



Hard Token Key Revoke and Backup

SAASPASS

SAASPASS HARD TOKEN(KEY) REVOKE AND BACKUP

As revoking a key in the event that it is lost, stolen, or broken and using a backup key in the event that the primary key is not available are important concerns when using hard tokens, SAASPASS provides support for both. Revoke key and Backup key methods in SAASPASS are both using the concepts of user accounts assignment and reassignment to a hard token/SAASPASS ID. To better understand how to use these methods in SAASPASS, it is recommended that you read the [Appendix 1](#) in this document that explains how to assign user accounts to hard tokens. In SAASPASS each added hard token(key) is automatically assigned with a unique SAASPASS ID. This ID can be found in the "Hard Token Management" section and used in the assignment/reassignment of user accounts to the tokens/keys.

REVOKE KEY

All keys can be revoked anytime if the admin wants. In case the hard token device is lost, stolen or broken, meaning that the user will not use it any longer, the admin of the company can log into the SAASPASS Admin portal and delete that key. Admin can temporarily revoke the key by adding another key to the user. Keys can also be reassigned to other user accounts from the admin portal.

Temporary Revoke

Temporary Revoke method is preferable when the user temporarily doesn't have access to the hard token which they expect to regain possession of. Therefore, until this hard token is not accessible for the user, the admin can temporarily revoke it.

Temporary Revoke is performed by removing the assignment of the user accounts to the hard token/SAASPASS ID - and in addition assigning these user accounts to another token/key (another SAASPASS ID).

Follow the steps below to perform a temporary revoke of the hard token/key which has user account/s assigned to it:

- Find your hard tokens/keys in the tokens table under the "FIDO & Hard Tokens" management section as shown in Image 1.
 - Here, the admin can check the serial number of the token/key that they want to revoke. Example, the token to be revoked has SAASPASS ID - 663459512 and is with "ACTIVE" status because it has user account/s assigned to it.

- Admin should make sure that there is another token/key created that will be used as a new hard token for the same user account once the previous one is revoked. For example, the new hard token has ID 115584831 and is with "No account assigned" status because it still doesn't have a user account/s assigned to it.

| SERIAL NUMBER | TYPE | STATUS | SAASPASS USER | ACTIONS |
|---------------|------------------------|---------------------------------|---------------|---------------|
| Yubico Test | YubiKey USB (non FIDO) | ACTIVE Has assigned accounts | 663459512 | MANAGE DELETE |
| Yubico | YubiKey USB (non FIDO) | ACTIVE No account assigned | 115584831 | MANAGE DELETE |
| 5313745 | HOTP USB Key | ACTIVE No account assigned | 024421774 | MANAGE DELETE |

Image 1: Find the hard token that will be revoked and create a new one.

- Select and COPY the SAASPASS ID associated with the hard token/key that is with status "No account assigned".
- Go to the "User Directories" section and search for the hard token that you want to revoke (in our example it is 663459512).

| USER ACCOUNT | DIRECTORY | SAASPASS USER |
|--------------------|--------------------|---------------|
| ismar@saasokay.com | SAASPASS Directory | 663459512 |
| ismar | SAASPASS Directory | |

Image 2: Find the hard token to be revoked.

- Now, click on the user account to open the "User Account Details" window.
- Next click on the *Change Owner* button as shown in Image 3.

Important Note: You need to remove the owner of this account if you do not want to assign this user account to any other token. You can do this by using the *Remove Owner* button that you can find under the *Change Owner* button.

ACCOUNT: ismar@saasokay.com

ACCOUNT IS VERIFIED FOR THIS SAASPASS USER: 663459512

YOU CAN CHANGE OWNER OF ACCOUNT TO BE ANOTHER SAASPASS USER

CHANGE OWNER

YOU CAN REMOVE THE OWNERSHIP TO MAKE ACCOUNT PENDING FOR VERIFICATION

REMOVE OWNER

Image 3: Change owner.

- Then PASTE the SAASPASS ID in the Account Verification entry field. Next, click on the *Search* button as shown in Image 4.

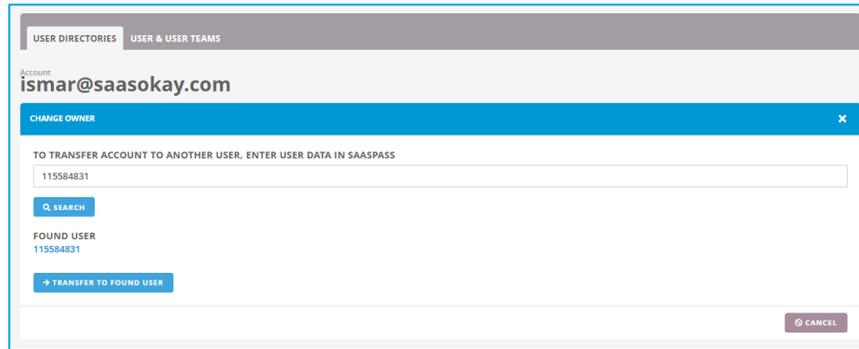


Image 4: Find an a user account.

- Once the user/token/key is found, click on the *Transfer to Found User* button.
- A pop up window will show up from where you will need to confirm your choice as shown in image 5.

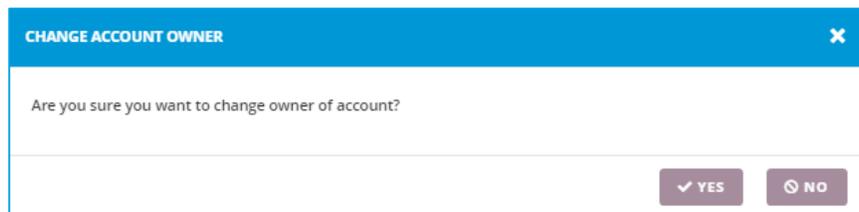


Image 5: Confirmation for changing account owner.

