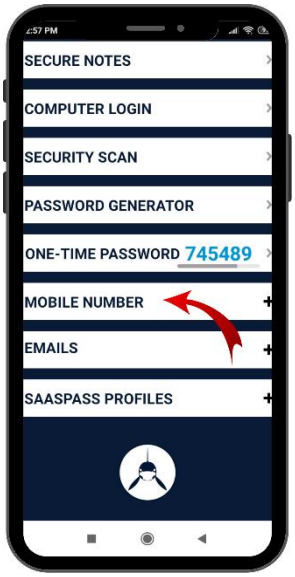
Once you download the mobile application, you will be required to create a 4-digit PIN, which can be changed in the future, or set another type of lock mechanism for your SAASPASS app. You will need to click on the blue *Get Started* button at the top of the screen. After, read the short in-app tutorial 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 *SAASPASS* app either by:

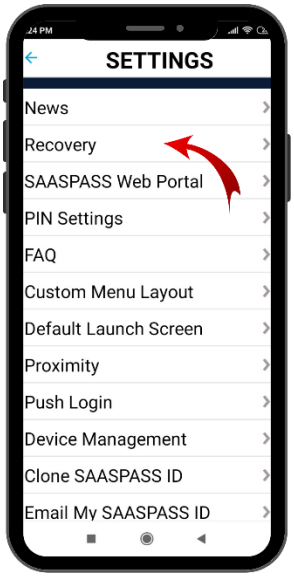
- clicking on the red alert message at the top of the screen,
- selecting “Mobile Number” in the menu, or
- from the settings, the gear icon at the top right side of your screen, choose “Recovery”.

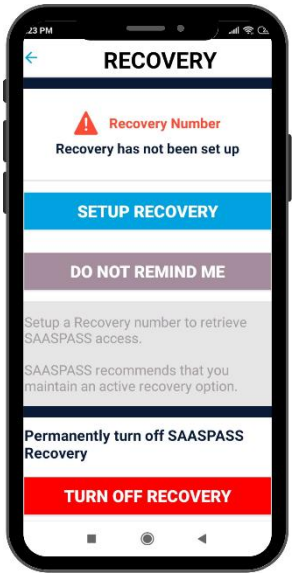
SAASPASS strongly recommends users to set their recovery number in their mobile app, no matter what use case be it personal, company or both types of user.

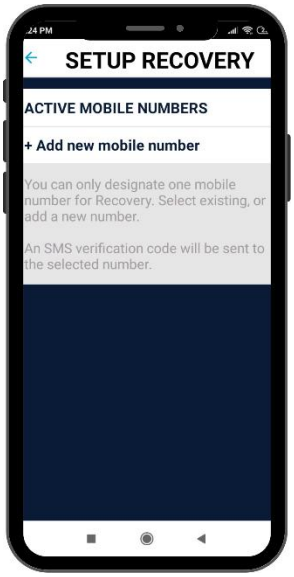

SAASPASS
SAASPASS UPDATE
WE ARE UPDATING SAASPASS
PLEASE BE PATIENT
CREATE PIN
CONFIRM PIN
App Security
You can change your security under PIN Settings in the Settings.
WELCOME TO SAASPA...
NEW USER
GET STARTED
EXISTING USER
RECOVER or CLONE your SAASPASS ID
Congratulations!
Your SAASPASS is activated
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
Search
Settings
Scan Barcode
Add Password Manager
Add Authenticator
Expand and Collapse Menu
OK
SAASPASS
Set up Recovery from SETTINGS
SAASPASS ID:
060231373
PASSWORD MANAGER
AUTHENTICATOR
SECURE NOTES
COMPUTER LOGIN
SECURITY SCAN
PASSWORD GENERATOR

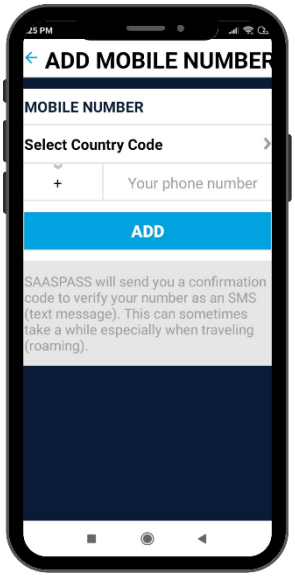


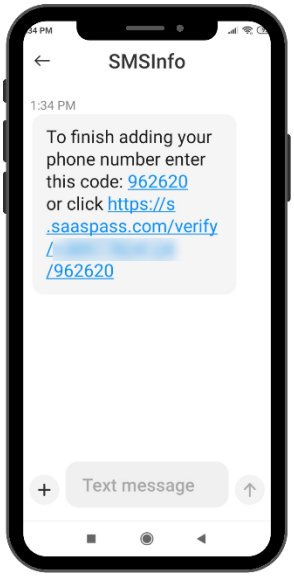


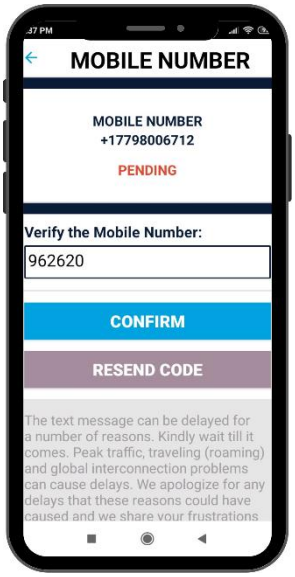


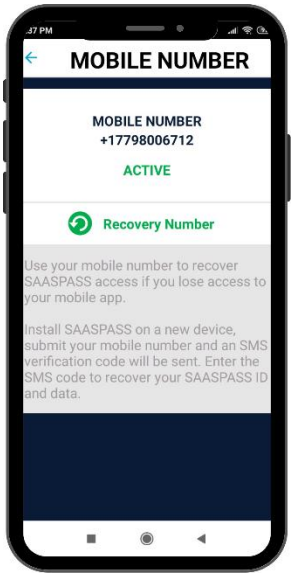












Once the recovery number is set, from the Settings icon at the top right corner of your screen, choose the option Recovery and from there you can:

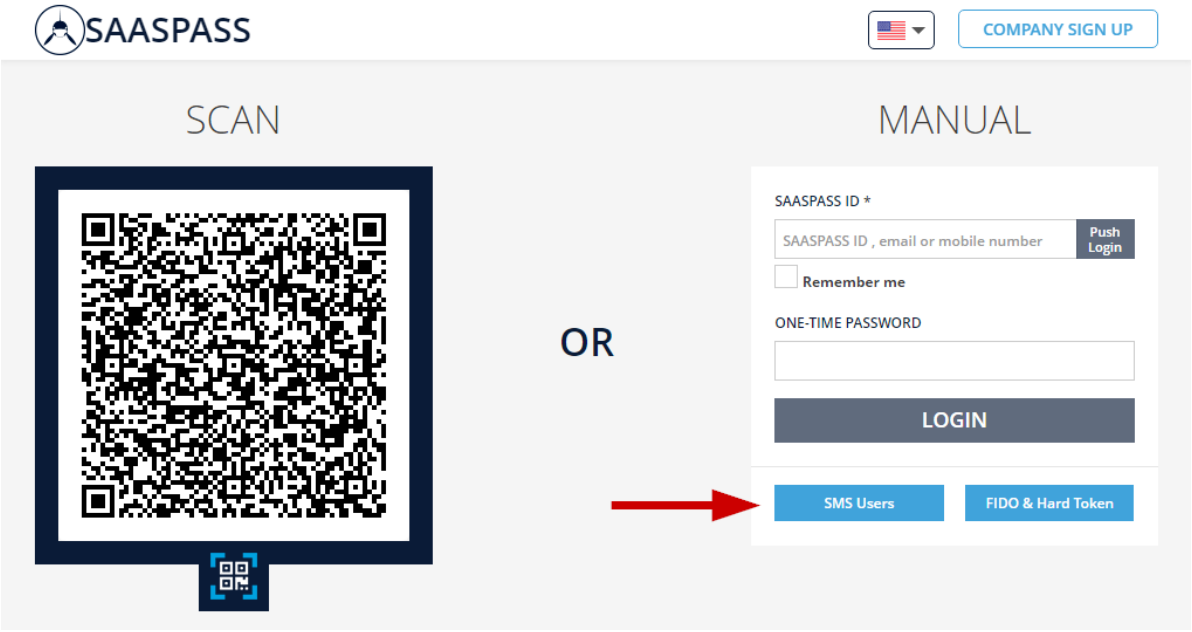
- Change the time period of 20 hours' delay for you to receive the verification code (a delay on the SMS delivery increases the security of your recovery, allowing you to contact your mobile carrier to avoid possible attacks).
- Add a customized recovery question and answer (right after the verification 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).

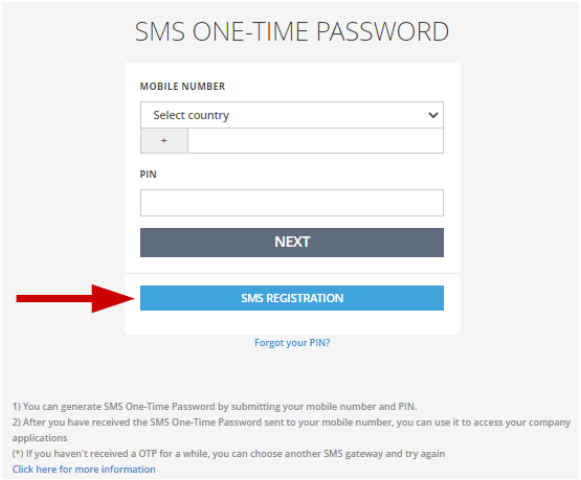
You can find more information at the Recovery Security section.

