



# Hard Token Support Manual

SAASPASS

# Contents

- HARD TOKEN MANAGEMENT ..... 3
  - SAASPASS ID - Hard Token User..... 3
  - User Accounts Assignment ..... 4
    - User Account assignment to a hard token: ..... 4
- ADDING TOKENS INTO SAASPASS ..... 7
  - Add and Import FIDO U2F Tokens ..... 8
  - Add and Import USB (non-FIDO) Tokens ..... 10
  - Add and Import Hard Tokens..... 13
- TOKEN CONFIGURATION & EDITS..... 15
  - Yubikey Token Configuration..... 15
    - Yubico OTP (non-FIDO U2F) Token Configuration ..... 16
    - USB OATH-HOTP Token Configuration ..... 17
    - USB OATH-HOTP (Event Based) Token Synchronization ..... 18
- HARD TOKEN (TOTP and HOTP) CONFIGURATION ..... 19
  - TOTP Hard Token Configuration ..... 19
  - TOTP (EVENT-BASED) HARD TOKEN SYNCHRONIZATION ..... 20
  - HOTP HARD TOKEN CONFIGURATION ..... 21
  - HOTP (EVENT-BASED) HARD TOKEN SYNCHRONIZATION ..... 21
- FIDO U2F TOKEN CONFIGURATION ..... 22
  - REGISTER FIDO U2F TOKEN..... 22
- DELETE HARD TOKEN ..... 23
- HARD TOKEN USAGE ..... 25
  - Hard Token login on SAASPASS Web Portal ..... 25
    - FIDO U2F Token login on SAASPASS Web Portal ..... 26
    - Non-FIDO USB Token login on SAASPASS Web Portal ..... 26
    - Hard Token login on SAASPASS Web Portal..... 27
  - Hard Token login on SAASPASS SAML Company Apps ..... 27
  - Hard Token login with SAASPASS Connectors ..... 28
    - Hard Token login with Windows SAASPASS Connector ..... 28
    - Hard Token login on Windows Desktop SSO App ..... 31

# HARD TOKEN MANAGEMENT

SAASPASS supports a number of physical hard/USB token solutions for companies and these include:

- USB FIDO Tokens
- USB (non-FIDO) Tokens
- OATH TOTP Hard Tokens
- OATH HOTP Hard Tokens

You can add them or import them from the admin portal of SAASPASS for your company.

## *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 as they do 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. See Image 1.

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.

Also, SAASPASS designates hard tokens for corporate use only, meaning that only an administrator of a company registered with SAASPASS can provision Hard Token Users.

Here, "provisioning" refers to an administrator's ability to:

- Add hard tokens, and therefore add Hard Token Users.
- Assign and Reassign user accounts to a Hard Token User.
- Remove user accounts from a Hard Token User.
- Manage the Hard Token User rights (Administrator, Developer, Company User).
- Change Ownership of a Hard Token User.
- Delete the hard tokens, and therefore delete Hard Token Users.

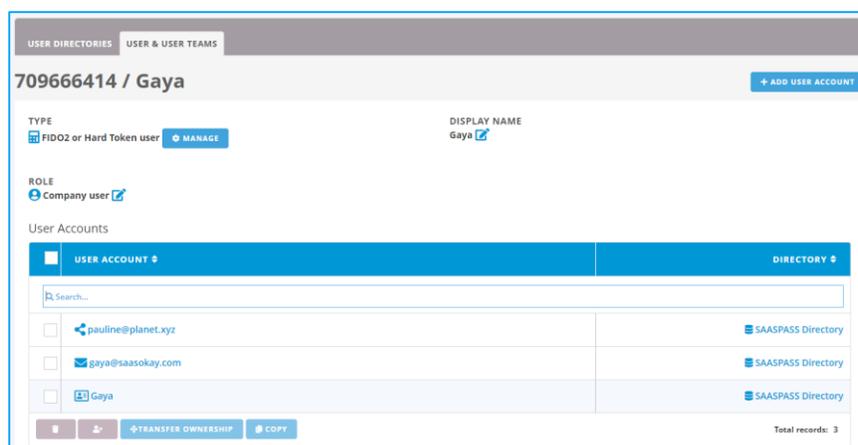


Image 1: Hard Token User

## 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.

**Important:** Before assigning user accounts to a hard token, it is recommended that you visit the Hard Token Specification section in this document and complete the setup/edit process by providing specifications of the selected token.

### 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 2.

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

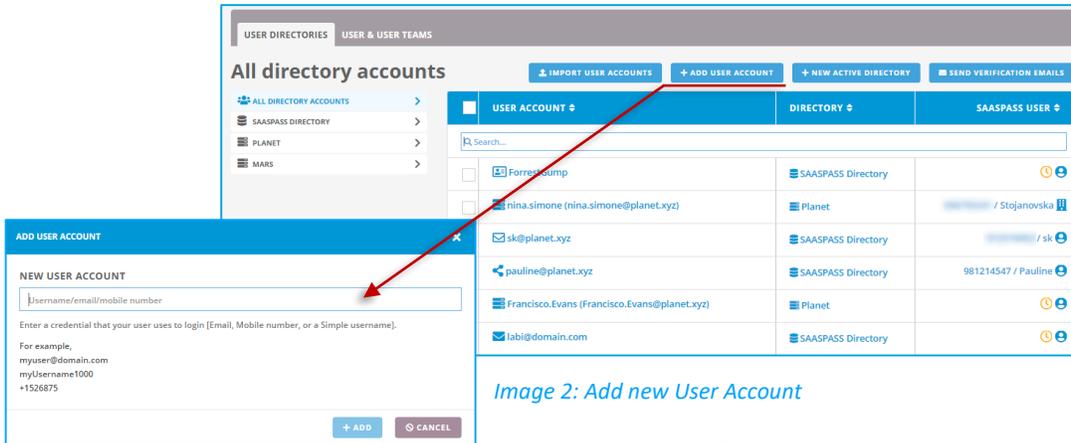


Image 2: Add new User Account

Find your hard token in the tokens table under the "Hard Token Management" tab as shown in Image 3.

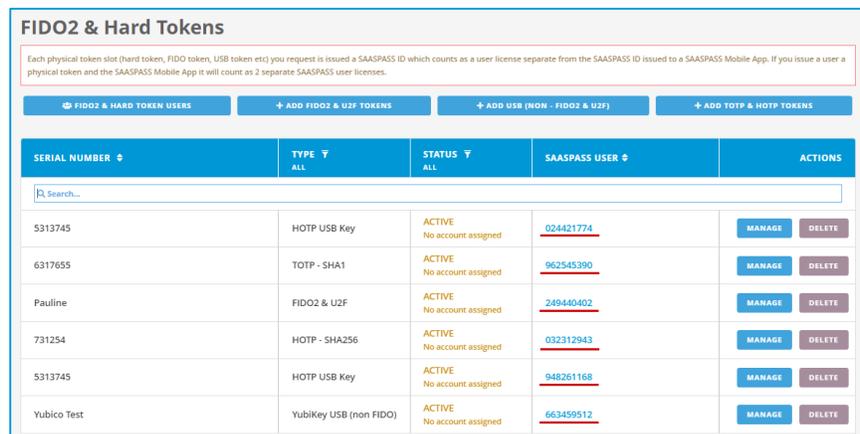


Image 3: Copy the SAASPASS ID of the hard token.

Select and COPY the SAASPASS ID associated with the hard token.

Go to the "User Directories" tab and find the user account you want to assign to the hard token, as shown in Image 4.

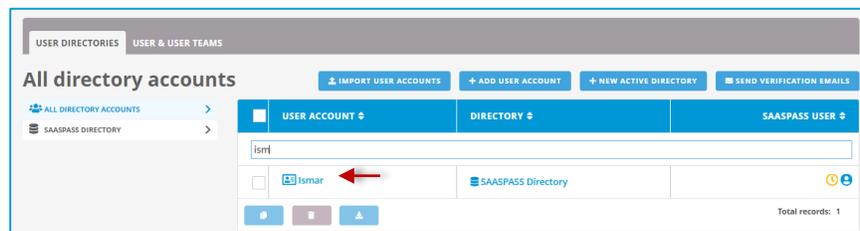


Image 4: Find the User Account.

Now, click on the user account to open the "User Account Details" window, then PASTE the SAASPASS ID in the "ACCOUNT VERIFICATION" entry field. Next, click the Search button as shown in Image 6.

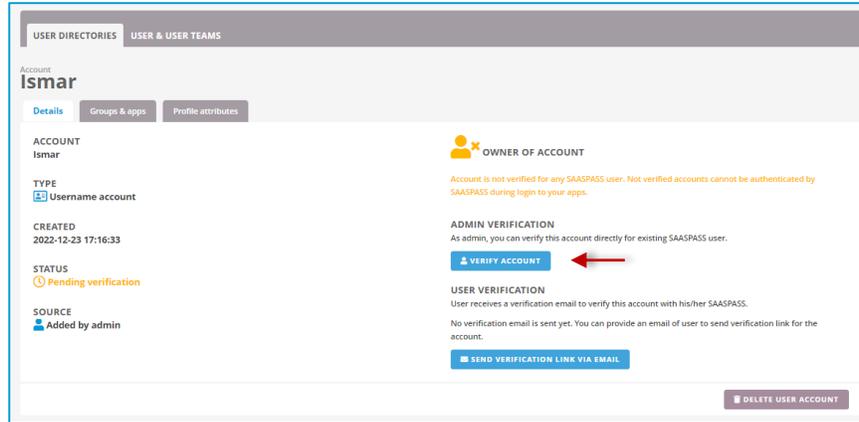


Image 5: Search for the SAASPASS ID of the hard token.