- You should receive a message that the verification has been done successfully, as shown in Image 6.

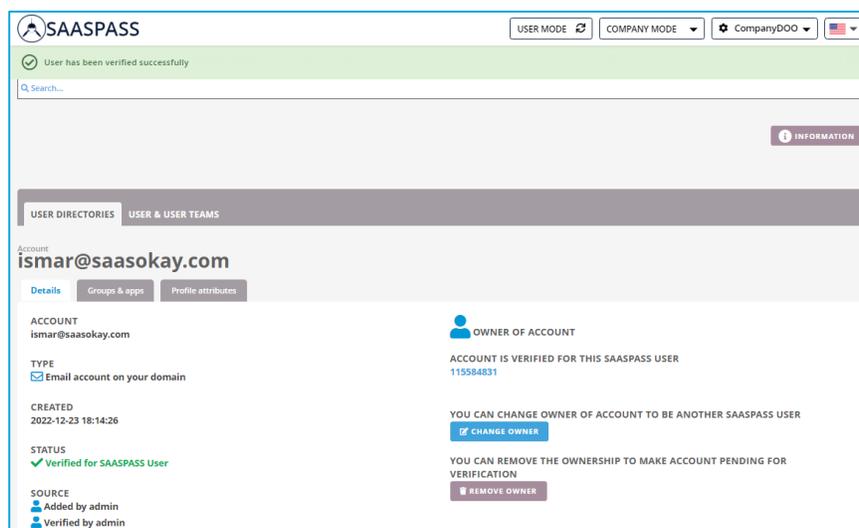


Image 6: Successful verification completed.

- Now, the previous hard token with SAASPASS ID 663459512 is revoked and the user account "ismar@saasokay.com" is now assigned to the new hard token that has SAASPASS ID 115584831 (Image 7). Do the previous steps to all the user accounts that are assigned to the token/key that the admin wants to revoke.

| USER ACCOUNT | DIRECTORY | SAASPASS USER |
|---|--------------------|---------------|
| <input type="checkbox"/> ismar@saasokay.com | SAASPASS Directory | 115584831 |
| <input type="checkbox"/> Ismar | SAASPASS Directory | 115584831 |

Image 7: User Account assigned to new hard token.

- Now, find your new hard token and the revoked one in the tokens table under the "FIDO & Hard Tokens" management section as shown in Image 8.
 - As a result, the revoked hard token that had SAASPASS ID 663459512 no longer has the "ACTIVE" status since the user account assigned to it was removed.
 - The new hard token that has SAASPASS ID 115584831 now has "ACTIVE" status because it has the user account assigned to it.

| SERIAL NUMBER | TYPE | STATUS | SAASPASS USER | ACTIONS |
|---------------|------------------------|---------------------------------|---------------|---------------|
| Yubico Test | YubiKey USB (non FIDO) | ACTIVE No account assigned | 663459512 | MANAGE DELETE |
| Yubico | YubiKey USB (non FIDO) | ACTIVE Has assigned accounts | 115584831 | MANAGE DELETE |

Image 8: Find the new hard token and the revoked token.

Important: By completing the steps above, the admin is temporarily revoking a hard token, therefore assigning the user account of that hard token to a new hard token. Because the admin is able to re-issue the previously revoked hard token by following the exact same steps that were explained above, this can be considered a temporary operation.

Permanent Revoke

The Permanent Revoke method is preferable in the case that the hard token is lost, stolen or broken, meaning that the user will no longer be using it.

Permanent Revoke is performed by deleting the hard token from the portal, which will unassign the token from the user.

Deleting Token will result in deleting the hard token device configuration in SAASPASS and deleting the Hard Token User/SAASPASS ID. All user accounts currently assigned to this hard token will remain pending in the company (not assigned to any user and can be assigned to another user/SAASPASS ID).

Follow the steps below to perform permanent revoking of the hard token which has a user account/s assigned to it:

- Go to the "FIDO & Hard Tokens" management section and click on the *Delete* button next to the hard token type you want to permanently revoke from SAASPASS. See Image 9.

| SERIAL NUMBER | TYPE | STATUS | SAASPASS USER | ACTIONS |
|---------------|------------------------|---------------------------------|---------------|---------------|
| Yubico Test | YubiKey USB (non FIDO) | ACTIVE No account assigned | 663459512 | MANAGE DELETE |
| Yubico | YubiKey USB (non FIDO) | ACTIVE Has assigned accounts | 115584831 | MANAGE DELETE |

Total records: 2

Image 9: Delete hard token.

- Due to the severity of the delete operation, you will need to authenticate by providing an OTP or scanning the barcode, as shown in Image 10.

DELETE TOKEN

Deleting token will result in deletion of the hard token device configuration in SAASPASS and deletion of the SAASPASS User. All accounts currently assigned to this user will remain pending in the company.

IDENTIFY TO CONTINUE



ONE-TIME PASSWORD

→ NEXT CANCEL

Image 10: Required identification/authentication to complete a delete operation.

- A message will be displayed when the token is successfully deleted, as shown in Image 11.