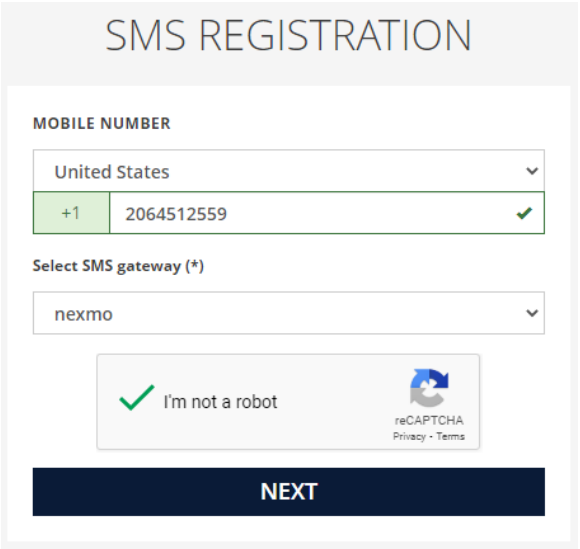
Setting Up the SAASPASS SMS User and a Recovery Option

Setting up an SMS User

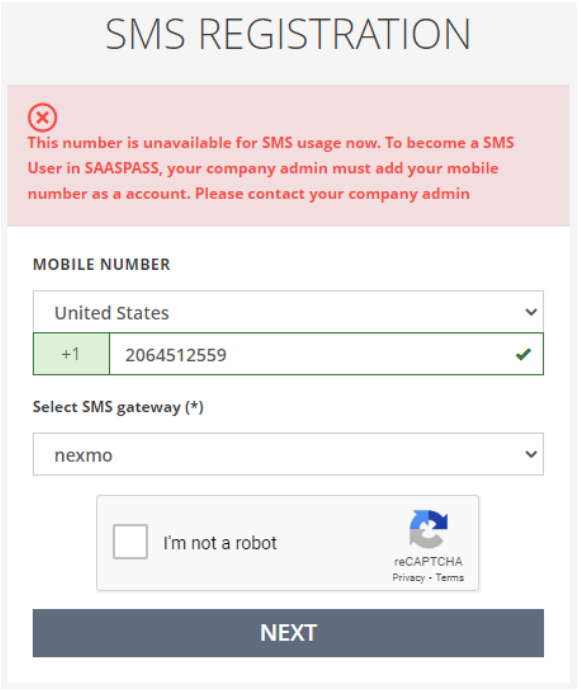
If you will be a SMS user, first what you will need to do is to register your mobile number with *SAASPASS*. To do so, go to the SAASPASS login portal and click on the SMS User button and on the next page choose the *SMS Registration* button. Choose the country and enter your phone number and click on the *Next* button.

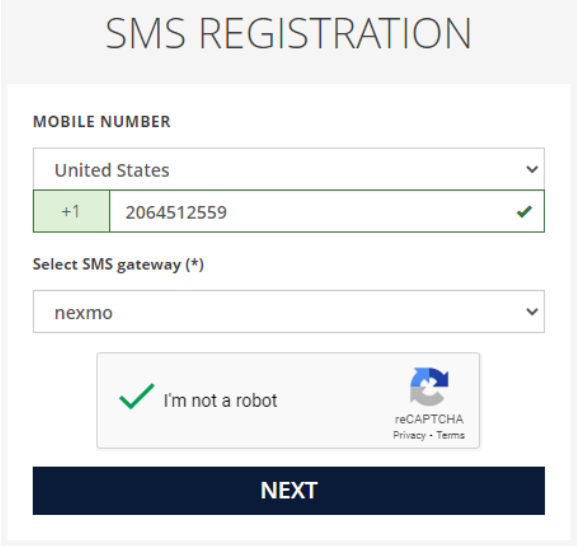




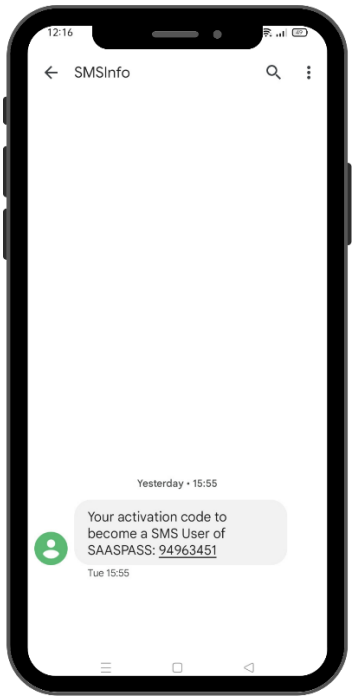


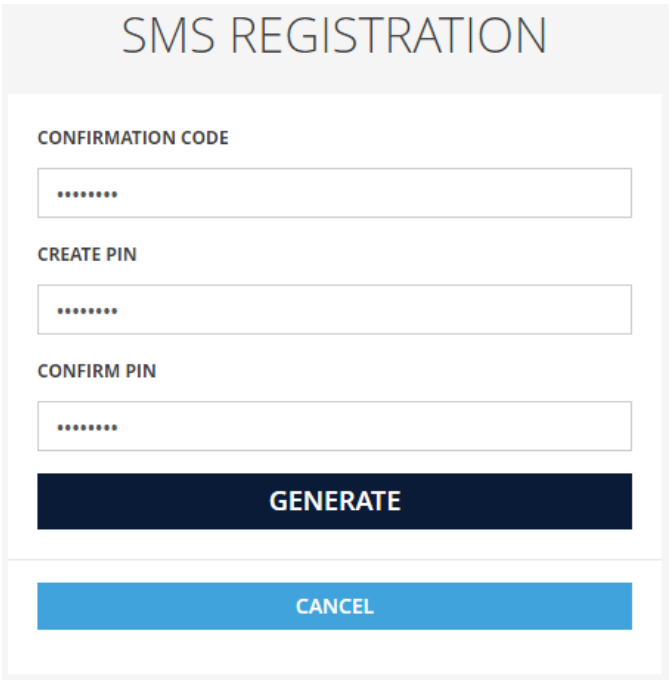
If the administrator in your company didn't register you as a SMS user, then you will get a proper error message and you will not be able to proceed with registering your phone number.





After, when you will receive the SMS on your mobile device, enter the confirmation code and create a PIN. You will need to remember the PIN because for every login, you will need to enter the PIN.

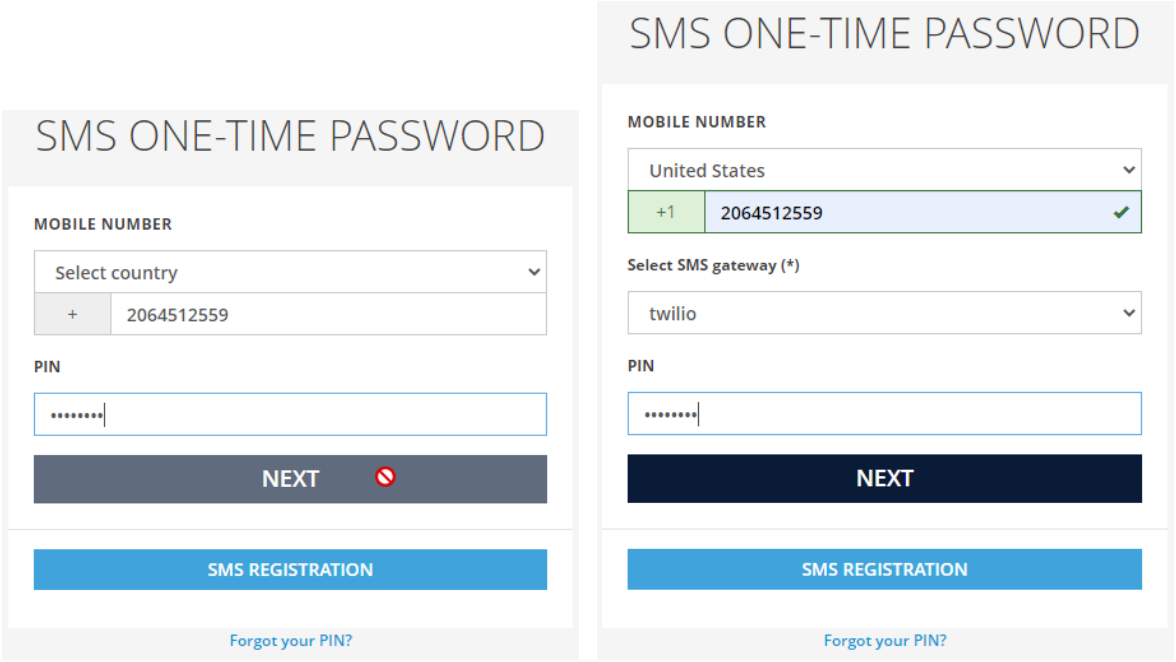




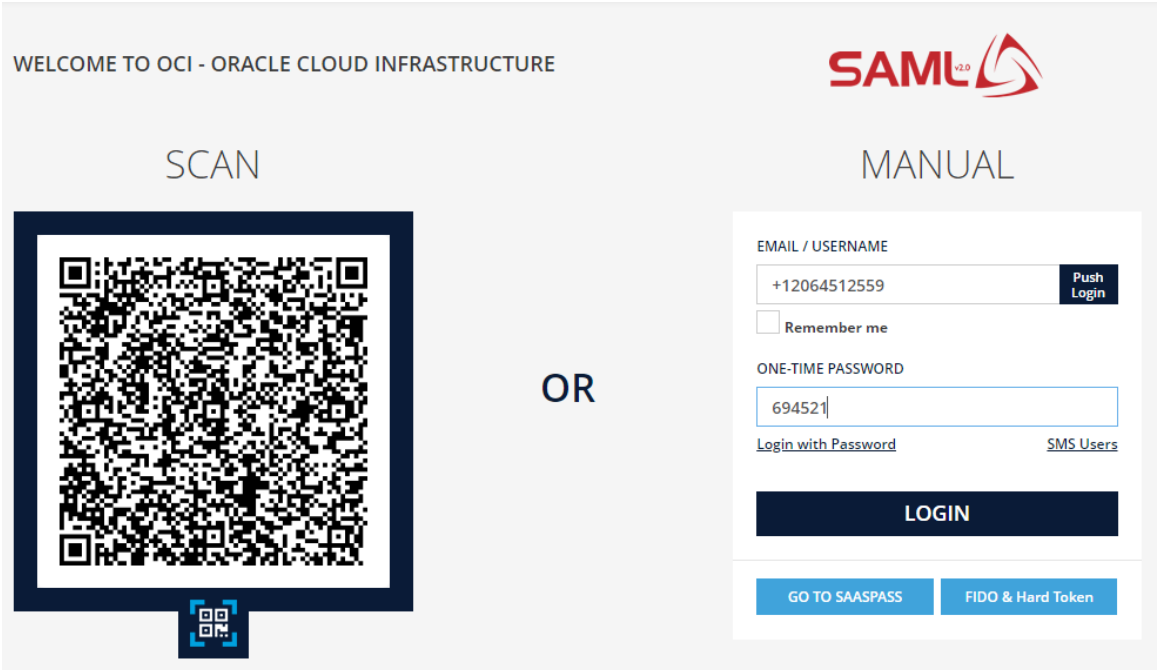
Getting an OTP by SMS

When you will need to generate an OTP, from the SAASPASS login portal, click on the *SMS User* button and from there choose your county, enter your mobile number, choose one of the SMS gateways and enter the PIN that you created in the beginning and click on the *Next* button. If the administrator did not enable your

account yet, you will not be able to proceed and a circle with a cross out line icon will appear on the *Next* button. You will receive an SMS with an OTP code that you can use for login into the End-User portal or a secure application. The OTP code is only available for 3 minutes, after which it will not be usable and thus, you will need to generate a new one if it's not input within that time period.