Next, once the SAASPASS ID is found, click the VERIFY button.

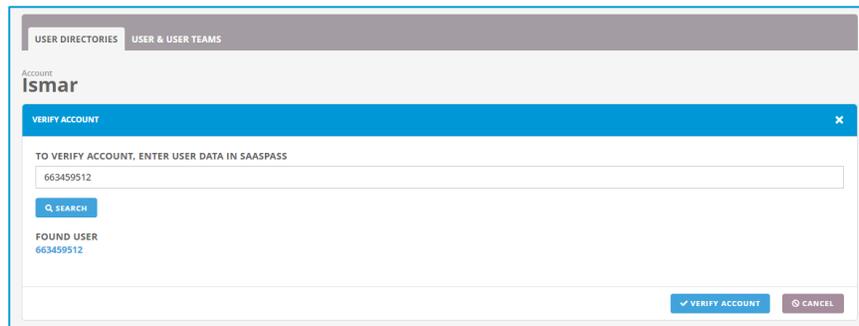


Image 6: Verify User Account.

You should receive a message that the verification has been done successfully, as shown in Image 7.

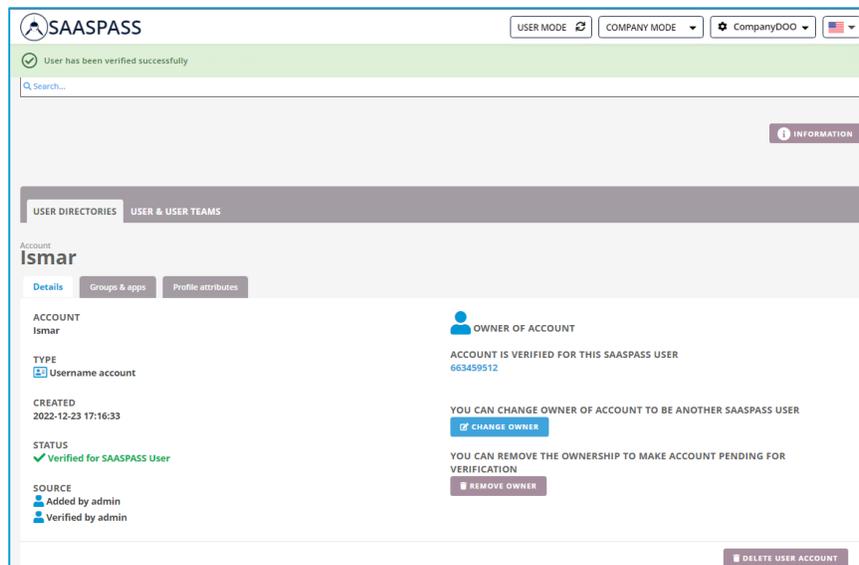


Image 7: Successful verification completed.

Now, the Hard Token User (hard token) should be visible under "User Accounts" with "Active" status, as shown in Image 8.

| SAASPASS USER | EMAILS             | TYPE                     | ROLE                | STATUS |
|---------------|--------------------|--------------------------|---------------------|--------|
| 663459512     | ismar@saasokay.com | FIDO2 or Hard Token user | Company user        | Active |
|               |                    |                          | Super administrator | Active |

Image 8: Check status for the hard token user.

If you go back to the "Hard Token Management" tab, the status is changed to "Active" here, as well, after a user account is assigned to the hard token. See Image 9.

| SERIAL NUMBER | TYPE                   | STATUS                          | SAASPASS USER | ACTIONS       |
|---------------|------------------------|---------------------------------|---------------|---------------|
| Yubico Test   | YubiKey USB (non FIDO) | ACTIVE<br>Has assigned accounts | 663459512     | MANAGE DELETE |
| 5313745       | HOTP USB Key           | ACTIVE<br>No account assigned   | 024421774     | MANAGE DELETE |
| 6317655       | TOTP - SHA1            | ACTIVE<br>No account assigned   | 962545390     | MANAGE DELETE |
| Pauline       | FIDO2 & U2F            | ACTIVE<br>No account assigned   | 249440402     | MANAGE DELETE |
| 731254        | HOTP - SHA256          | ACTIVE<br>No account assigned   | 032312943     | MANAGE DELETE |
| 5313745       | HOTP USB Key           | ACTIVE<br>No account assigned   | 948261168     | MANAGE DELETE |

Total records: 6

Image 9: Status change to Active after user account assignment to a hard token.

## ADDING TOKENS INTO SAASPASS

When you log into the SAASPASS web portal, click on "SWITCH TO COMPANY MODE" and select your company (if you manage more than one).

Once you are in company mode, select the Hard Tokens tab and pick the relevant token type that you want to add or import.

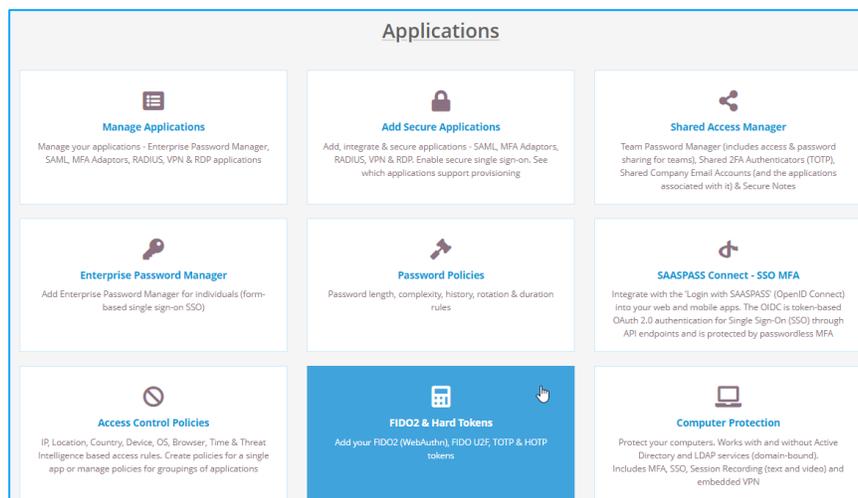


Image 10: Hard Tokens.

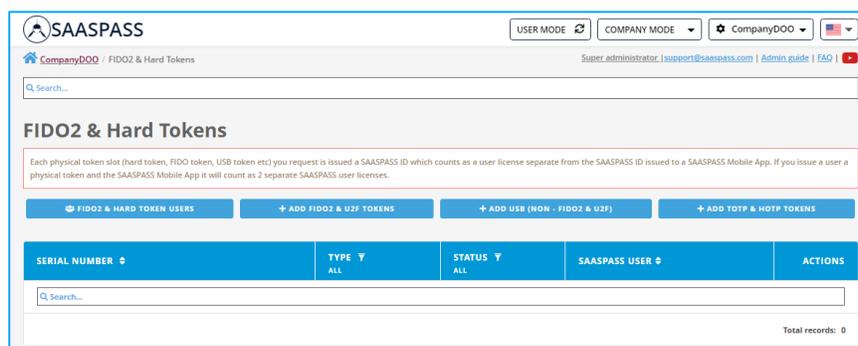


Image 11: Add Hard Tokens.

## Add and Import FIDO U2F Tokens

*Add FIDO U2F Tokens:*

You can enter a device name to help identify the device (optional). Providing an email address will send the registration email to your user (optional). You can add the email later in the MANAGE section of each token. You can also register devices and test authentication in the MANAGE section and then distribute it to your users.

You can have your users self-register their FIDO2 devices with their emails. You can add their emails and click on the *Save Tokens* button to send them the registration email for their FIDO2 devices. The email link is valid for 72 hours and they should check their spam and junk folders if necessary.

**ADD FIDO2 & U2F TOKENS**

NUMBER OF FIDO2 & U2F TOKENS

You can enter a device name to help identify the device (optional). Providing an email address will send the registration email to your user (optional). You can add the email later in the MANAGE section of each token. You can also register devices and test authentication in the MANAGE section and then distribute it to your users.  
 You can have your users self-register their FIDO2 devices with their emails. You can add just their emails and click on the "SAVE TOKENS" button to send them the registration email for their FIDO2 devices. The email link is valid for 72 hours and they should check their spam and junk folders if necessary. To do bulk imports or send out bulk emails to users click on the BULK IMPORT button.

**BULK IMPORT**

| # | Serial Number                            | Registration Email                         | Actions       |
|---|--|--|---------------|
| 1 | Pauline                                  | pauline@domain.com                         | <b>DELETE</b> |
| 2 | <input type="text" value="Device Name"/> | <input type="text" value="Email Address"/> | <b>DELETE</b> |

**+ ADD NEW TOKEN**

**SAVE TOKENS** **CANCEL**

*Image 12: Add FIDO U2F Tokens.*

- Choose the number of FIDO U2F tokens you want to add.
- Write down the Serial Number or a device name of the FIDO U2F token in the specified field.
- Click the *Save Tokens* button.
- After saving, find the newly added FIDO U2F tokens in the tokens table under the "Hard Token Management" tab.