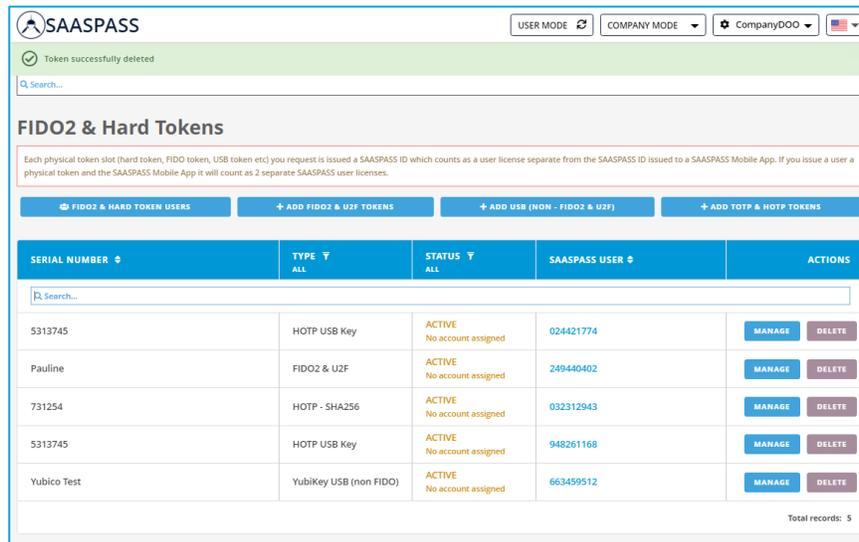


Image 11: Hard Token successfully deleted.

BACKUP KEY

Backup key is set in the event a primary key is not available. Admin can add the backup keys in the same way as adding the primary keys and they will have their own SAASPASS IDs. In case the admin decides to move the user from the primary key to the backup key, all they need to do is to re-assign the user accounts from the primary key to the backup key. On the other hand, if you would want the backup key to always be ready for the user, then you need to go to the sharing center in the SAASPASS admin portal, and share the user access between the two SAASPASS IDs of the primary key and the backup key. For more details on how to share different types of user accounts read the [Appendix 2](#) in this document.

In SAASPASS as the SAASPASS ID is considered as a unique identifier, it can also be referred to as a key. Admin can create multiple hard tokens/keys therefore each of them will have a unique SAASPASS ID that can be designated as primary key and backup key.

To meet the concept of a backup method for a given user, the admin needs to create two hard tokens/keys from the "Hard Token Management" section. Admin will choose which one of the hard tokens/keys will be used as a primary SAASPASS ID and as a secondary SAASPASS ID.

- Primary SAASPASS ID - Referred to as Primary KEY
- Secondary SAASPASS ID - Referred to as Backup KEY

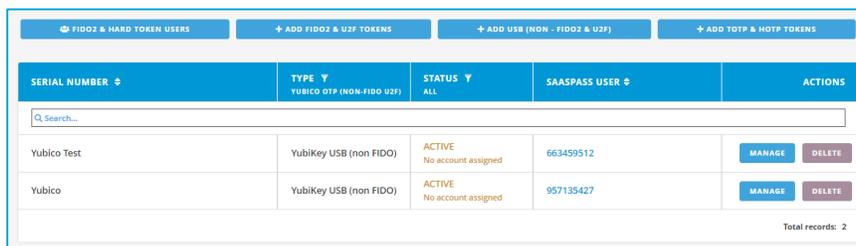
Active Backup Scenario

With an active backup scenario there will be two hard tokens/keys and both will always have the same user accounts assigned for a given user. Admin can designate one of the hard tokens/keys as a primary key to be in possession of the user and used on a regular basis and the other hard token/key to be used by admin or be granted to the user as a backup key in cases when the primary key is not available.

Active backup scenario is met by assigning the same user account/s and the access rights (groups) of the primary key to the secondary key.

Follow the steps below to setup active backup of the hard token/key which has user account/s assigned to it:

- **Important:** In the steps below, assigning the same user account/s to primary and backup hard tokens/keys is demonstrated for accounts of type Simple username. Demonstration on how to assign same account of Email type to primary and backup hard tokens/keys is given in [Appendix 2](#).
- Find your hard tokens in the tokens table under the "FIDO & Hard Tokens" management section as shown in Image 12.
 - Here, initially both hard tokens don't have any user account/s assigned to them and are with "No Account Assigned" status.



| SERIAL NUMBER | TYPE | STATUS | SAASPASS USER | ACTIONS |
|---------------|------------------------|-------------------------------|---------------|---------------|
| Yubico Test | YubiKey USB (non FIDO) | ACTIVE No account assigned | 663459512 | MANAGE DELETE |
| Yubico | YubiKey USB (non FIDO) | ACTIVE No account assigned | 957135427 | MANAGE DELETE |

Image 12: Find the hard tokens/keys to set up active backup.

- Next, assign the same user account/s to both of these hard tokens/keys.
- Select and COPY the SAASPASS ID associated with the hard token/key that will be the primary key (primary SAASPASS ID 663459512).
- Go to the "User Directories" section and find the user account you want to assign to the hard token/key designated as primary key, as shown in Image 13.

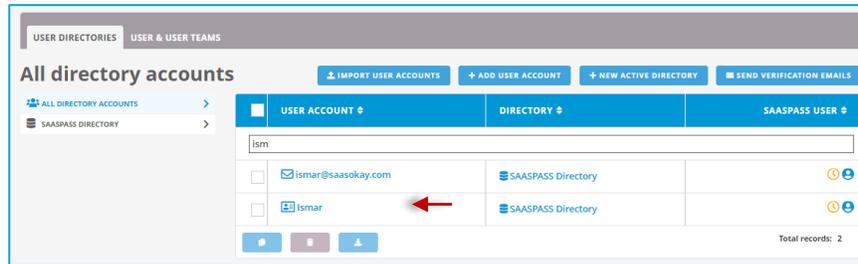


Image 13: Find the User Account.