After you receive the SMS with the valid OTP, go back to the login page of *SAASPASS* and enter your SPID that the administrator shared with you or your phone number and then populate the field with the One Time Password.

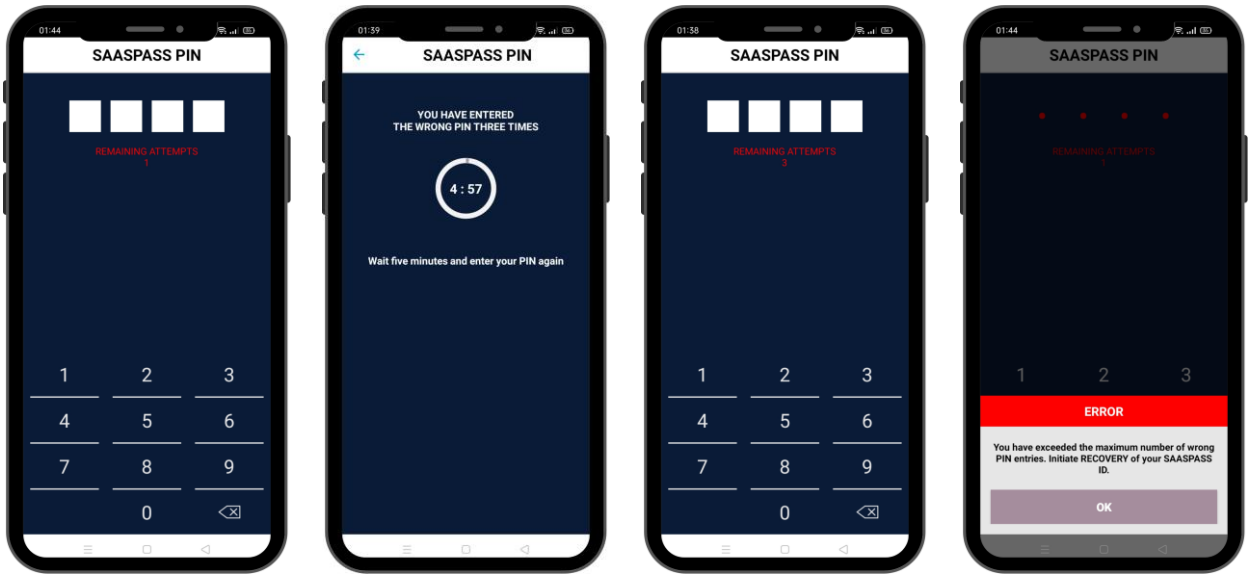


Recovery option and resetting a PIN

If by any chance you forgot your PIN, first thing what you need to do is to inform your company administrator! Your administrator will send a reset PIN code that you will get in an SMS format. After, go to the SAASPASS login portal click on the *SMS User* button and from there choose the Forgot your PIN option. Enter the Country and your mobile number, populate the Reset PIN Code field with the code that you get by SMS and create your new PIN and confirm it. At the end, click on the *Reset PIN* button and you are done.

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 PINs 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:

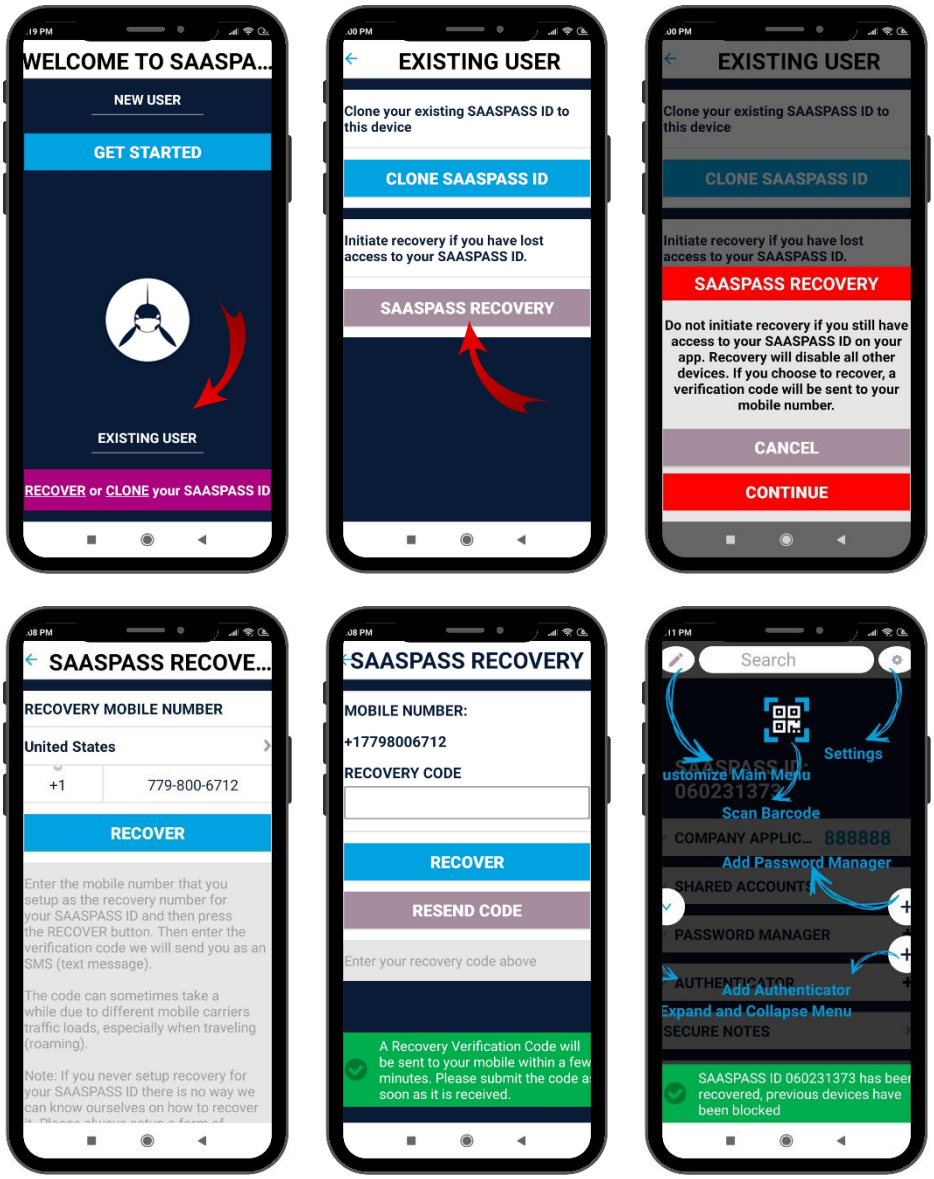
The easiest method to restore your account in the case of a lost or disabled mobile device is to initiate a *SAASPASS* Recovery. After you obtain a new device, and re-activate your original mobile number onto it, simply download a new *SAASPASS* app and select the purple button which says: *Recovery 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.

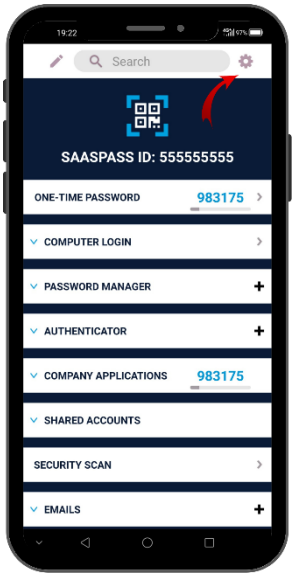
Also, after an employee initiates a recovery, access to all personal accounts will be immediately restored, but as an extra security precaution, the employee will still be blocked from all company apps and services if the administrator of that company sets that option as a rule. To be unblocked, the company admin will need to unblock the employee.

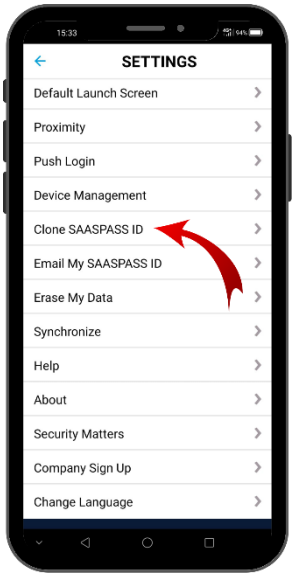
If you did not pair your account with a mobile number during initial setup, we strongly recommend you to do so now, otherwise this method of restoring your account will not be possible. Go to the "Mobile Number" section in your *SAASPASS* mobile app and add a mobile number there if you do not see one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

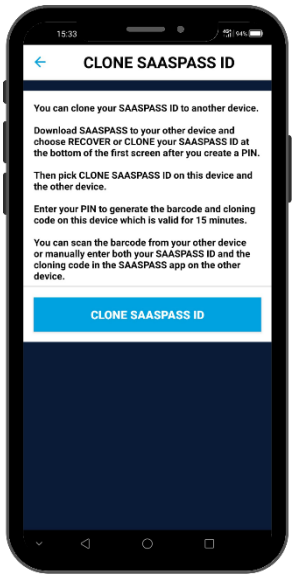


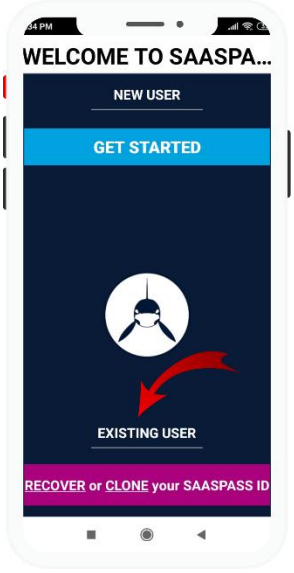
Cloning an Account

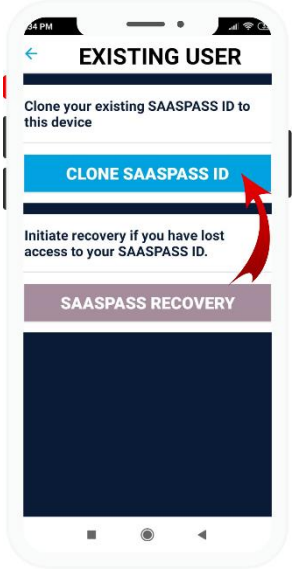
Cloning your *SAASPASS* account to a second device (or multiple devices) is another way to back up your *SAASPASS* account. Using this method, it is not necessary to have a recovery number. If you lose your primary device, the account remains on the cloned device(s) from which the account on the primary 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.