*Import FIDO U2F Tokens:*

CSV content can be deviceName,emailAddress or the device name on each line. If you provide the email address, the registration link will be sent to the users so that they can register the token by themselves.

You can have your users self-register their FIDO2 devices with their emails. The email link is valid for 72 hours and they should check their spam and junk folders if necessary. For bulk emails for self-service registration, just paste the CSV email file in the format of:

Testing token,test1@company.com  
 228463,test2@company.com  
 ,test3@company.com

**Note:** When email is provided you can continue managing the device and assign accounts before the user registers. Always keep in mind that the user is expected to register themselves when managing a token.

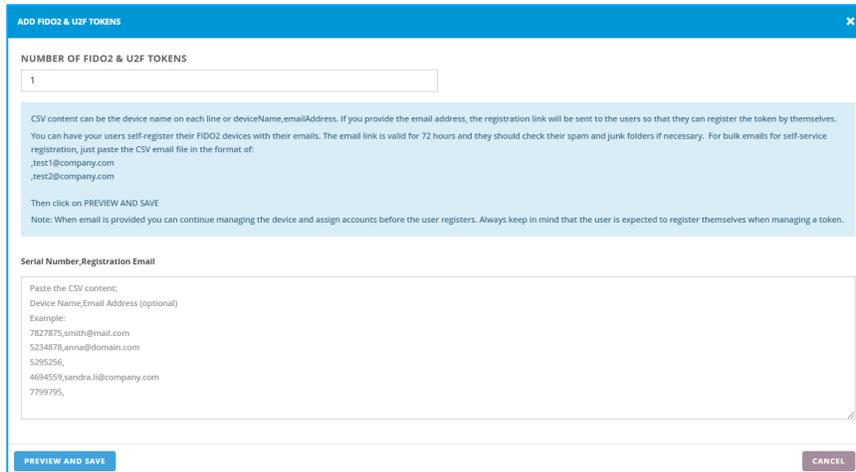


Image 13: Import FIDO U2F Tokens.

- To import FIDO U2F tokens click the *Bulk Import* button.
- Copy and paste the serial numbers of your FIDO U2F tokens from the CSV file, which should be formatted as in the example.
- Click the *Preview and Save* button to check if the pasted content is properly parsed.
- Click the *Save Tokens* button.
- After saving, find the newly added FIDO U2F tokens in the tokens table under the "Hard Token Management" tab.

## Add and Import USB (non-FIDO) Tokens

Add Yubico OTP (non-FIDO U2F) Tokens:

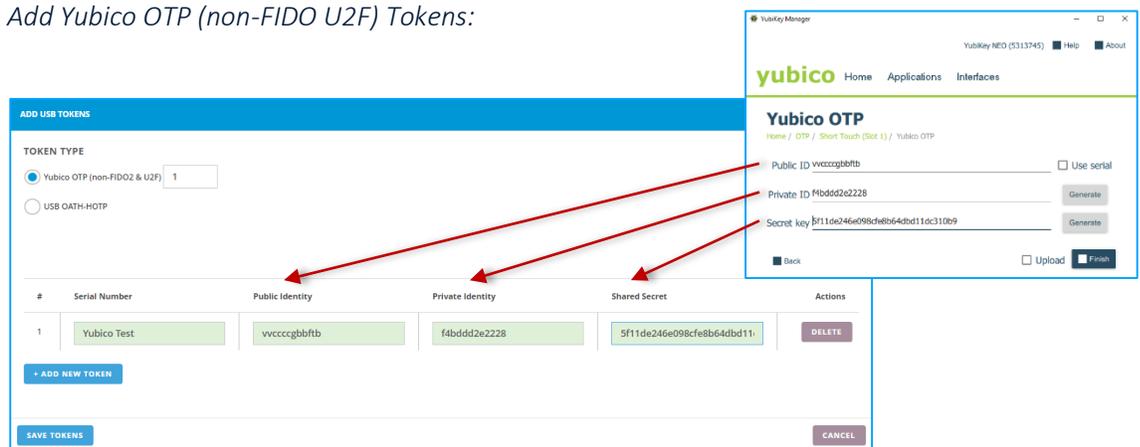


Image 14: Add Yubico OTP (non-FIDO U2F) Tokens.

- For the token type choose the Yubico OTP (non-FIDO U2F).

- Choose the number of YubiKey OTP (non-FIDO U2F) tokens you want to add.
- Write down the: Serial Number, Public Identity, Private Identity and Shared Secret of the YubiKey OTP (non-FIDO U2F) token in the specified fields. Click the *How to Setup* button to see the example.
- Click the *Save Tokens* button.
- After saving, find the newly added YubiKey OTP (non-FIDO U2F) tokens in the tokens table under the "Hard Token Management" tab.

*Import Yubico OTP (non-FIDO U2F) Tokens:*

**ADD USB TOKENS**

**TOKEN TYPE** [How to set it up](#)

Yubico OTP (non-FIDO2 & U2F)

USB OATH-HOTP

Serial Number, Public Identity, Private Identity, Shared Secret

Paste the CSV content:  
 Decimal, 1-16 Bytes Modhex, 6 bytes Hex, 16 bytes Hex  
 Example:  
 7826735,95c8fe2c7f46,ebb6f9762c28,96411a713b3546f8931e04b4d6647322  
 5888878,c223f1a7a644,bd5b6c27de98,ae03d762f1af43b5a6d0769c0447f8d6  
 4215256,d2c9e7c81f1f1,b6320a610806,b37b3650a8b452d9ad3ad1f055d8e9b  
 465459,dc5aa377be86,374d6741b42f,5b436a31f4534de99e6940d3fc1127e  
 7799793,e1ac784d2341,b80e4c693938,1ae76c959ece4216bd2af1b477542d0

**PREVIEW AND SAVE** **CANCEL**

*Image 15: Import Yubico OTP (non-FIDO U2F) Tokens.*

- To import Yubico OTP (non-FIDO U2F) tokens click the *Bulk Import* button.
- Copy and paste the content of the CSV file containing the Serial Number, Public Identity, Private Identity and Shared Secret of your YubiKey OTP (non-FIDO U2F) Tokens. The file should be formatted as in the example (Image 15).
- Click the *Preview and Save* button to check if content pasted is properly parsed.
- Click the *Save Tokens* button.
- After saving, find the newly added YubiKey OTP (non-FIDO U2F) tokens in the tokens table under the "Hard Token Management" tab.

Add USB OATH-HOTP Tokens:

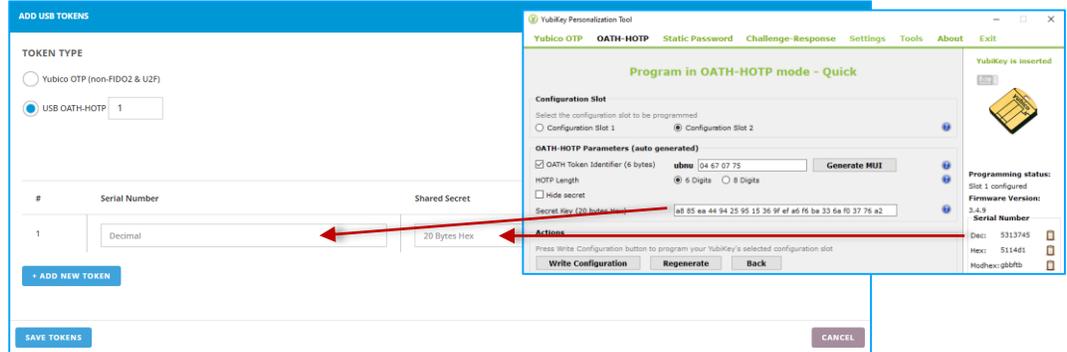


Image 16: Add USB OATH-HOTP Tokens.

- For the token type choose the USB OATH-HOTP.
- Choose the number of USB OATH-HOTP tokens you want to add
- Write down the: Serial Number and Shared Secret of the USB OATH-HOTP token in the specified fields. Click the *How to Setup* button to see the example.
- Click the *Save Tokens* button.
- After saving, find the newly added USB OATH-HOTP tokens in the tokens table under the "Hard Token Management" tab.

Import USB OATH-HOTP Tokens:

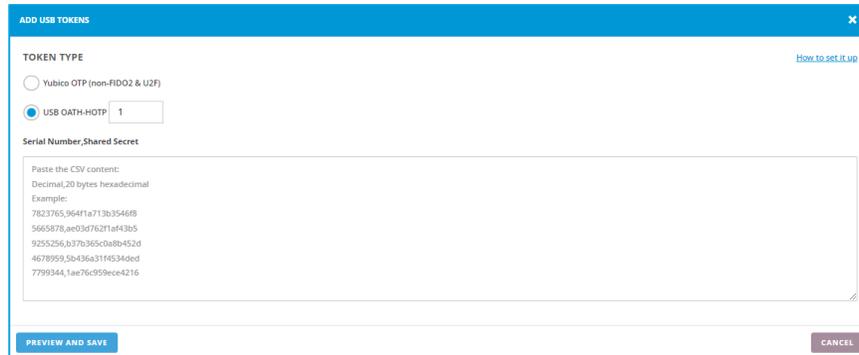


Image 17: Import USB OATH-HOTP Tokens.