- Now, click on the user account "Ismar" to open the "User Account Details" window, then PASTE the primary SAASPASS ID in the Account Verification entry field. Next, click on the *Search* button and once it is found, verify it by clicking on the *Verify Account* button.
- You should receive a message that the verification has been done successfully.

* More details on how to assign a user account to a hard token can be found in the [Appendix 1](#).

- Next, create a new user account with the same username "Ismar" as the one that was assigned to the hard token with (primary SAASPASS ID / primary key). Image 14.
 - During the process of creating the new user account, you can provide the SAASPASS ID associated with the second hard token/key that will be the backup key (secondary SAASPASS ID 957135427) or
 - You can create this new user account as a "Pending" one and assign it to the secondary SAASPASS ID 957135427 by following the steps for User assignment to a hard token demonstrated in [Appendix 1](#).

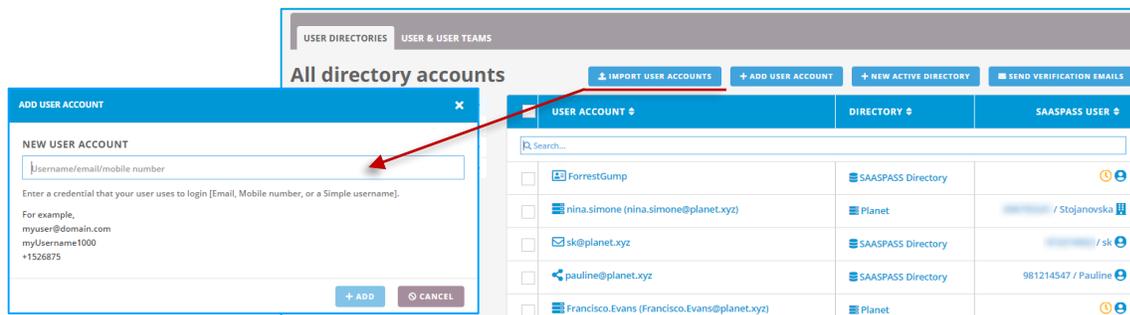


Image 14: Create the new User Account with the same username as the one assigned to Primary SAASPASS ID.

- After the steps above are completed, there should be two user accounts with the same username "Ismar" and with "Active" status assigned to the primary key and backup key hard tokens.

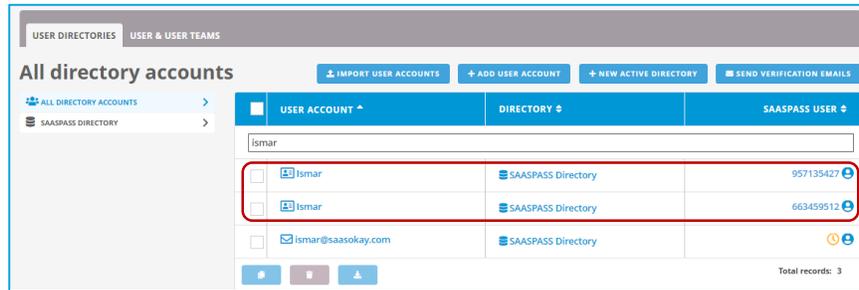


Image 15: Verified status for both users.

- If you go back to the "FIDO & Hard Tokens" sections, the status is changed to "Active" here, as well, after both user accounts with the same username "Ismar" are assigned to both hard tokens/keys (primary key and backup key). See Image 16.



Image 16: Status change to Active after user account assignment to a hard token.

Passive Backup Scenario

With a passive backup scenario there will be two hard tokens/keys, but only one of them will have user accounts assigned to it for a given user and designated as the primary key. The second one, which will be the backup key, will not have any user accounts assigned to it. On demand, when there is a need for usage of the backup key, the admin will assign the same user accounts from the primary key to the backup key and grant access to the user in cases when the primary key is not available.

Passive backup scenario is met by assigning the same user account/s and the access rights (groups) of the primary key (Primary SAASPASS ID) to the backup key (Secondary SAASPASS ID) when there is a need for it (on demand).

Admin can choose whether they will:

- Remove the assignment of the user account/s from the primary key and in addition assign the user account/s to the backup key.
- Keep the user account/s assigned to the primary key and assign the same user account/s also to the backup key.

Follow the steps below to setup passive backup of the hard token/key which has user accounts/s assigned to it:

- **Important:** In the steps below, assigning the same user account/s to primary and backup hard tokens/keys is demonstrated for accounts of type Simple username. Demonstration on how to assign the same account of Email type to primary and backup hard tokens/keys is given in [Appendix 2](#).
- Find your hard tokens in the tokens table under the "FIDO & Hard Tokens" management section as shown in Image 17.
 - Here, initially the hard token that is designated as a primary key (primary SAASPASS ID) is with "ACTIVE" status because it has user account/s assigned to it. The second hard token, designated as backup key (secondary SAASPASS ID) is with "No Account Assigned" status because it still doesn't have a user account/s assigned to it.

| SERIAL NUMBER | TYPE | STATUS | SAASPASS USER | ACTIONS |
|---------------|------------------------|---------------------------------|---------------|---------------|
| Yubico | YubiKey USB (non FIDO) | ACTIVE Has assigned accounts | 957135427 | MANAGE DELETE |
| Yubico Test | YubiKey USB (non FIDO) | ACTIVE No account assigned | 663459512 | MANAGE DELETE |

Total records: 2

Image 17: Find the hard tokens/keys designated as primary and backup keys.