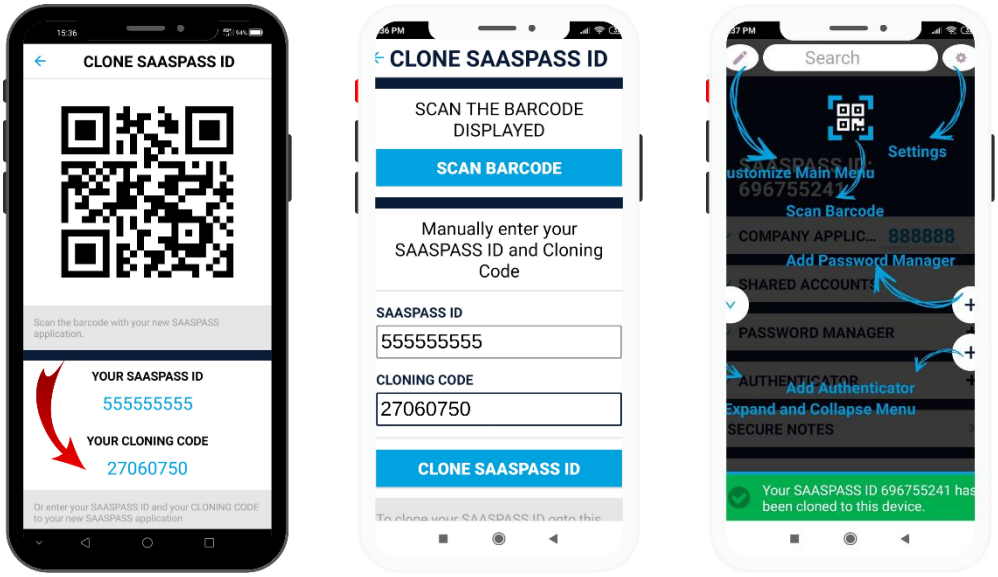












Other Methods for Temporary Account Access

If your phone is not lost or disabled but is unavailable only temporarily (i.e. you left the device at home or its battery is dead and cannot be charged), your admin may be able to allow you temporary access to your company accounts by one of the following methods:

a) The administrator of your company will provide you with emergency access MFA codes and can only be used to access your company applications or *SAASPASS* Web. The codes are time limited from the moment of issuance and can only be used within 24 hours of issuance. The codes are both sequential and time-based emergency access MFA 'One-Time Password' codes.
b) Removing *SAASPASS* protection from select computers and apps so that you can simply login with your username and password into your working machine.
c) Issuing you a hard token or extra mobile device then temporarily assigning all of your company apps to the SPID associated with that hard token or spare 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. Your admin can reassign all of your company accounts to your new *SAASPASS* ID, but 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. For 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?

1. Your company's admin can only manage the apps for which they provision you. Your personal apps that you add, on the other hand, are entirely invisible to the admin. Although, sometimes there will be a need for you to share credential that you create and for that purpose the administrator will grant you the right to do so. The sharing personal credentials can be done only from the End-User Portal under the Shared Accounts tab.

2. *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*.

The SAASPASS Experience

SAASPASS features can be used partially or individually, but when the product is used in entirety, the full *SAASPASS* employee user experience could look something like in this example:

Bob works at XYZ Company. Each morning, he arrives at the office, opens his *SAASPASS* app in his mobile device, types his PIN code into the app, then uses the app to scan the barcode on the login screen of his desktop computer. Without typing in any usernames or passwords, and without having to manually enter dynamic passcodes off a token, he is now automatically logged into his computer as well as a desktop client (single sign-on console) at the top of his computer screen. Bob has securely verified his identity using strong multi-factor authentication and all he had to do was sign into his mobile app and scan a barcode on his computer (or login using another method such as the Bluetooth feature that initiates login when it senses Bob's proximity).

Next, by clicking the single sign-on console at the top of the desktop screen, a list of all Bob's company applications (i.e. Salesforce, Office 365, Dropbox, etc.) and personal websites (Facebook, Amazon, Wells Fargo) is displayed. If he clicks on the names of any of these applications or websites, again, he will be automatically signed in without ever having to type in any usernames, passwords, or dynamic passcodes. Bob can easily lock down everything with a single button when he leaves his desk for lunch, then quickly log back in and resume work when he returns. And none of Bob's personal websites can be managed, accessed, or even seen by Alice, Bob's company administrator. Alice sees only the company applications for which she provisioned him.

Bob returns home after a relaxing password less day at the office and opens his personal laptop. Using the same *SAASPASS* mobile app (always free and unlimited for personal use), he is able to login to his personal computer and securely access all of his company and personal apps without every typing in a username or password or dynamic passcode.

In his free time, Bob is planning a vacation and needs to purchase an airline ticket, so with a single click he logs into the website of his favorite airline, Killer Whale Airways. To complete the purchase, he needs to enter his credit card info and passport number, but both his passport and credit cards are in the other room. Fortunately, Bob has saved his passport details, credit card info, and other sensitive info in the SECURE NOTES section of his *SAASPASS* mobile app. By clicking SECURE NOTES, then retyping his PIN as an extra layer of security, he is able to quickly and securely access all of the sensitive information he has stored there so that he can complete his purchase.

Bob now needs to set up an online account for the hotel where he will stay during his vacation, the Grand Orca Hotel. The hotel's website supports *SAASPASS* registration (as well as Facebook, Twitter, and other social login options), so from the *SAASPASS* mobile app Bob selects one of his *SAASPASS* PROFILES to autofill and complete the registration application.

He also needs to create a strong password for the Grand Orca's website, so he goes to PASSWORD GENERATOR in the *SAASPASS* app where he generates a strong password with the desired number of digits and symbols, then automatically copies and pastes it into his PASSWORD MANAGER, where he adds the hotel website and his username for the site. Now Bob has one-click access from all his synced devices to the online account he has with the hotel.

The same level of security and convenience is also applied within the mobile device itself. After Bob closes his computer, he remembers that he had needed to check his bank balance. From the phone, and within the AUTHENTICATOR section of the *SAASPASS* app, Bob clicks on 'Bank of the Sea'--the name of Bob's bank. Suddenly, Bob's username and password are auto-filled within the phone's browser, then a dynamic passcode also auto-fills, and Bob is automatically logged in.

While on vacation, Bob will still need to check emails and do some limited work, so before leaving, he will clone his *SAASPASS* ID onto his iPad as a convenient backup in case he loses his phone or drops it in the ocean. Even on his whale watching cruise, with no Internet connection, Bob will be able to use proximity or manual login to access any files on his laptop securely.

But Bob's vacation is still days away. For now, with his personal tasks completed, it's time for bed. Bob logs out and sleeps the sleep of the saved and thankful.

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 its own End-User Portal and it doesn't matter if the SPID belongs to a company user or it is a personal one. The End-User Portal is unique and personal to every user, no other SPID has access to it. Every time, when you will login into *SAASPASS* the first thing where you are redirected is the End-User Portal, from there, you can manage your personal credentials, SSO into the company and personal applications, if you are a company administrator, you can switch into the company mode. In the following section all capabilities are explained for a mobile app, hard token or a SMS user.

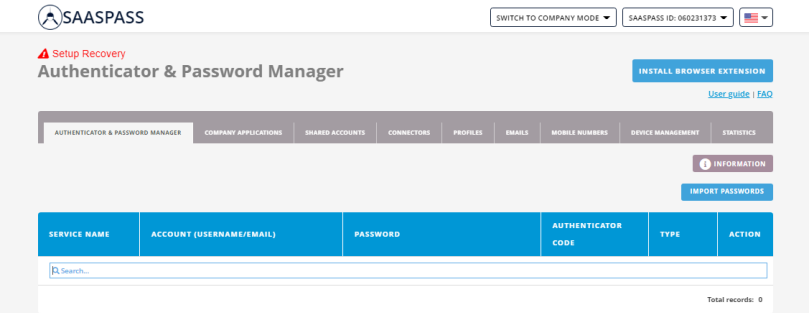
AUTHENTICATOR & PASSWORD MANAGER

Mobile app Users

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.

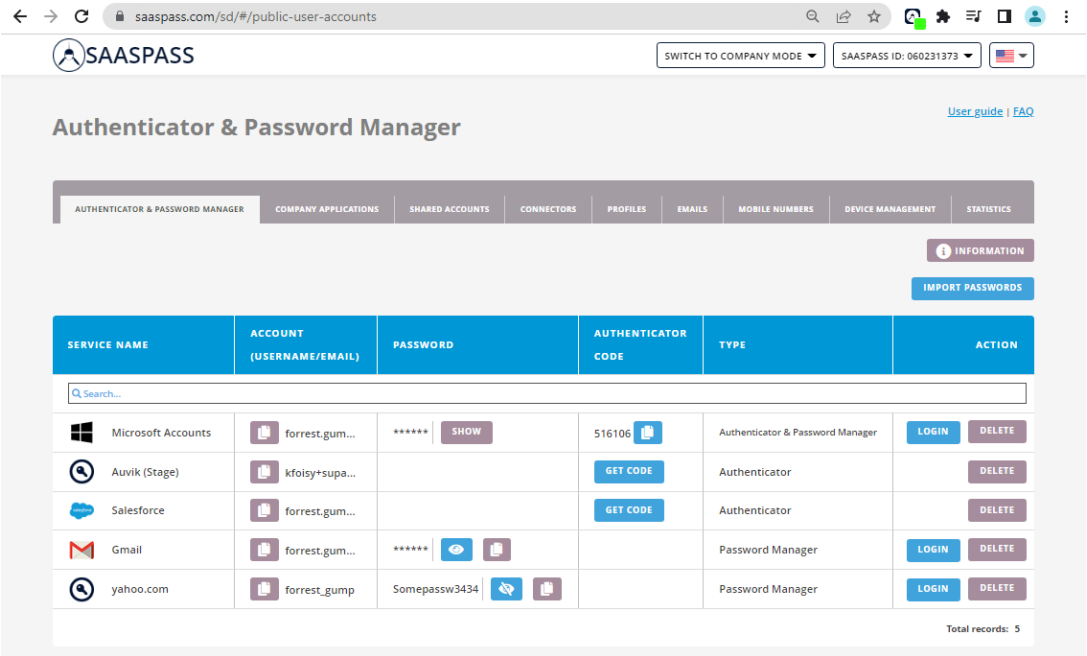
You can download the extension directly from the End-User Portal or from the *SAASPASS* web site from the Download page.