- To import USB OATH-HOTP tokens click the *Bulk Import* button.
- Copy and paste the CSV file containing the Serial Number and Shared Secret of your USB OATH-HOTP tokens. The file should be formatted as in the example (Image 17).
- Click the *Preview and Save* button to check if the pasted content is properly parsed.
- Click the *Save Tokens* button.
- After saving, find the newly added USB OATH-HOTP tokens in the tokens table under the "Hard Token Management" tab.

## Add and Import Hard Tokens

Add TOTP Hard Tokens:

The screenshot shows a web form titled "ADD HARD TOKENS (HOTP OR TOTP)". It has three main sections: "TOKEN TYPE", "ALGORITHM", and "TOTP GENERATION TIME (SECONDS)".

- TOKEN TYPE:** Radio buttons for "TOTP" (selected) and "HOTP". A text input field next to "TOTP" contains the number "1".
- ALGORITHM:** Radio buttons for "SHA1" (selected), "SHA256", and "SHA512".
- TOTP GENERATION TIME (SECONDS):** A text input field containing "30".

Below these sections is a "BULK IMPORT" button. Underneath is a table with columns: "#", "Serial Number", "Shared Secret", and "Actions".

| # | Serial Number | Shared Secret | Actions |
|---|---------------|---------------|---------|
| 1 | Hexadecimal   | Hexadecimal   | DELETE  |

At the bottom of the form are buttons for "+ ADD NEW TOKEN", "SAVE TOKENS", and "CANCEL".

Image 18: Add TOTP Hard Tokens.

- For the token type choose TOTP
- Choose the number of TOTP Hard Tokens you want to add
- Choose the secure hash algorithm type (SHA1, SHA256 or SHA512).
- Choose the TOTP generation time in seconds (only for time-based generation tokens).
- Write down the: Serial Number and Shared Secret of the TOTP Hard Token in the specified fields.
- Click on the *Save Tokens* button.
- After saving, find the newly added TOTP Hard Tokens in the tokens table under the "Hard Token Management" tab.

Import TOTP Hard Tokens:

The screenshot shows the same "ADD HARD TOKENS (HOTP OR TOTP)" form as in Image 18, but with a large text area for pasting CSV content.

**TOKEN TYPE:** "TOTP" (selected), "HOTP". Input field: "1".

**ALGORITHM:** "SHA1" (selected), "SHA256", "SHA512".

**TOTP GENERATION TIME (SECONDS):** "30".

**Serial Number, Shared Secret:** A large text area with the following text:

```
Paste the CSV content:  
Hexadecimal,Hexadecimal  
Example:  
782d7b5,964f1a713b3546f8  
5ffe878,ae03d7621af43b5  
b2b5256,b37b365d0a8b452d  
46bee59,5b436a31f4534ded  
7799d9e,1ae76c959ece4216
```

Buttons at the bottom: "PREVIEW AND SAVE" and "CANCEL".

Image 19: Import TOTP Hard Tokens.

- To import TOTP Hard Tokens click the *Bulk Import* button.
- Copy and paste the CSV file containing the Serial Number and Shared Secret of your TOTP Hard Tokens. The file should be formatted as in the example (Image 19).

- Click on the *Preview and Save* button to check if the pasted content is properly parsed.
- Click on the *Save Tokens* button.
- After saving, find the newly added TOTP Hard Tokens in the tokens table under the "Hard Token Management" tab.

*Add HOTP Hard Tokens:*

*Image 20: Add HOTP Hard Tokens.*

- For the token type choose HOTP.
- Choose the number of HOTP Hard Tokens you want to add
- Choose the secure hash algorithm type (SHA1, SHA256 or SHA512).
- Write down the: Serial Number and Shared Secret of the HOTP Hard Token in the specified fields.
- Click the *Save Tokens* button.
- After saving, find the newly added HOTP Hard Tokens in the tokens table under the "Hard Token Management" tab.

*Import HOTP Hard Tokens:*

*Image 21: Import HOTP Hard Tokens.*

- To import HOTP Hard Tokens click the *Bulk Import* button.

- Copy and paste the CSV file containing the Serial Number and Shared Secret of your HOTP Hard Tokens. The file should be formatted as in the example (Image 21).
- Click the *Preview and Save* button to check if the pasted content is properly parsed.
- Click on the *Save Tokens* button.
- After saving, find the newly added HOTP Hard Tokens in the tokens table under the "Hard Token Management" tab.

## TOKEN CONFIGURATION & EDITS

If you ever configure any of your physical tokens, make sure to keep it synced with SAASPASS. In order to do that, find the token under the "Hard Token Management" tab and click on *Manage* button.

The screenshot displays the SAASPASS administration interface for FIDO2 & Hard Tokens. At the top, there are navigation elements including 'SAASPASS', 'CompanyDOO / FIDO2 & Hard Tokens', and user information. Below this is a search bar and a section titled 'FIDO2 & Hard Tokens' with a warning message. A row of buttons allows for adding different types of tokens. The main part of the interface is a table with the following data:

| SERIAL NUMBER | TYPE                   | STATUS                        | SAASPASS USER | ACTIONS       |
|---------------|------------------------|-------------------------------|---------------|---------------|
| 5313745       | HOTP USB Key           | ACTIVE<br>No account assigned | 024421774     | MANAGE DELETE |
| 6317655       | TOTP - SHA1            | ACTIVE<br>No account assigned | 962545390     | MANAGE DELETE |
| Pauline       | FIDO2 & U2F            | ACTIVE<br>No account assigned | 249440402     | MANAGE DELETE |
| 731254        | HOTP - SHA256          | ACTIVE<br>No account assigned | 032312943     | MANAGE DELETE |
| Yubico Test   | YubiKey USB (non FIDO) | ACTIVE<br>No account assigned | 663459512     | MANAGE DELETE |

At the bottom of the table, it indicates 'Total records: 5'. Below the table are several navigation buttons: 'HELP', 'YUBICO STORE', 'YUBIKEY EXPERIENCE PACK', 'BUY HYPERSECU', and 'GENERIC HARD TOKEN SYNC URL'.

Image 22: Edit Token.

### Yubikey Token Configuration

YubiKey devices featuring Yubico OTP and OATH-HOTP authentication methods (standards) need specific configurations in order to work with SAASPASS. SAASPASS supports both (Yubico OTP and OATH-HOTP) authentication methods and also supports other USB keys based on the OATH-HOTP standard.

To set up the token, go to the [Yubico Support page](#) and download the [Yubico Personalization Tool](#).

For login, users just need to plug the USB key into their computer, select the One-Time Password field on the login form, and press the USB key button. The Login form will be auto-filled and submitted.

### Yubico OTP (non-FIDO U2F) Token Configuration

To set up the Yubico OTP (non-FIDO U2F) token, click the *Manage* button for the YubiKey USB (non-FIDO) token type previously added. This is listed in the tokens table under the "Hard Token Management" tab. (Image 22).

The Hard Token Management window will appear and you can edit the following settings:

- Token Serial Number
- Public Identity
- Private Identity
- Shared Secret value

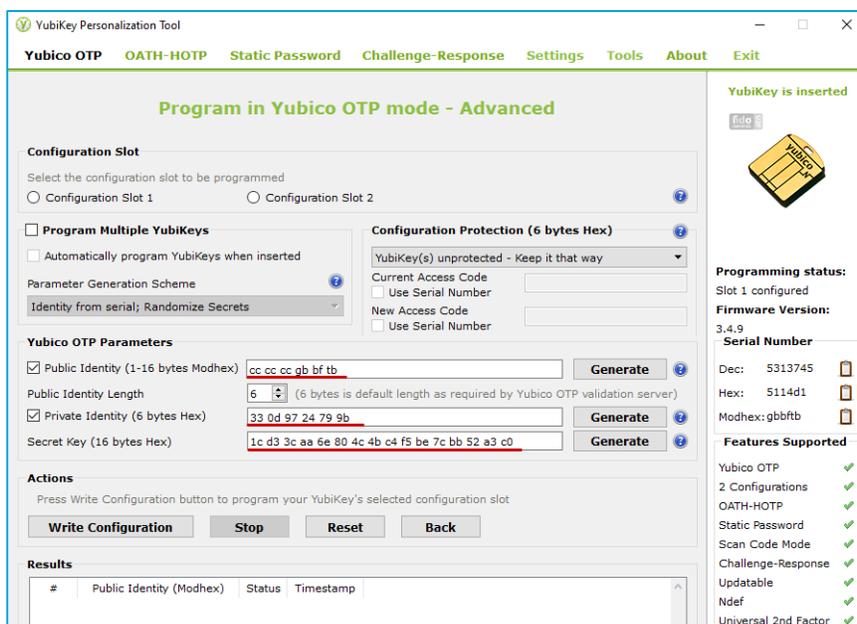
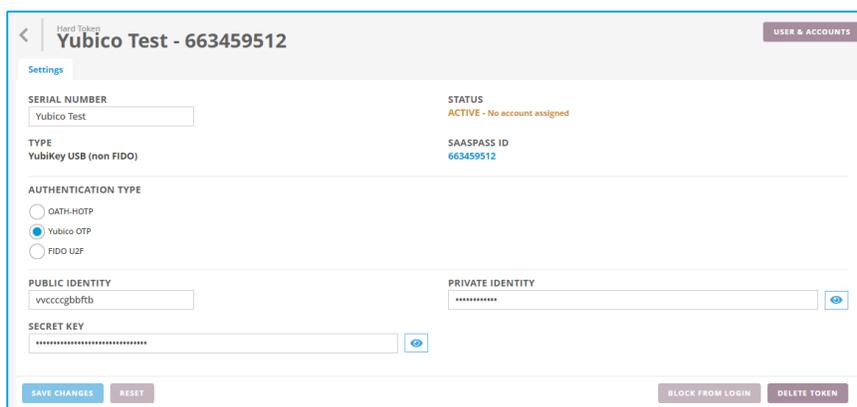
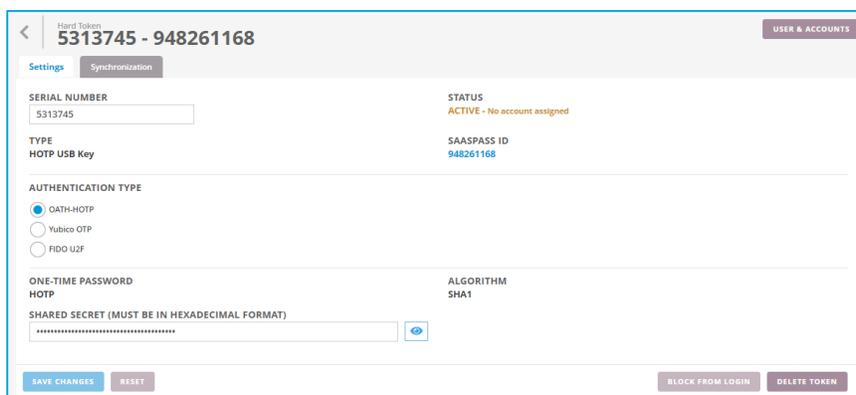