- On demand here, when the primary key is not available for the user, admin has two options:
 - Remove the assignment of the user account/s from the primary key and in addition assign the user account/s to the backup key or
 - Keep the user account/s assigned to the primary key and assign the same user account/s also to the backup key
- With the first option, similar like with Temporary Revoke method, the admin needs to find the user account/s under the "User Accounts" section, then "Change owner" of the primary key (primary SAASPASS ID - 957135427) to the new owner of the backup key (secondary SAASPASS ID - 663459512)
 - The outcome with choosing this option is that only the backup key will remain "Active" and will have the user account "Ismar" assigned to it. Image 18.

| SERIAL NUMBER | TYPE | STATUS | SAASPASS USER | ACTIONS |
|---------------|------------------------|---------------------------------|---------------|---------------|
| Yubico Test | YubiKey USB (non FIDO) | ACTIVE Has assigned accounts | 663459512 | MANAGE DELETE |
| Yubico | YubiKey USB (non FIDO) | ACTIVE No account assigned | 957135427 | MANAGE DELETE |

Total records: 2

| USER ACCOUNT | DIRECTORY | SAASPASS USER |
|--------------------------------|--------------------|---------------|
| ismal | | |
| <input type="checkbox"/> Ismar | SAASPASS Directory | 663459512 |

Image 18: User account re-assigned to Backup key only.

- With the second option, similar to the Active Backup Scenario, the admin needs to create new user account with the same username "Ismar" as the already existing one that is assigned to the primary key (primary SAASPASS ID - 663459512) and assign this new user account to the backup key (secondary SAASPASS ID - 957135427)
 - The outcome with choosing the second option is that both the primary key and the backup key will become "Active" and will have the user account "Ismar" assigned to it. Image 19.

| USER ACCOUNT | DIRECTORY | SAASPASS USER |
|--------------------------------|--------------------|---------------|
| ismal | | |
| <input type="checkbox"/> Ismar | SAASPASS Directory | 957135427 |
| <input type="checkbox"/> Ismar | SAASPASS Directory | 663459512 |

Image 19: User account/s assigned to both Primary and Backup key.

APPENDIX 1

SAASPASS ID - Hard Token User

Each hard token added into the system receives a unique SAASPASS ID, meaning each hard token functions as a standalone user. Different user accounts can be assigned to the same SAASPASS ID, in this case to the same hard token. A user should have only one token, and it will be able to generate one-time passwords for all of the user's assigned accounts. In other words, a user should NOT have a different hard token for each account they have in the company. Instead, multiple user accounts of the same or even different types (Simple username, Email, or Active Directory type) can be assigned to the single SAASPASS ID associated with the hard token.

Important: In SAASPASS, the SAASPASS ID of the hard token is referred to as the "Hard Token User" or simply "hard token." As explained above, the Hard Token User can have multiple user accounts assigned to it, that can be the same or different types.

USER ACCOUNTS ASSIGNMENT

The process of assigning user accounts is similar for each type of hard token available in SAASPASS, so we will refer to user account assignment to a "hard token" rather than to a specific token type (FIDO U2F, YubiKey or HOTP USB Key and TOTP or HOTP Hard Token).

The types of user accounts in SAASPASS that can be assigned to a hard token are: Simple username, Email, and Active Directory account.

User Account assignment to a hard token:

- In order to assign a user account to a hard token, add a new user account from the "User Accounts" tab or find an existing one listed under the "User Accounts" table, as shown in Image 20.

Important: The type of user account can be: Simple username, Email, and Active Directory account.

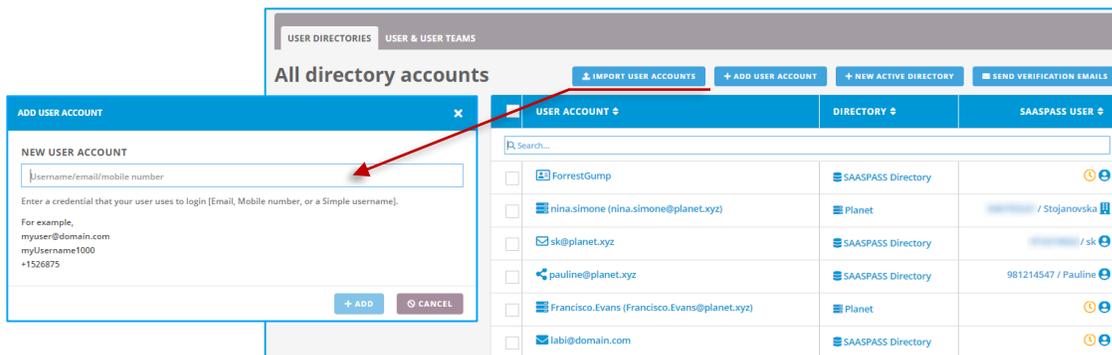


Image 20: Add new User Account.

- Find your hard token in the tokens table under the "FIDO & Hard Tokens" management section as shown in Image 21.

| SERIAL NUMBER | TYPE | STATUS | SAASPASS USER | ACTIONS |
|---------------|------------------------|-------------------------------|------------------|---------------|
| 5313745 | HOTP USB Key | ACTIVE No account assigned | <u>024421774</u> | MANAGE DELETE |
| Pauline | FIDO2 & U2F | ACTIVE No account assigned | <u>249440402</u> | MANAGE DELETE |
| 731254 | HOTP - SHA256 | ACTIVE No account assigned | <u>032312943</u> | MANAGE DELETE |
| 5313745 | HOTP USB Key | ACTIVE No account assigned | <u>948261168</u> | MANAGE DELETE |
| Yubico Test | YubiKey USB (non FIDO) | ACTIVE No account assigned | <u>663459512</u> | MANAGE DELETE |
| Yubico | YubiKey USB (non FIDO) | ACTIVE No account assigned | <u>957135427</u> | MANAGE DELETE |

Image 21: Copy the SAASPASS ID of the hard token.