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 authenticators/password managers, the view will be similar to the picture below.



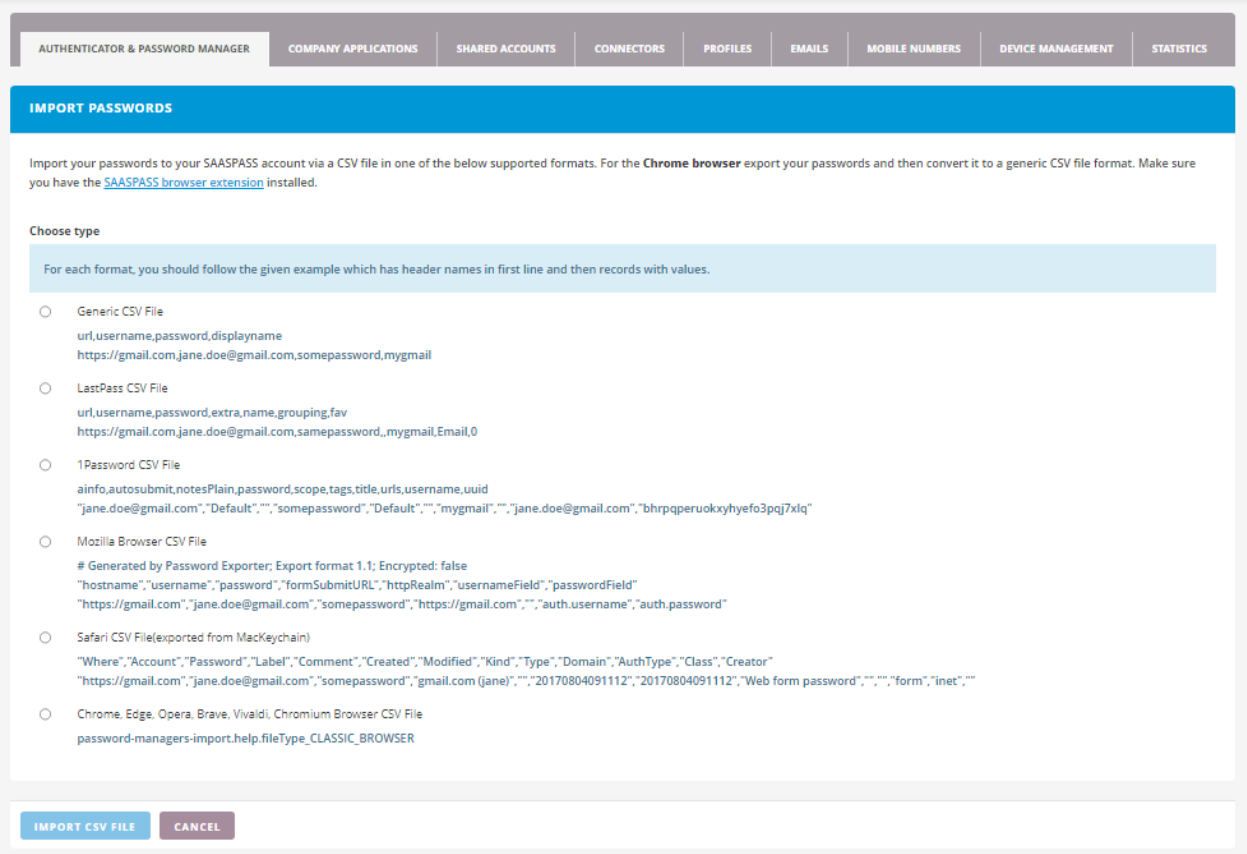
Import Passwords

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

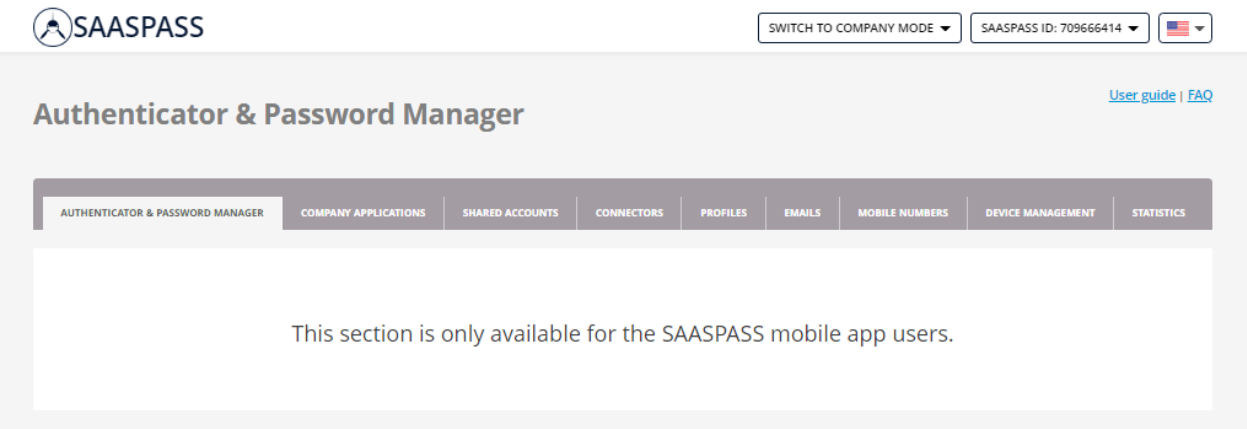
https://gmail.com,jane.doe@gmail.com,somepassword,mygmail

https://login.salesforce.com/, forrest.gump@popcornfly.com,Forres.GumP2022,Salesforce



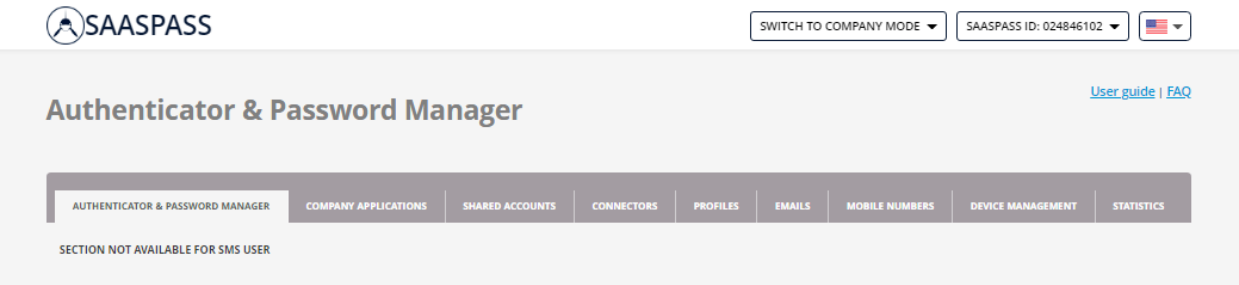
Hard Token Users

The Hard Token users don't have access to the Authenticator and Password Manager tab. With that being said, the personal perimeter for those users is not allowed and only users who are company users, can be Hard Token users.



SMS Users

The SMS users don't have access to the Authenticator and Password Manager tab. That being said, the personal perimeter for those users is not allowed and only users which can be SMS users are the company users.



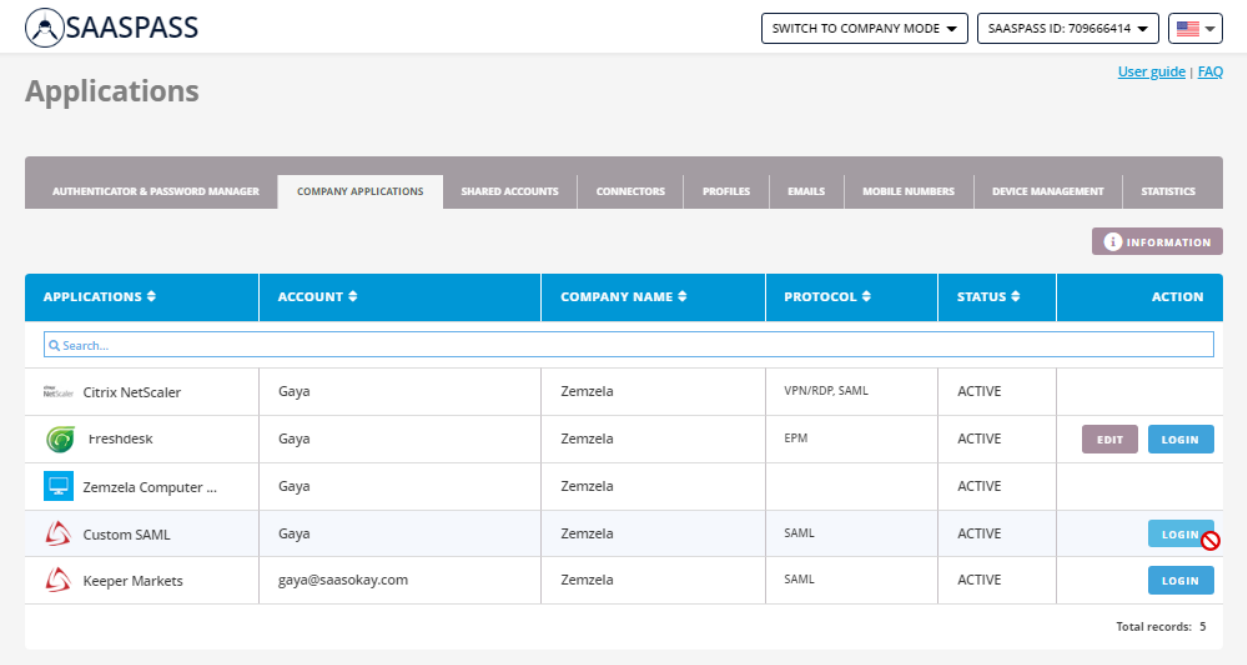
COMPANY APPLICATIONS

This section is available for all types of company users, if your company is using *SAASPASS* for secure access to applications and an active enterprise password manager.

This section is available for all types of company users, and all things said applies to all SMS, Hard token and mobile app users.

In the table, you can see the name of the secure application, account of the user which is assigned to that application, company that assigned that application to the user, the protocol of the application and actions that can be taken for that application.