Image 23: Edit Yubico OTP (non-FIDO U2F) Token.

## USB OATH-HOTP Token Configuration

To set up the USB OATH-HOTP token, click the EDIT button for the HOTP USB Key token type previously added and listed in the tokens table under the "Hard Token Management" tab (Image 22). The Hard Token Management window will appear and you can edit the following settings:

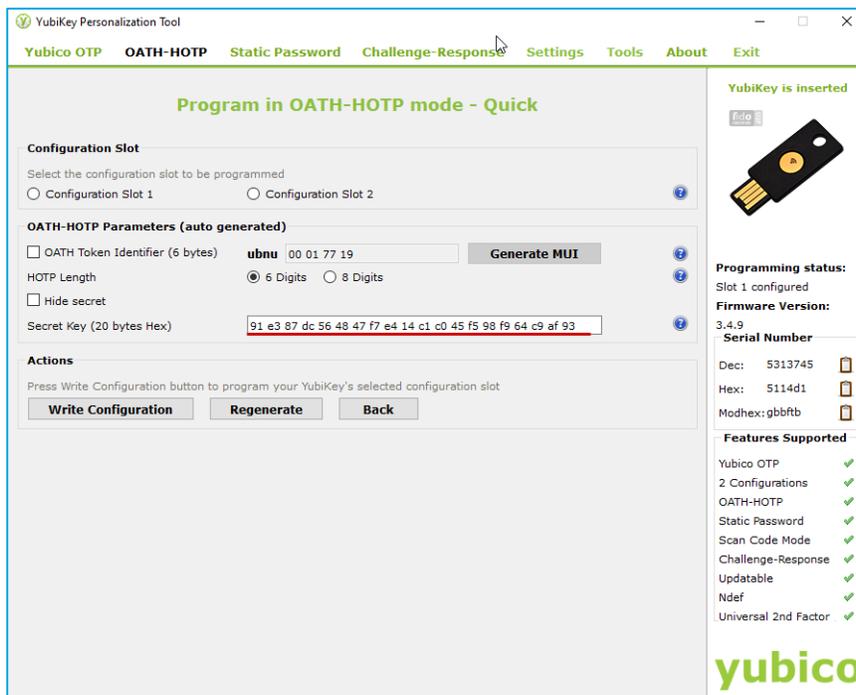
- Token Serial Number
- Shared Secret value



The screenshot shows the 'Hard Tokens' management interface. At the top, the token ID is '5313745 - 948261168'. The 'Settings' tab is active, showing the following configuration:

- SERIAL NUMBER:** 5313745
- STATUS:** ACTIVE - No account assigned
- TYPE:** HOTP USB Key
- SAASPASS ID:** 948261168
- AUTHENTICATION TYPE:** OATH-HOTP (selected), Yubico OTP, FIDO U2F
- ONE-TIME PASSWORD:** HOTP
- ALGORITHM:** SHA1
- SHARED SECRET (MUST BE IN HEXADECIMAL FORMAT):** A field with a masked secret value and a copy icon.

Buttons at the bottom include 'SAVE CHANGES', 'RESET', 'BLOCK FROM LOGIN', and 'DELETE TOKEN'.



The screenshot shows the 'YubiKey Personalization Tool' interface. The 'OATH-HOTP' tab is selected. The main area is titled 'Program in OATH-HOTP mode - Quick'.

**Configuration Slot:** Select the configuration slot to be programmed. Radio buttons for 'Configuration Slot 1' and 'Configuration Slot 2' are present.

**OATH-HOTP Parameters (auto generated):**

- OATH Token Identifier (6 bytes) **ubnu** 00 01 77 19 **Generate MUI**
- HOTP Length:  6 Digits  8 Digits
- Hide secret
- Secret Key (20 bytes Hex): 91 e3 87 dc 56 48 47 f7 e4 14 c1 c0 45 f5 98 f9 64 c9 af 93

**Actions:** Press Write Configuration button to program your YubiKey's selected configuration slot. Buttons: **Write Configuration**, **Regenerate**, **Back**.

**YubiKey is inserted:** A USB key icon is shown.

**Programming status:** Slot 1 configured

**Firmware Version:** 3.4.9

**Serial Number:** Dec: 5313745, Hex: 5114d1, Modhex: gbbftb

**Features Supported:**

- Yubico OTP ✓
- 2 Configurations ✓
- OATH-HOTP ✓
- Static Password ✓
- Scan Code Mode ✓
- Challenge-Response ✓
- Updatable ✓
- Ndef ✓
- Universal 2nd Factor ✓

The Yubico logo is visible at the bottom right.

Image 24: Edit USB OATH-HOTP Token.

**Important:** On Image 24, it describes how to set up token specifications for YubiKey devices that support the OATH-HOTP standard.

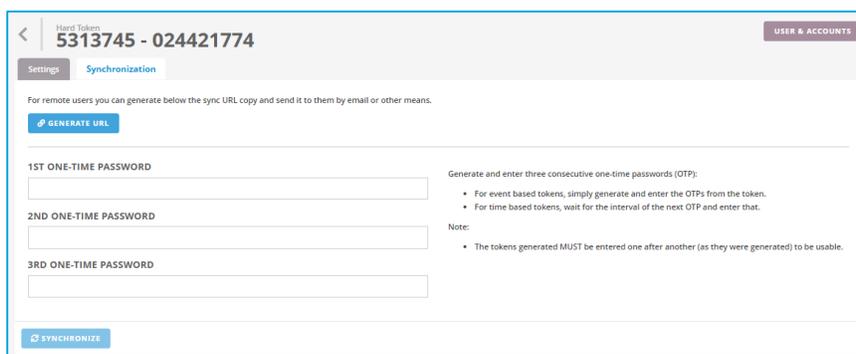
## USB OATH-HOTP (Event Based) Token Synchronization

USB OATH-HOTP tokens are event-based (counter-based). YubiKey tokens may be event-based (HOTP) if the device is supporting the OATH-HOTP standard. This means they generate one-time passwords only when it is requested (usually pressing the button on the token). It's up to the user how many one-time passwords to generate, so it's easy that the token and SAASPASS servers will go out of sync. When the token and SAASPASS are out of sync, the one-time password will not work.

After the token is integrated with SAASPASS for the first time, it must be synchronized. Locate the USB OATH-HOTP token in the tokens table under the "Hard Token Management" tab and click the *Manage* button and then navigate to the "Synchronization" tab.

**Important:** If the token goes out of sync, you will need to synchronize the token again.

When the synchronization window appears, generate three one-time passwords in a row, then submit. The SAASPASS server will synchronize the tokens.



The screenshot shows a web interface for token synchronization. At the top, it displays "Hard Token" and the ID "5313745 - 024421774". There are tabs for "Settings" and "Synchronization". A "GENERATE URL" button is visible. Below, there are three input fields labeled "1ST ONE-TIME PASSWORD", "2ND ONE-TIME PASSWORD", and "3RD ONE-TIME PASSWORD". To the right of these fields, there is a section titled "Generate and enter three consecutive one-time passwords (OTP):" with two bullet points: "For event based tokens, simply generate and enter the OTPs from the token." and "For time based tokens, wait for the interval of the next OTP and enter that." Below this is a "Note:" section with one bullet point: "The tokens generated MUST be entered one after another (as they were generated) to be usable." At the bottom, there is a "SYNCHRONIZE" button.

Image 25: Synchronize USB OATH-HOTP Token.

In case you don't have the token with you to generate the OTPs, you can generate a URL and send it to the user of the out-of-sync token. The URL opens a page where the user is able to submit the three OTPs required for the synchronization (Image 26).