- Select and COPY the SAASPASS ID associated with the hard token
- Go to the "User Accounts" tab and find the user account you want to assign to the hard token, as shown in Image 22.



Image 22: Find the User Account.

- Now, click on the user account to open the "User Account Details" window.
- Click on the *Verify Account* button and then PASTE the SAASPASS ID in the Account Verification entry field. Image 23.

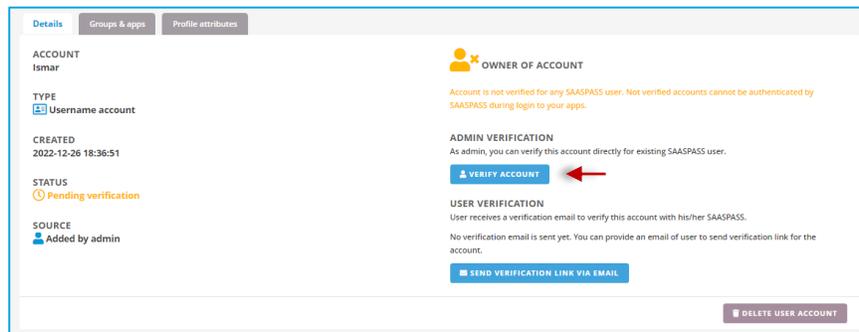


Image 23: User account details window.

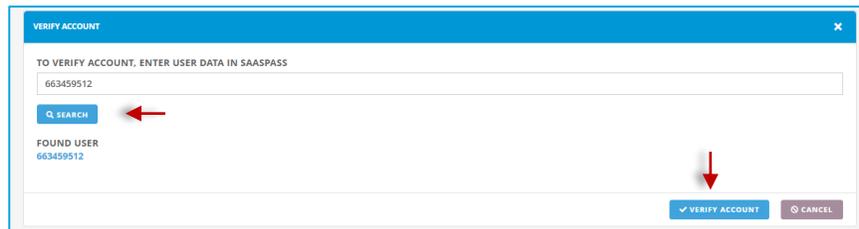


Image 24: Search for the SAASPASS ID of the hard token.

- You should receive a message that the verification has been done successfully.

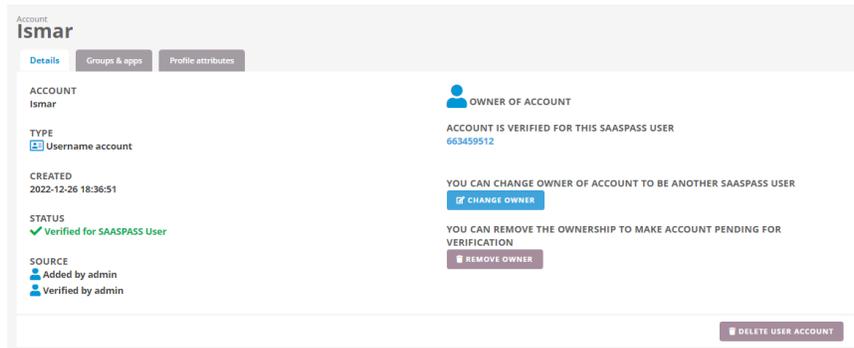


Image 25: Verify User Account.

- Now the Hard Token User (hard token) should be visible under "User Accounts" with "Active" status.
- If you go back to the "FIDO & Hard Tokens" sections, the status is changed to "Active" here, as well, after a user account is assigned to the hard token.

APPENDIX 2

SHARE USER ACCOUNTS

When there is a need for a single user account to be used by multiple SAASPASS Users, SAASPASS provides user accounts sharing in different ways depending on the type of the user account. There are different types of user accounts in SAASPASS such as: Simple username, Email, or Active Directory type and in this section a demonstration is given on how can each of these be shared among multiple SAASPASS IDs.

SHARE COMPANY EMAIL ACCOUNT

Sharing a company email account is done through the "Sharing Center" section. The company email accounts that are shared will also share the company applications associated. You can add, remove and manage the email accounts that are shared afterwards.

The steps below demonstrate how two (or more) Hard Token Users (hard tokens/keys) can share the same company email account:

- First, go to the "User & User Teams" section and make sure that you already have a company email account that is assigned to one hard token/key as shown in Image 26.
- **Important:** In case you don't have a company email account assigned to a hard token than follow the steps from [Appendix 1](#)

on how to assign a user account to a hard token with that the difference that you will use an Email type of account instead of the Simple username account type as given in the example.

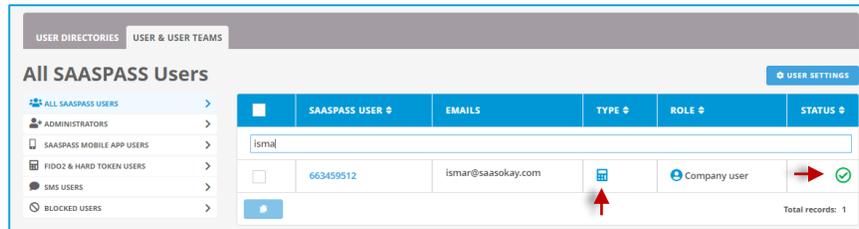


Image 26: Assure that there is a company email account assigned to one hard token/key.

- Next, from the main menu go to the "Shared Access Manager" section, as shown in Image 27.