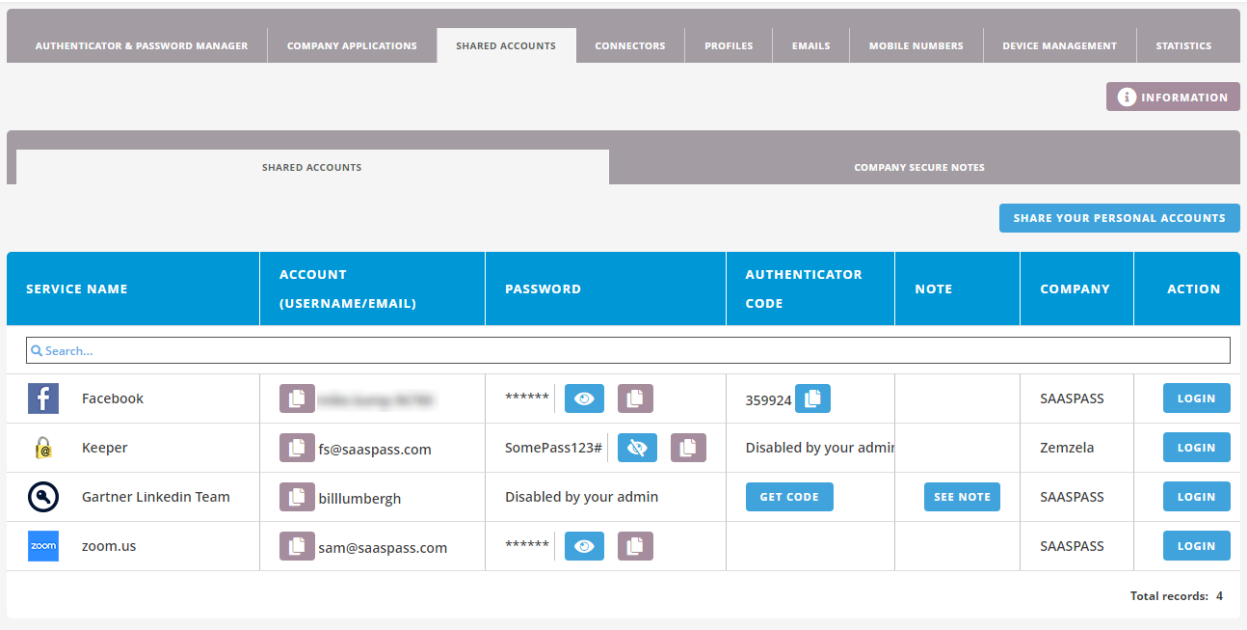
If the application login button is not clickable, that means that the application is currently unavailable. The applications which don't have a Login button, are those which have their SSO option disabled by the administrator of the company. The Edit button means that that application allows the password to be set or changed from there.



SHARED ACCOUNTS

This section is available for all types of company users and you need to install the browser extension for shared accounts to work.

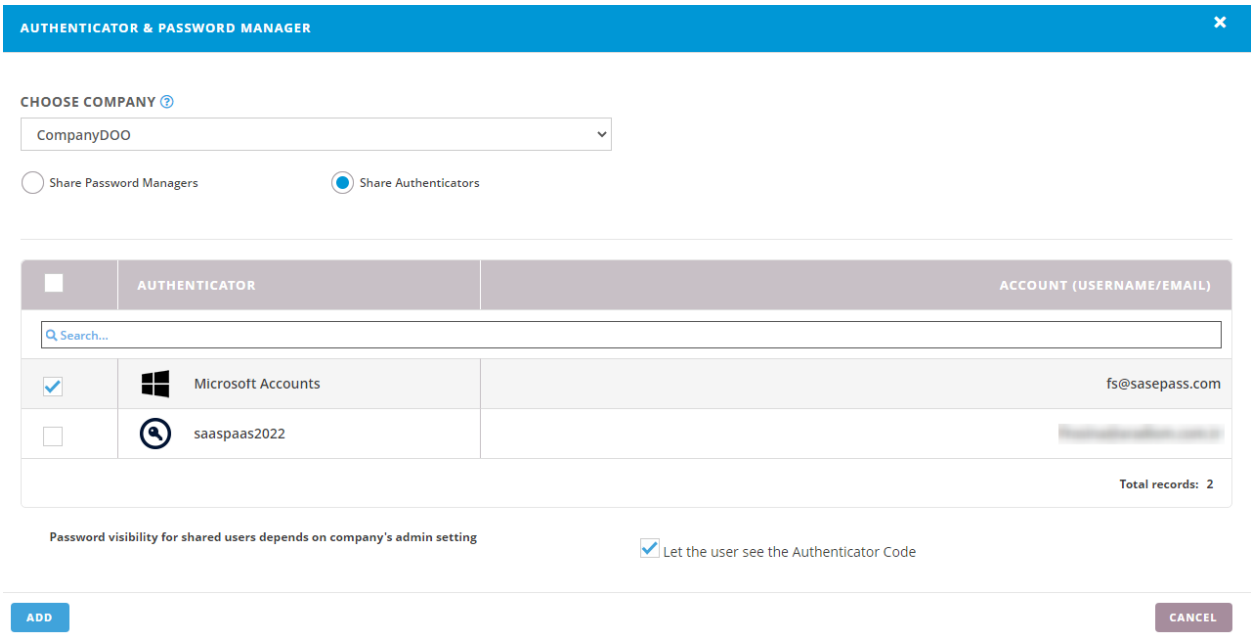
This is where a company has shared access with you to services - with or without sharing passwords and/or authenticator codes. This means that multiple users can have access into a service with a single credential.

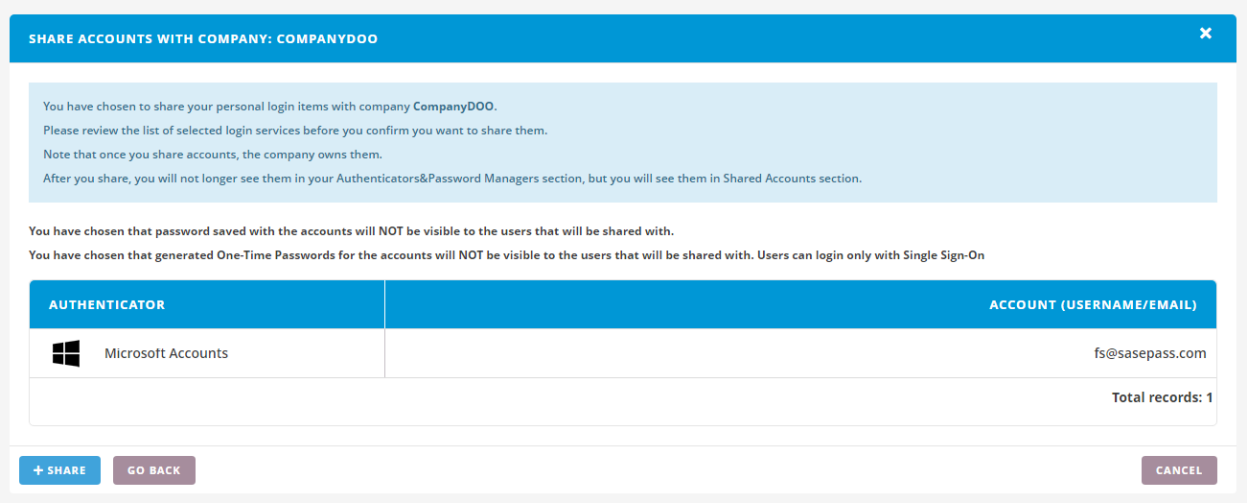


From the Shared Accounts section, you can see the name of the service shared with you, the account that shared that application, the password of the application which can be visible or disabled by the

administrator, the authenticator code if the shared service is an authenticator type and if the admin allowed that, the notes for that app if they are available, the company that is sharing that app with you and the Login button for that application.

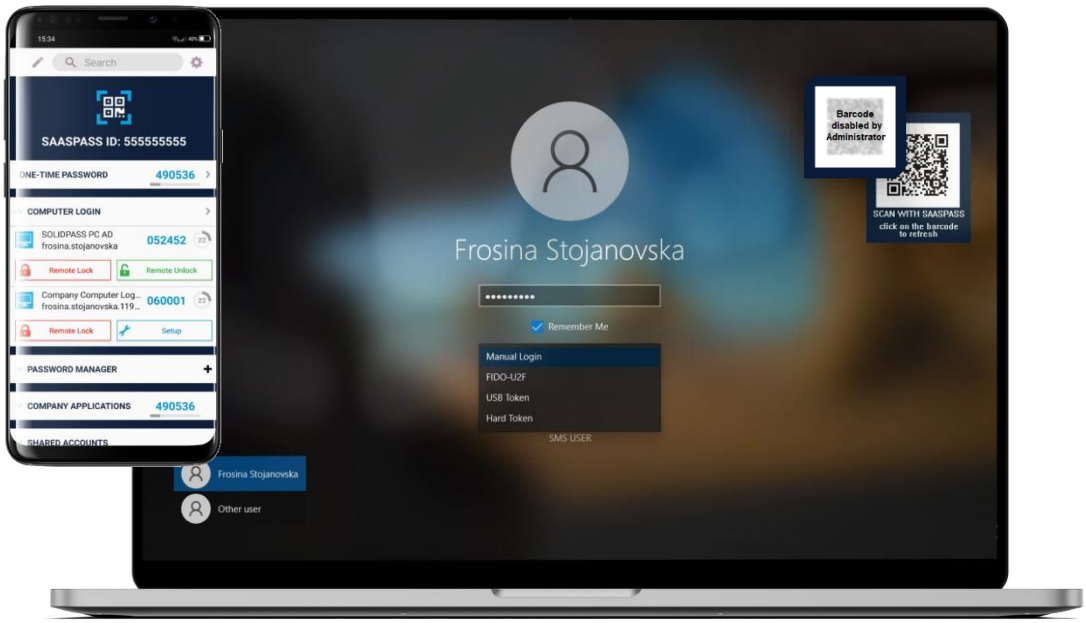
From here, If the administrator has allowed you, you can share your personal credentials with the company only if you are a mobile user, since the Hard Token and SMS users don't have access to the personal perimeter. If this option is available, you will see a blue button “Share Your Personal Accounts” above the table. By clicking on the button, you will be redirected to a form from where you need to choose with which company you want to share the credentials, choose the type (Authenticator or Password Manager) and select the desired services. After doing that, depending on the admin settings you can choose the preferences for visibility of the credentials and click on the Add button. Lastly, you can review the credentials that you want to share, and by clicking on the Share button, you actually will share your personal credential. After you share, you will no longer see them in your Authenticators & Password Managers section, but you will see them in the “Shared Accounts” section. That means that they will no longer belong to you, instead they will belong to the company and the administrator of that company will be the only one who can manage them in the future.