Settings Synchronization

For remote users you can generate below the sync URL copy and send it to them by email or other means.

https://www.saaspass.com/sd/#/htsync/9f8sh7jCC3wppmRaGI9nwdStqkk80Fis

1ST ONE-TIME PASSWORD

2ND ONE-TIME PASSWORD

3RD ONE-TIME PASSWORD

Generate and enter three consecutive one-time passwords (OTP):

- For event based tokens, simply generate and enter the OTPs from the token.
- For time based tokens, wait for the interval of the next OTP and enter that.

Note:

- The tokens generated MUST be entered one after another (as they were generated) to be usable.

Image 26: Generate URL for USB OATH-HOTP Token synchronization.

Also, the user can synchronize a token anytime without needing the admin to generate a URL. For that, a user should go to the [SAASPASS Hard Token Synchronization page](#) and enter the three OTPs plus the serial number displayed on the hard token.

## HARD TOKEN (TOTP and HOTP) CONFIGURATION

### TOTP Hard Token Configuration

To set up the TOTP Hard Token, click the *Manage* button for the TOTP Token type previously added and listed in the tokens table under the "Hard Token Management" tab (Image 22).

When the Hard Token Management window appear, you will be able to edit the following settings:

- Token Serial Number.
- One-time password type (time based TOTP or event based HOTP).
- Algorithm (SHA1, SHA256 or SHA512).
- OTP generation time in seconds (only for time-based generation tokens).
- Shared Secret value.

Hard Token 6317655 - 962545390

Settings Synchronization

SERIAL NUMBER: 6317655

TYPE: TOTP - SHA1

ONE-TIME PASSWORD:  TOTP,  HOTP

TOTP GENERATION TIME (SECONDS): 30

ALGORITHM:  SHA1,  SHA256,  SHA512

SHARED SECRET (MUST BE IN HEXADECIMAL FORMAT): [masked]

Image 27: Edit TOTP Hard Token.

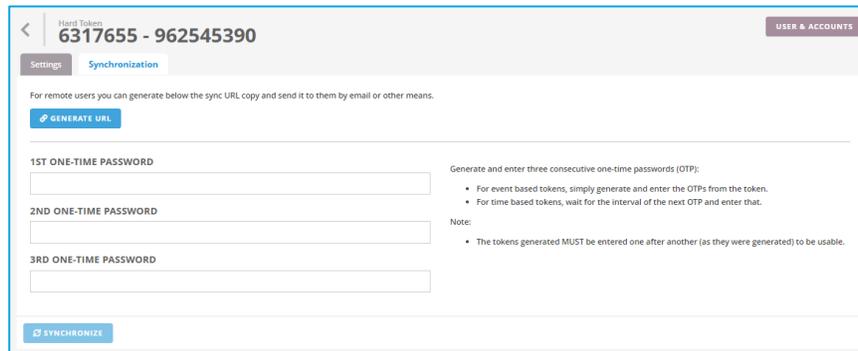
## TOTP (EVENT-BASED) HARD TOKEN SYNCHRONIZATION

When Hard Tokens are event-based (TOTP), they generate one-time passwords only when prompted (usually by pressing the button on the token). AS it's up to the user how many one-time passwords to generate, it's easier for the token and the SAASPASS servers to become out of sync. When the token and SAASPASS are out of sync, the one-time password generated will not work.

When a token is integrated with SAASPASS for the first time, it must be synchronized. Locate the TOTP Hard Token in the tokens table under the "Hard Token Management" tab and click the *Manage* button and then navigate to the "Synchronization" tab.

**Important:** A token must be synchronized anytime it becomes out of sync.

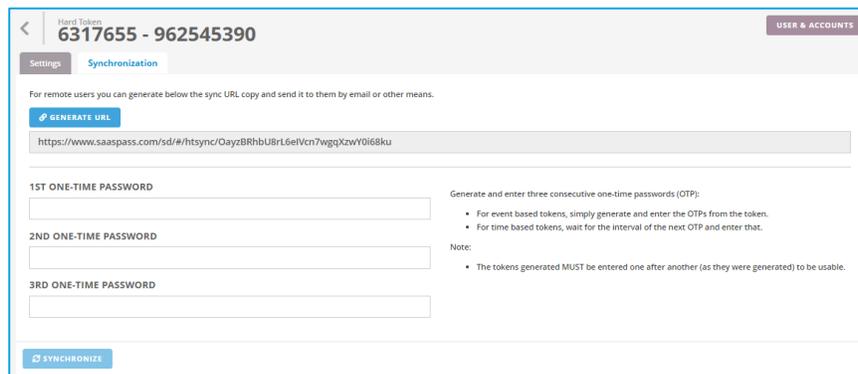
In the synchronization window, generate three one-time passwords in a row, then submit. SAASPASS will synchronize the token.



The screenshot shows the 'Synchronization' tab for a hard token with ID 6317655 - 962545390. It features a 'GENERATE URL' button and three input fields for '1ST ONE-TIME PASSWORD', '2ND ONE-TIME PASSWORD', and '3RD ONE-TIME PASSWORD'. A 'SYNCHRONIZE' button is at the bottom. Instructions and a note are provided on the right side of the form.

Image 28: Synchronize TOTP Hard Token.

When you don't have the token with you, you can generate a URL and send it to the user of the out-of-sync token. The URL opens a page where the user can submit the three OTPs required for the synchronization.



This screenshot is identical to the previous one, but the 'GENERATE URL' button has been clicked, and a URL is displayed in the input field: <https://www.saaspass.com/sd/#/htsync/OayzBRhbURl6elVcn7wggKzwY0i68ku>.

Image 29: Generate URL for Hard Token synchronization.

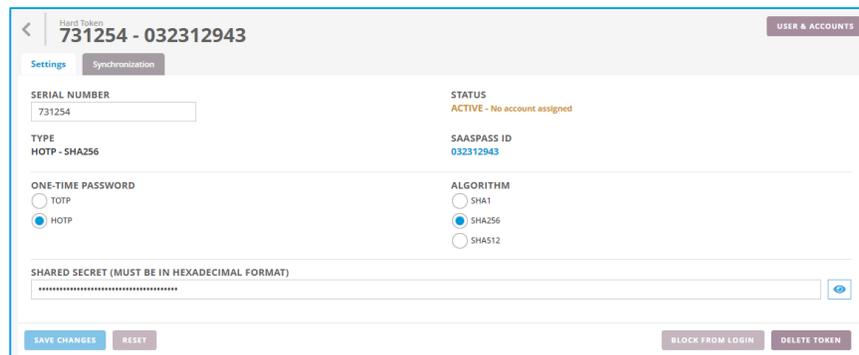
The user can also synchronize a token anytime without needing the admin to generate a URL. In order to do that, a user should go to the [SAASPASS Hard Token Synchronization page](#) and enter the three OTPs plus the serial number displayed on the hard token.

## HOTP HARD TOKEN CONFIGURATION

To set up the HOTP Hard Token, click the *Manage* button for the HOTP Token type previously added and listed in the tokens table under the "Hard Token Management" tab (Image 22).

When the Hard Token Management window appears, you will be able to edit the following settings:

- Token Serial Number.
- One-time password type (event based HOTP).
- Algorithm (SHA1, SHA256 or SHA512).
- Shared Secret value.



The screenshot shows the 'Hard Token Management' window for a specific token. The token ID is '731254 - 032312943'. The 'Settings' tab is active, and the 'Synchronization' sub-tab is selected. The configuration includes:

|   |   |                                    |   |
|---|---|------------------------------------|---|
| SERIAL NUMBER                                 | 731254  | STATUS                             | ACTIVE - No account assigned  |
| TYPE  | HOTP - SHA256   | SAASPASS ID                        | 032312943   |
| ONE-TIME PASSWORD                             | <input type="radio"/> TOTP<br><input checked="" type="radio"/> HOTP | ALGORITHM                          | <input type="radio"/> SHA1<br><input checked="" type="radio"/> SHA256<br><input type="radio"/> SHA512 |
| SHARED SECRET (MUST BE IN HEXADECIMAL FORMAT) |   | <input type="text" value="*****"/> |   |

At the bottom, there are buttons for 'SAVE CHANGES', 'RESET', 'BLOCK FROM LOGIN', and 'DELETE TOKEN'.

Image 30: Edit HOTP Hard Token.

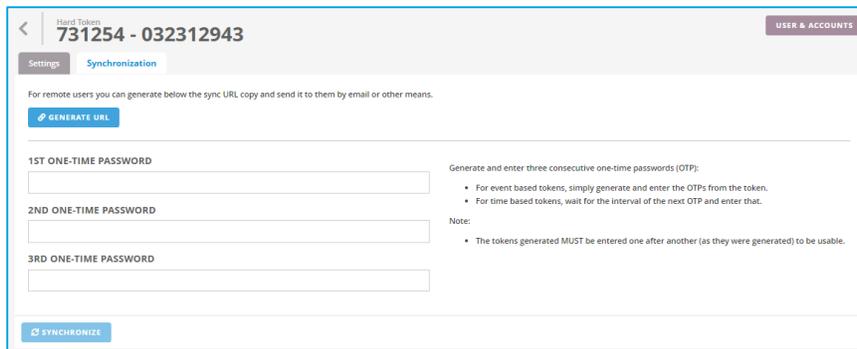
## HOTP (EVENT-BASED) HARD TOKEN SYNCHRONIZATION

When Hard Tokens are event-based (HOTP), they generate one-time passwords only when prompted (usually by pressing the button on the token). Because it's up to the user how many one-time passwords to generate, it's easier for the token and the SAASPASS servers to become out of sync. When the token and SAASPASS are out of sync, the one-time password generated will not work.