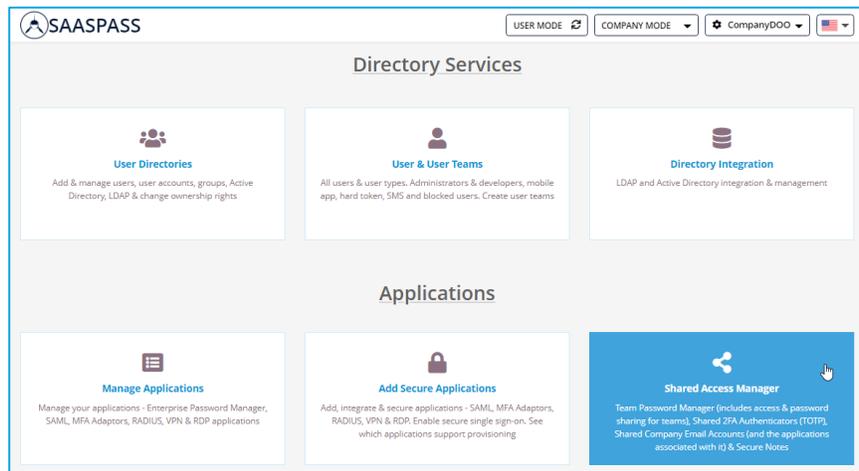


Image 27: Sharing Center.

- Here, click on the "Shared Company Email Accounts" tab, and then click on the *Share an Additional Email Account* button. Image 28.

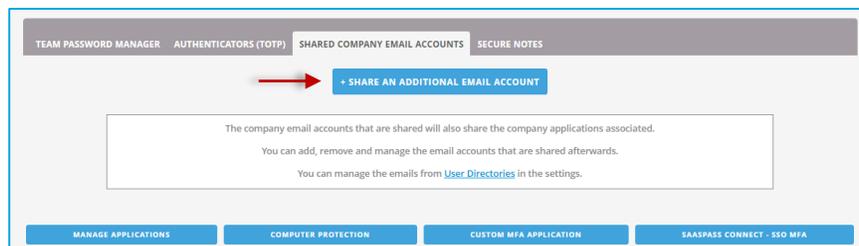
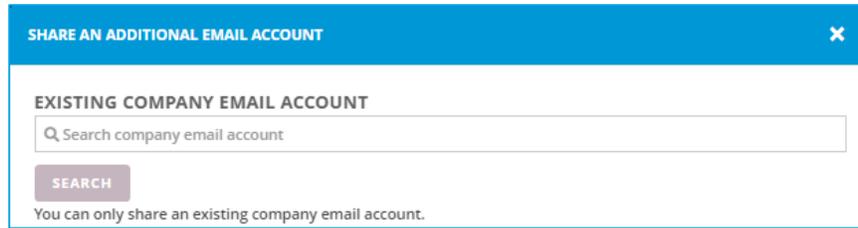


Image 28: Search for your company email account.

- Next, search for the company email account you want to share with another hard token/key (SAASPASS ID). Image 29.



SHARE AN ADDITIONAL EMAIL ACCOUNT ✕

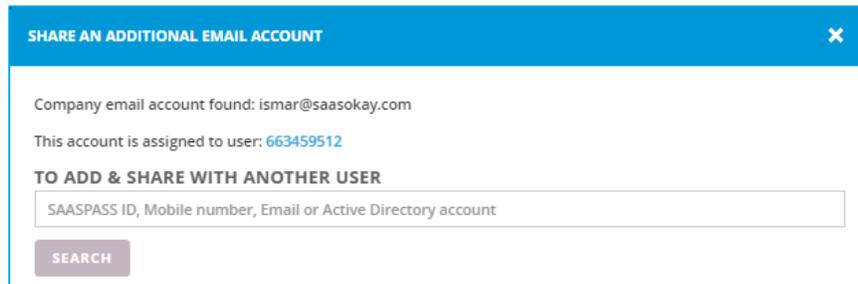
EXISTING COMPANY EMAIL ACCOUNT

Search company email account

SEARCH

You can only share an existing company email account.

Image 29: Search for your company email account.



SHARE AN ADDITIONAL EMAIL ACCOUNT ✕

Company email account found: ismar@saasokay.com

This account is assigned to user: 663459512

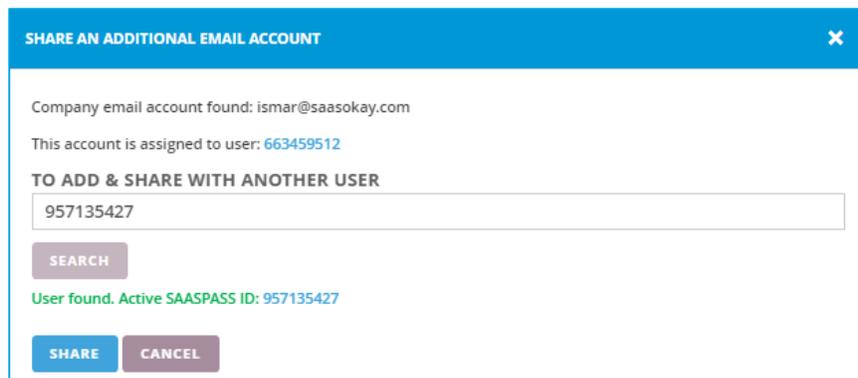
TO ADD & SHARE WITH ANOTHER USER

SAASPASS ID, Mobile number, Email or Active Directory account

SEARCH

Image 30: Search for the hard token that you want to share with.

- Once the SAASPASS ID is found click on the *Share* button.