CONNECTORS

SAASPASS offers two types of Computer Protection, personal and company protection. If a local user account is already protected with *SAASPASS* as personal protection, this account cannot be switched to Computer Protection with AD. It is recommended that you remove the personal protection first and later add Computer Protection. However, if a local user uses personal protection in their own machine, and there is a need for the same SPID to be bound with Computer Protection on a working machine which is not AD connected, in that case this option is available.



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.

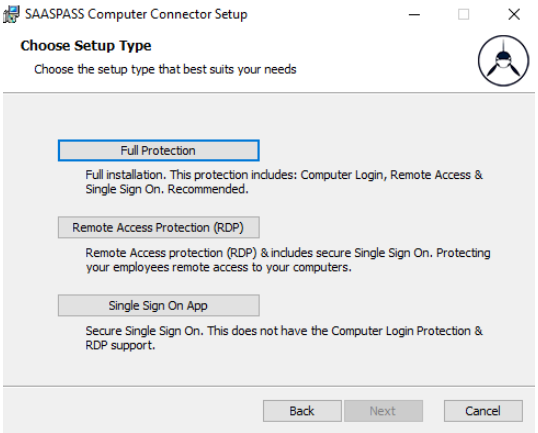
The Computer Protection can be used in offline mode as well. It is required at least once for the user to login with OTP while an internet connection is available and after, they can use the offline mode of authentication with a one-time password.

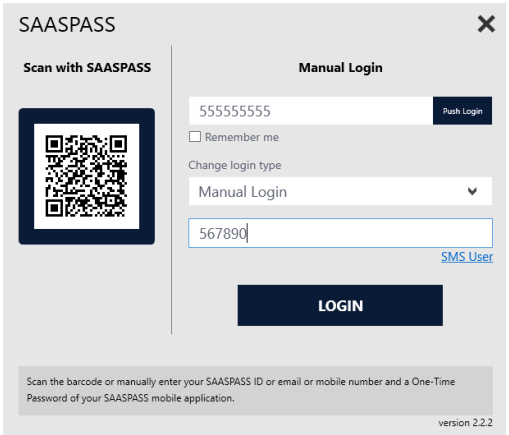
Before installation, ensure that your firewalls or VPNs will not interfere with *SAASPASS* connections. There are some Antivirus programs (such as Avast) that may treat *SAASPASS* as a threat and may not allow the full installation of *SAASPASS* Computer Connector. In such cases we strongly recommend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

WARNING: If your Computer is a domain bound/Active Directory Company computer, please make sure your admin has signed up as a Company for *SAASPASS*. 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.

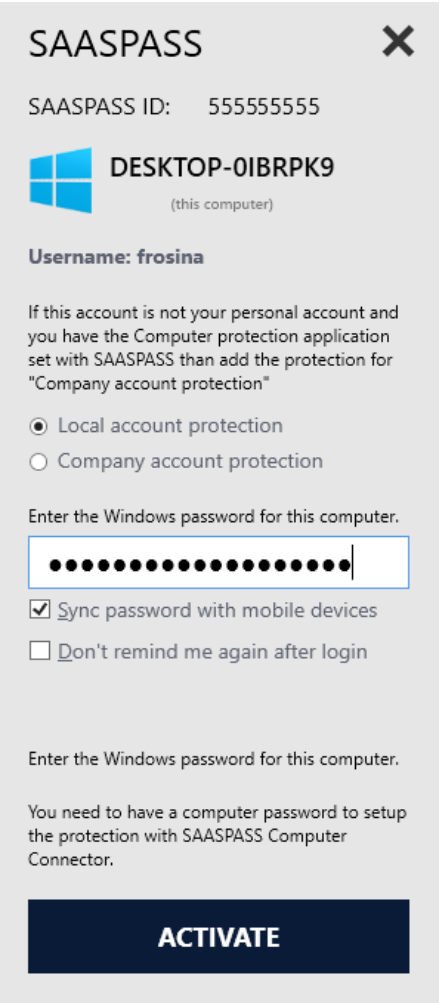
Personal Users

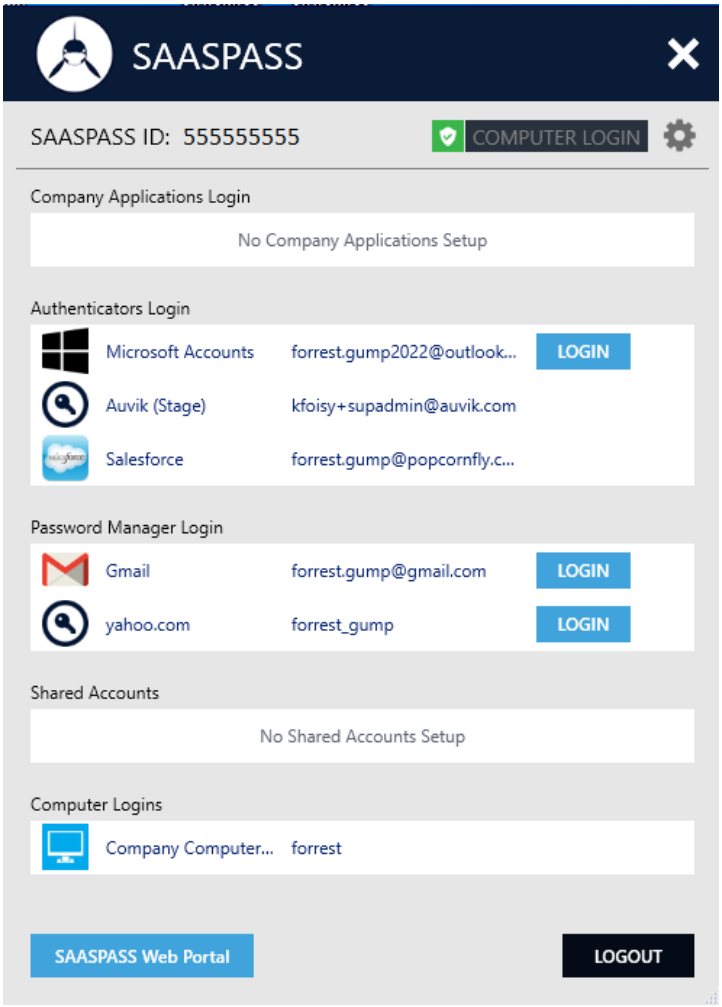
Go to the End-User Portal or to the *SAASPASS* web site where there is the Download page and download the matching version. Open the package and follow the installation wizard, when you will need to choose the setup type, we recommend choosing the Full Protection option. After the installation process 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.





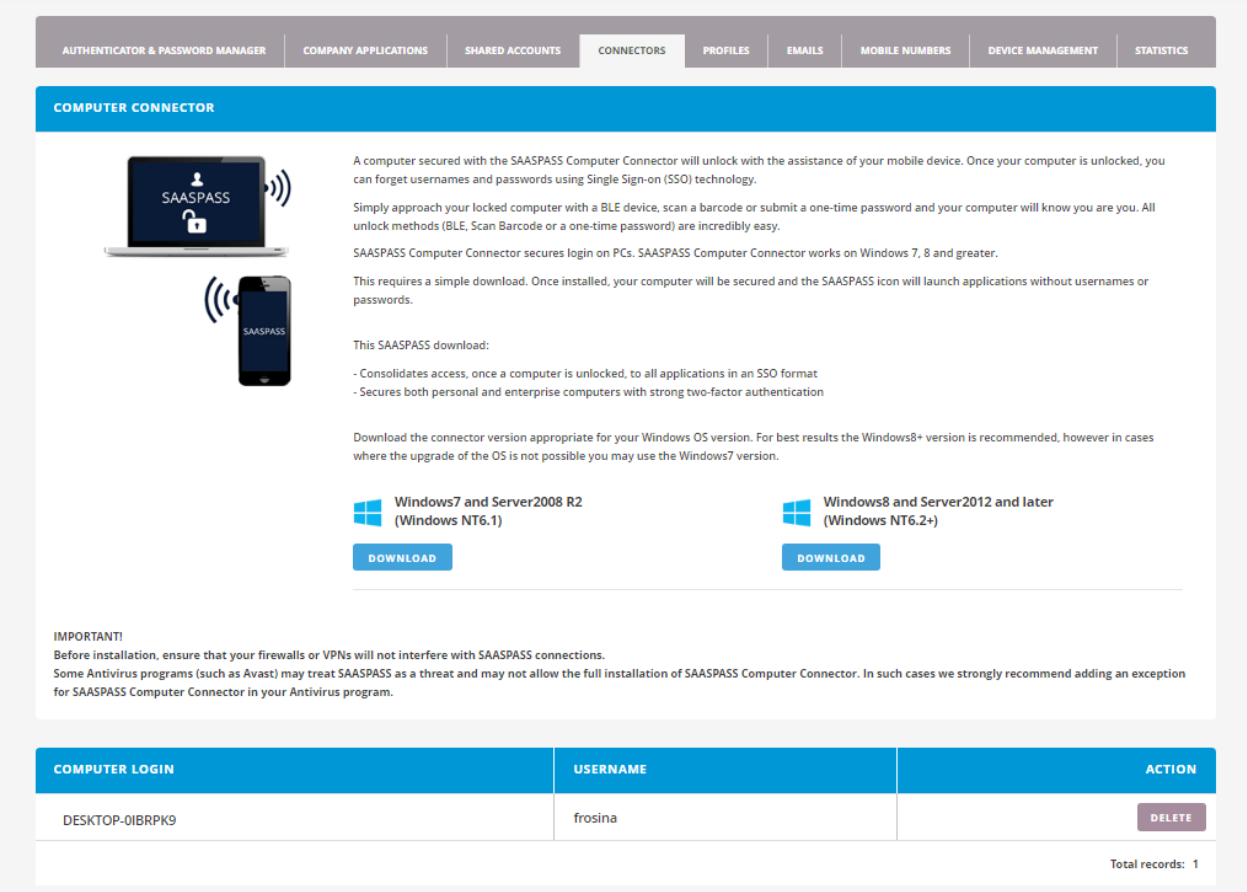
Next, from the opened form, choose Local account protection, fill in the Windows password for the computer and check the box for password synchronization with the *SAASPASS* mobile app. After doing that, click on the *Activate* button and then the *Finish* button.





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



Company Users

If your company decides to use the *SAASPASS* Computer Protection, then, the administrator will provide you with documentation with all the necessary information and needed instructions for initiating setting it up and using the computer protection. This type of protection is available for all types of users.