When a token is integrated with SAASPASS for the first time, it must be synchronized. Locate the HOTP Hard Token in the tokens table under the "Hard Token Management" tab and click the *Manage* button and then navigate to the "Synchronization" tab.

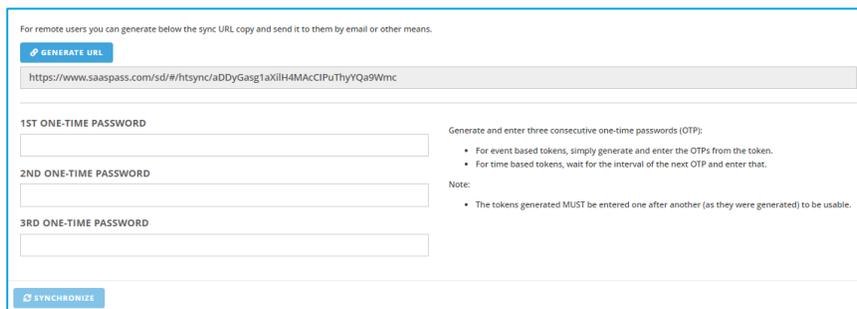
**Important:** If the token goes out of sync, you will need to synchronize the token again.

When the synchronization window appears, generate three one-time passwords in a row, then submit. The token will be synchronized with the SAASPASS server.



*Image 31: Synchronize HOTP Hard Token.*

In case you don't have the token with you to generate the OTPs, you can generate a URL and send it to the user of the out-of-sync token. The URL opens a page where the user can submit the three OTPs required for the synchronization.



*Image 32: Generate URL for Hard Token synchronization.*

The user can also synchronize a token anytime without needing the admin to generate a URL. In order to do that, a user should go to the [SAASPASS Hard Token Synchronization page](#) and enter the three OTPs plus the serial number displayed on the hard token.

## ***FIDO U2F TOKEN CONFIGURATION***

In order to use the FIDO U2F token with SAASPASS, you must complete the token registration process specific to this type of token.

### **REGISTER FIDO U2F TOKEN**

- Locate the FIDO U2F token in the tokens table under the "Hard Token Management" tab and click the *Manage* button. The Hard Token Management window will appear with the FIDO settings.

- Next, navigate to the “Registration” tab and plug in your FIDO U2F token and click the *Register Token* button as shown in Image 33.

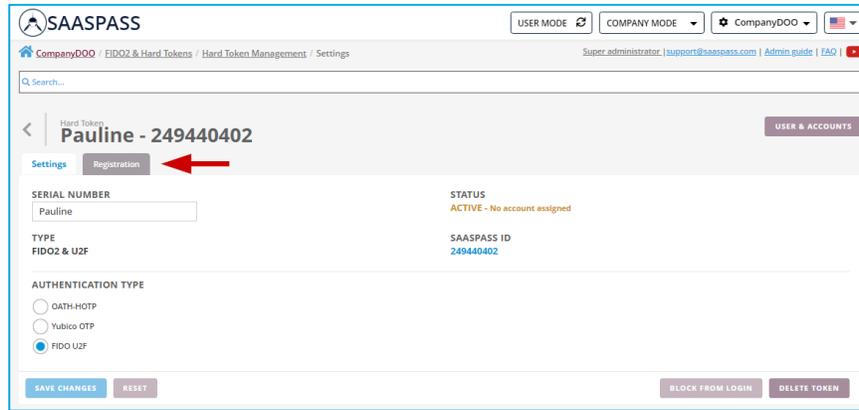


Image 33: Register FIDO U2F Token.

- When a message appears that the registration has started, touch your FIDO U2F token. A new message should now appear that the registration has been completed successfully (as shown in Image 34).

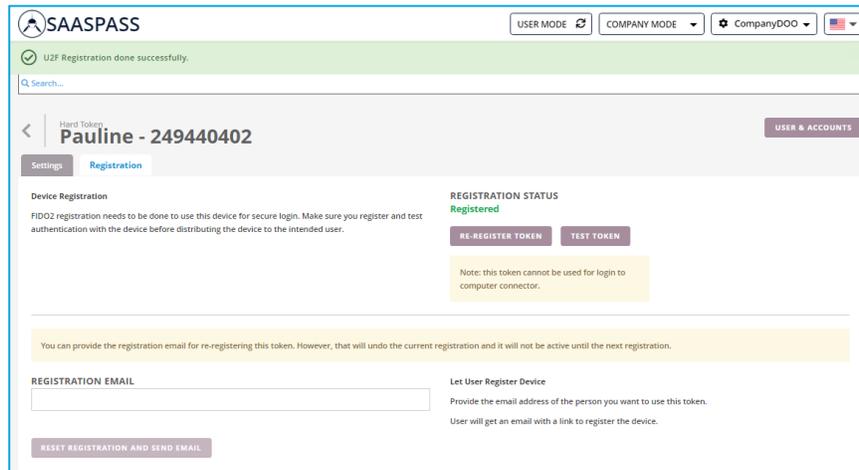
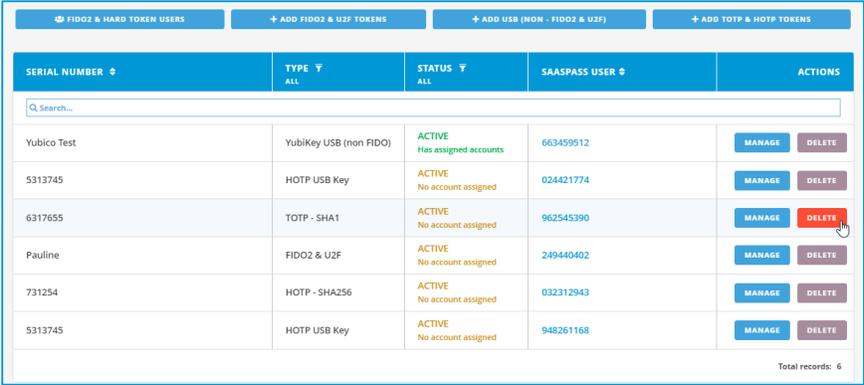


Image 34: Successful FIDO U2F Token registration.

## DELETE HARD TOKEN

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

To delete a hard token, go to the "Hard Token Management" tab and click the *Delete* button next to the hard token type you want to delete from SAASPASS (see Image 33).

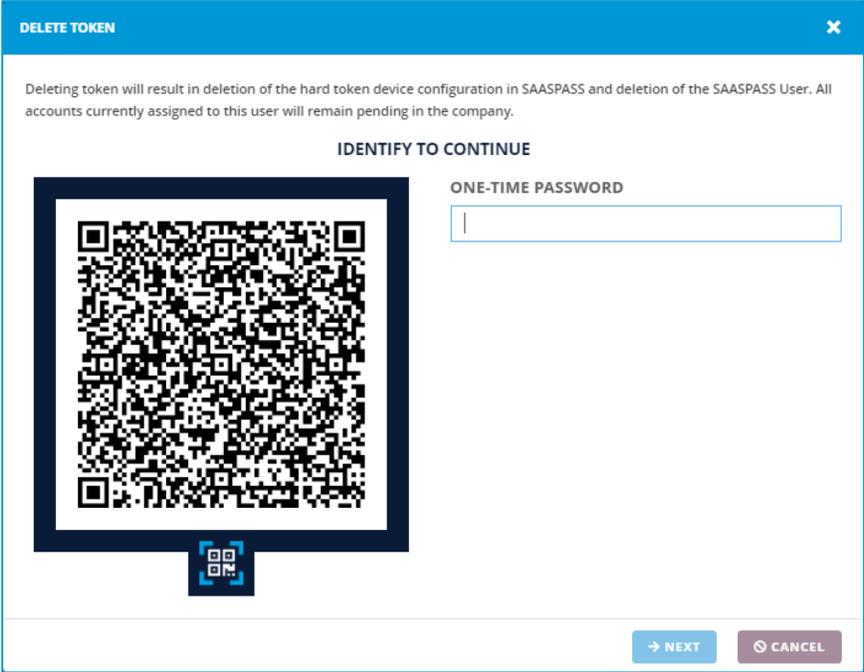


| SERIAL NUMBER | TYPE                   | STATUS                          | SAASPASS USER | ACTIONS       |
|---------------|------------------------|---------------------------------|---------------|---------------|
| Yubico Test   | YubiKey USB (non FIDO) | ACTIVE<br>Has assigned accounts | 663459512     | MANAGE DELETE |
| 5313745       | HOTP USB Key           | ACTIVE<br>No account assigned   | 024421774     | MANAGE DELETE |
| 6317655       | TOTP - SHA1            | ACTIVE<br>No account assigned   | 962545390     | MANAGE DELETE |
| Pauline       | FIDO2 & U2F            | ACTIVE<br>No account assigned   | 249440402     | MANAGE DELETE |
| 731254        | HOTP - SHA256          | ACTIVE<br>No account assigned   | 032312943     | MANAGE DELETE |
| 5313745       | HOTP USB Key           | ACTIVE<br>No account assigned   | 948261168     | MANAGE DELETE |

Total records: 6

Image 35: 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 36.