SHARE AN ADDITIONAL EMAIL ACCOUNT ✕

Company email account found: ismar@saasokay.com

This account is assigned to user: 663459512

TO ADD & SHARE WITH ANOTHER USER

957135427

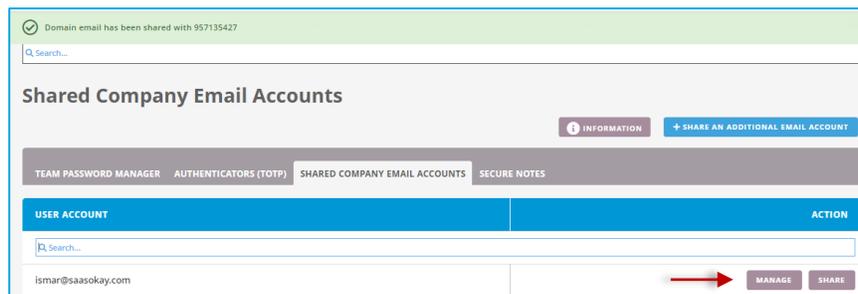
SEARCH

User found. Active SAASPASS ID: 957135427

SHARE CANCEL

Image 31: Share the company email account found with another hard token/key.

- When the share operation is completed you will get a message that the company email is successfully shared with the hard token/key (SAASPASS ID 957135427).



Domain email has been shared with 957135427

Search...

Shared Company Email Accounts

INFORMATION + SHARE AN ADDITIONAL EMAIL ACCOUNT

TEAM PASSWORD MANAGER AUTHENTICATORS (TOTP) SHARED COMPANY EMAIL ACCOUNTS SECURE NOTES

| USER ACCOUNT | ACTION |
|--------------------|--------------|
| ismar@saasokay.com | MANAGE SHARE |

Image 32: Sharing Center of your shared company email account.

- After the above steps are completed, check the status of your shared company email under the sharing center. Image 33.

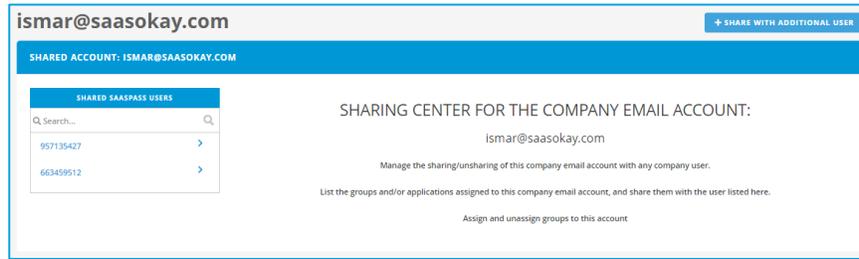


Image 33: Sharing Center of your shared company email account.

- Now, go back to the "Groups & Users" section and verify that your company email account is now shared between the two hard tokens/keys (SAASPASS IDs). Image 34.

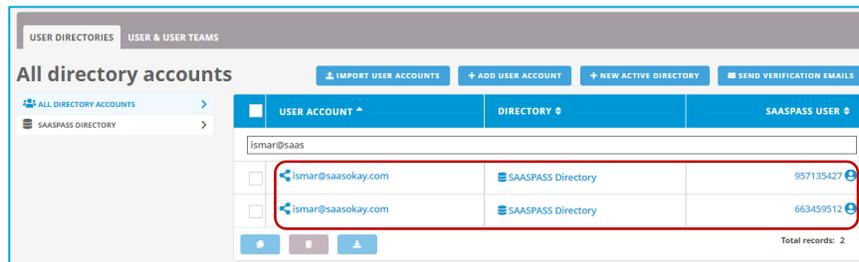


Image 34: Verify that the company email account is shared under the "Groups & Users" section.

SHARE SIMPLE USERNAME ACCOUNT

Sharing a simple username type of account is done by creating simple user accounts with same usernames from the "Groups & Users" section and assigning them to different SAASPASS IDs. Admin can add as many simple user accounts as they need as long as they assign them to different SAASPASS IDs.

The final result in completing the sharing for the Simple username type of user accounts is shown in Image 35.

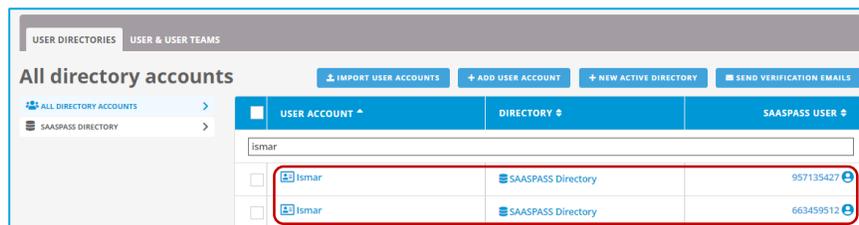


Image 35: Shared Simple username account.

SHARE ACTIVE DIRECTORY USER ACCOUNT

Sharing an Active Directory type of account is done by creating a simple user account, from the "Groups & Users" section, that will have the same username as the active directory account and assigning it to a different SAASPASS ID. Admin can add as many simple user accounts as they need as long as they assign them to different SAASPASS IDs.

The final result in completing the sharing for an Active Directory type of user account is shown in Image 36.

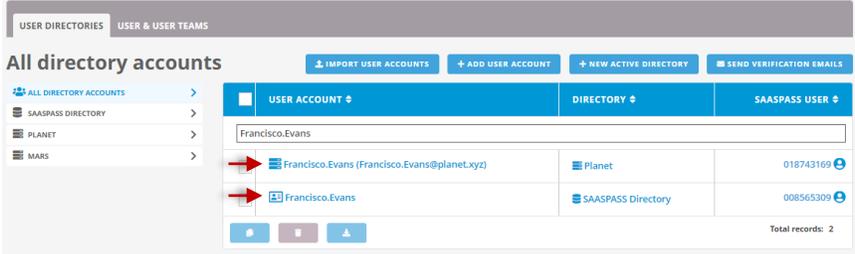


Image 36: Shared Active Directory user account.

For any questions, you can always contact us at:
support@saaspass.com