PROFILES

Mobile app Users

Profiles are used to register and login instantly to applications that support *SAASPASS*. While the only mandatory fields are name and email address, expanding these profiles can streamline Instant Registration submissions with sites, forms and applications.

When you login to an application using the *SAASPASS* Connect button or use instant registration for an application, the default profile will be used automatically and its data will be shared with your application provider.

Hard Token Users

This section is not available for Hard Token users and is only available for the SAASPASS mobile app users.

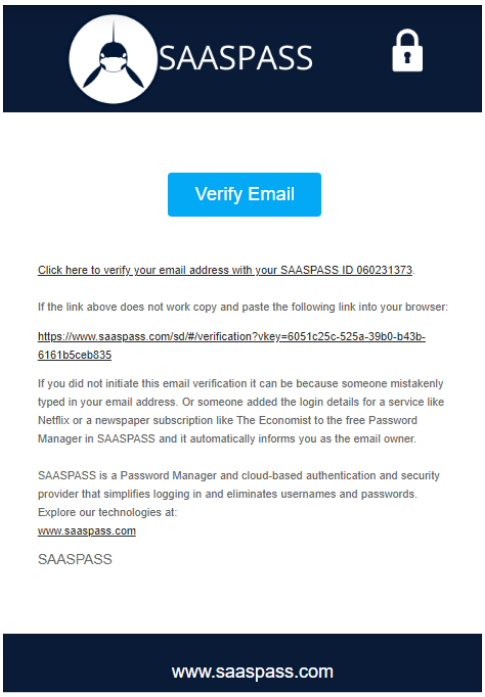
SMS Users

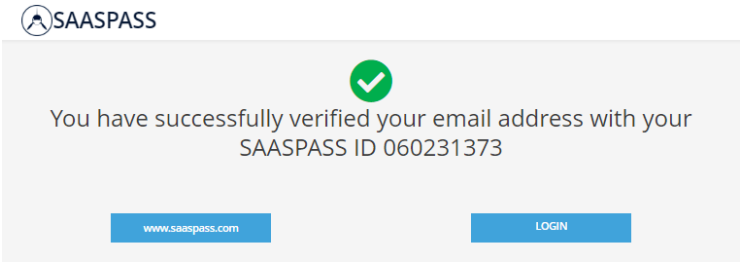
This section is not available for SMS users and is only available for the SAASPASS mobile app users.

EMAILS

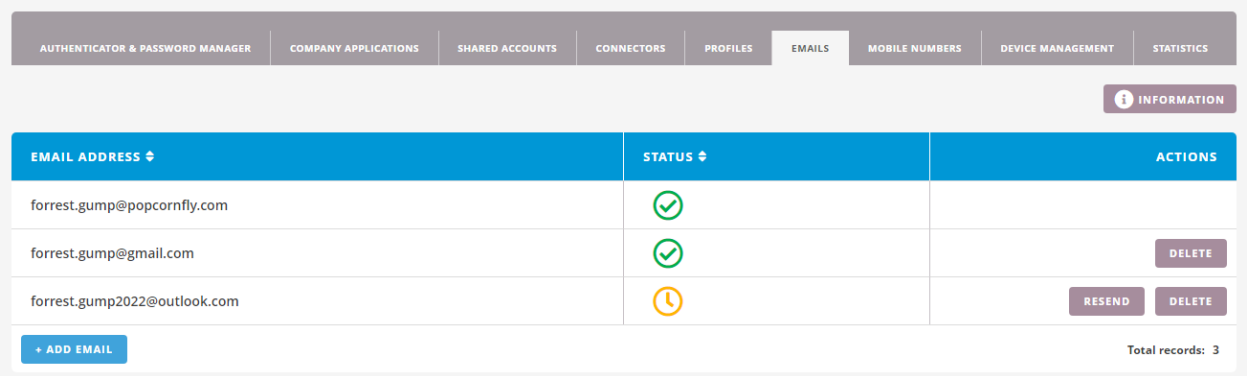
Mobile app Users

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.





Also, whenever the administrator assignee a new user account with your SPID, the email will be shown here. The company emails, that are bonded with some of the Secure applications cannot be deleted.



Hard toke Users

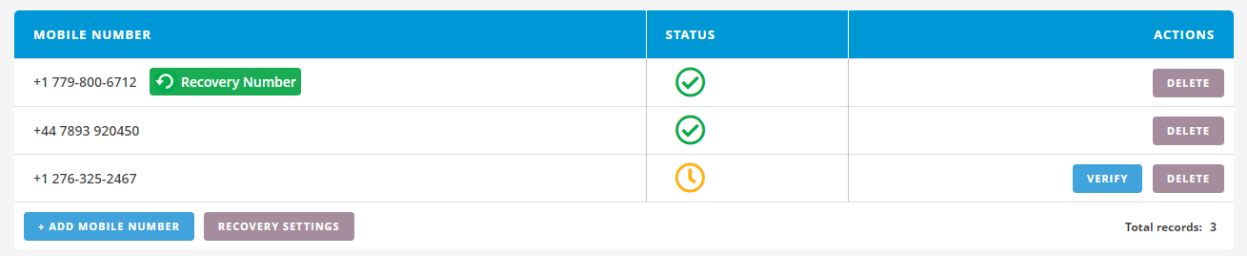
This section is not available for Hard Token users and is only available for the *SAASPASS* mobile app users.

SMS Users

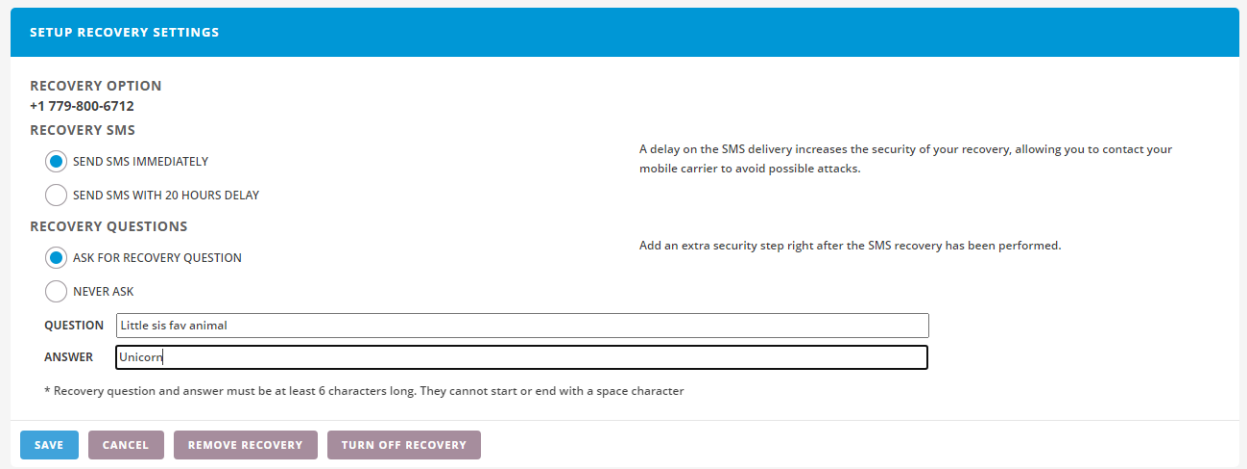
This section is not available for SMS users and is only available for the *SAASPASS* mobile app users.

MOBILE NUMBERS

Mobile app Users



In this section, you can change your Recovery Settings. 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.



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.

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.

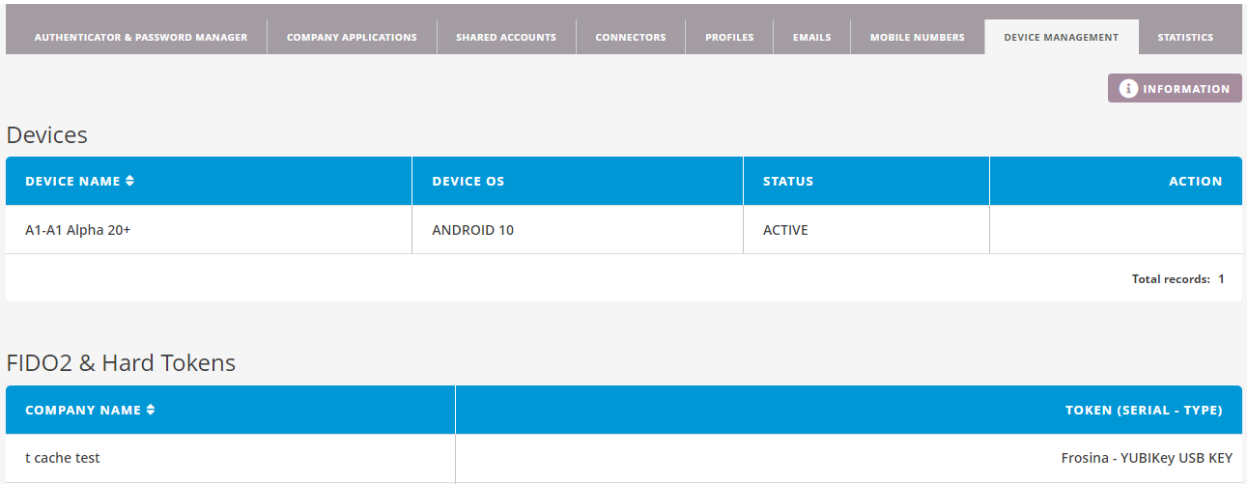
Hard toke Users

This section is not available for Hard Token users and is only available for the *SAASPASS* mobile app users.

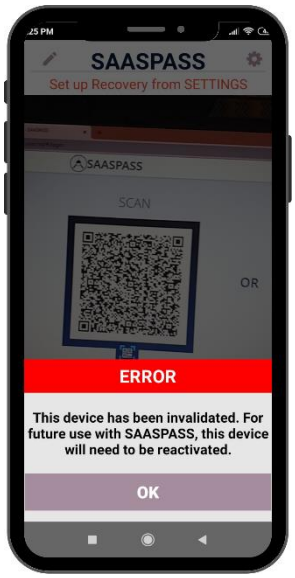
DEVICE MANAGEMENT

Mobile app Users

The same *SAASPASS* ID can be used across multiple devices. Download the *SAASPASS* mobile app on a new device, navigate to the 'gear' icon and choose “Clone SAASPASS ID”. Active devices will be shown listed here.



You can find out more about cloning *SAASPASS* in the Cloning an Account section.



If you delete a device that 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

For any questions, you can always contact us at:

support@saaspass.com