**DELETE TOKEN** [X]

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 36: Required identification for delete operation.

A message will be displayed when the token is successfully deleted, as shown in Image 37.

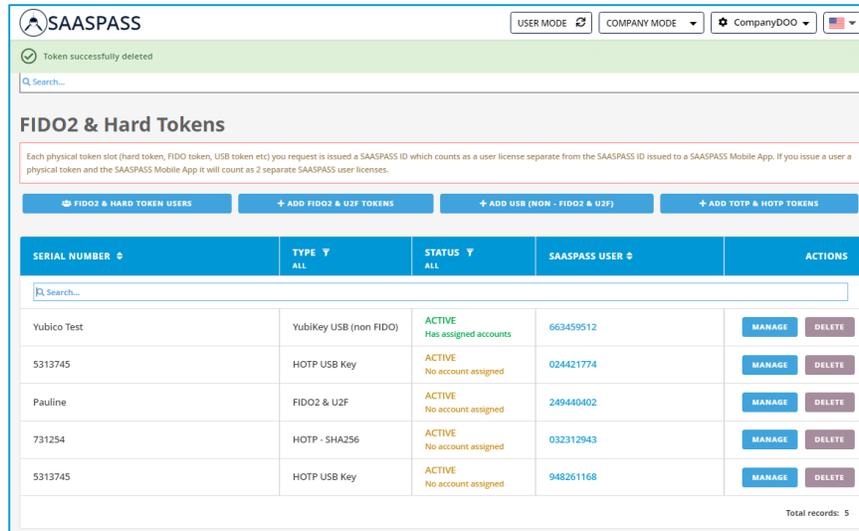


Image 37: Hard Token successfully deleted.

## HARD TOKEN USAGE

This section describes how and where to use the hard token to login. In SAASPASS, hard token login is supported in: the web portal, SAML applications web pages, and the desktop SSO and Computer Login screens in Windows connectors.

### Hard Token login on SAASPASS Web Portal

Users can login from the web portal by clicking the *Hard/USB Token* button or they can go directly to the [FIDO2 / USB and Hard Token Login](#) physical token page.

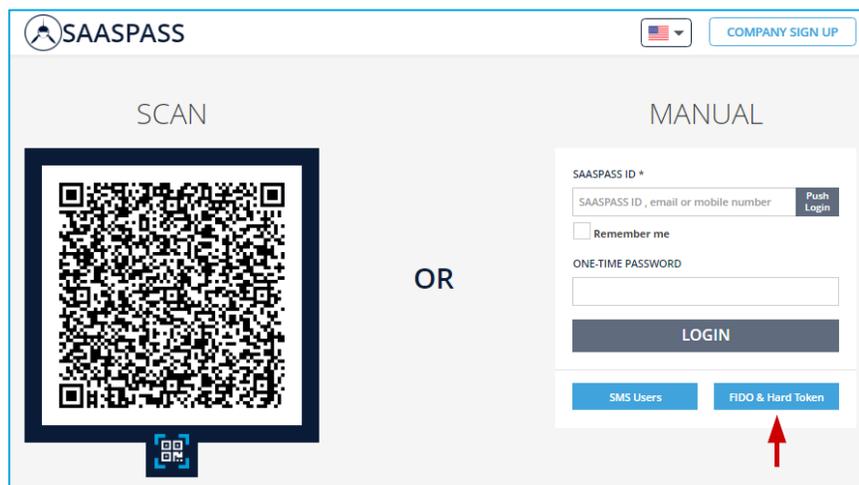
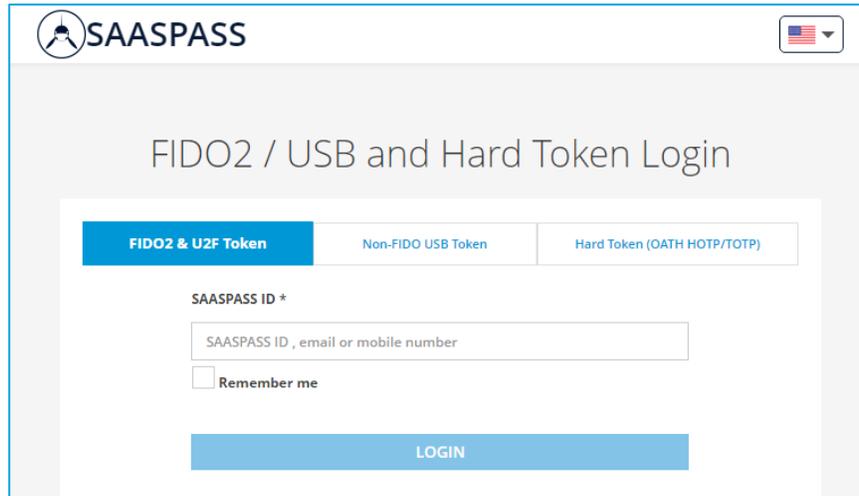


Image 38: Hard Token login on web portal.

Next, they should pick the relevant token type: FIDO U2F Token, Non-FIDO USB Token (OATH HOTP/TOTP) or Hard Token (OATH HOTP/TOTP).

Also, users can check the "**Remember me**" box to avoid manually typing in their static credentials again.

### FIDO U2F Token login on SAASPASS Web Portal



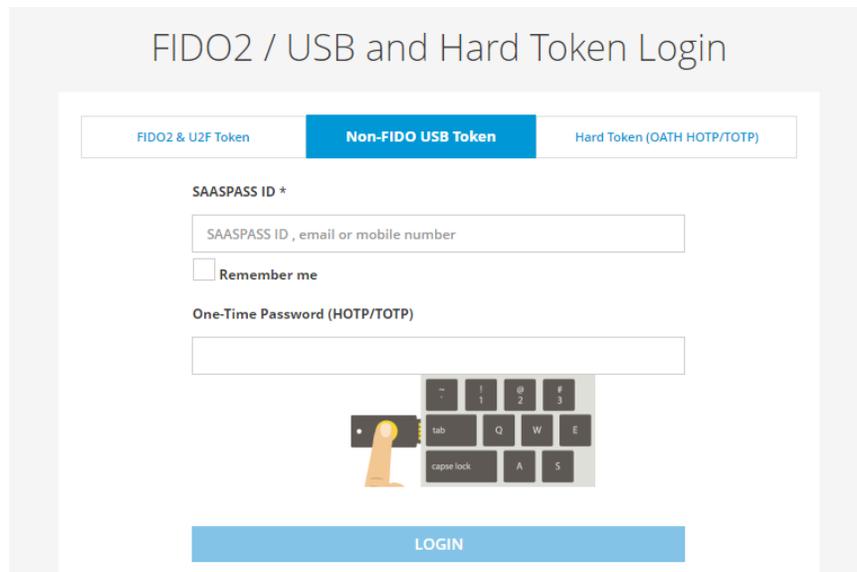
The screenshot shows the SAASPASS web portal interface. At the top left is the SAASPASS logo, and at the top right is a language selection dropdown showing the US flag. The main heading is "FIDO2 / USB and Hard Token Login". Below this, there are three tabs: "FIDO2 & U2F Token" (which is highlighted in blue), "Non-FIDO USB Token", and "Hard Token (OATH HOTP/TOTP)". The "FIDO2 & U2F Token" tab contains a form with the following elements: a label "SAASPASS ID \*", a text input field with the placeholder "SAASPASS ID , email or mobile number", a checkbox labeled "Remember me", and a blue "LOGIN" button at the bottom.

Image 39: FIDO U2F Token login on SAASPASS Web Portal.

### Non-FIDO USB Token login on SAASPASS Web Portal

Choose the token type to login with your YubiKey:

- Yubico OTP (non-FIDO U2F) Token
- OATH-HOTP Token



The screenshot shows the SAASPASS web portal interface with the "Non-FIDO USB Token" tab selected. The form includes a "SAASPASS ID \*" field with the placeholder "SAASPASS ID , email or mobile number", a "Remember me" checkbox, and a "One-Time Password (HOTP/TOTP)" field. Below the password field is a graphic of a YubiKey and a portion of a keyboard showing the top row of keys (tab, Q, W, E, caps lock, A, S). A blue "LOGIN" button is at the bottom.

Image 40: Non-FIDO USB Token login on SAASPASS Web Portal.

## Hard Token login on SAASPASS Web Portal

FIDO2 / USB and Hard Token Login

FIDO2 & U2F Token    Non-FIDO USB Token    **Hard Token (OATH HOTP/TOTP)**

SAASPASS ID \*

55555555

Remember me

One-Time Password (HOTP/TOTP)

LOGIN

Image 41: Hard Token login on SAASPASS Web Portal.

## Hard Token login on SAASPASS SAML Company Apps

Hard token users can login to the SAML Company applications for which the user has been provisioned by the company's administrator.

From the SAML webpage for the given application, users can login by clicking the *Hard / USB Token* button. The Microsoft365 SAML app is given as an example to describe the hard token login.

Next, select the relevant token type: FIDO U2F Token, Non-FIDO USB Token (OATH HOTP/TOTP) or Hard Token (OATH HOTP/TOTP).

WELCOME TO MICROSOFT 365

Microsoft 365

SCAN    OR    MANUAL

EMAIL

Email    Push Login

Remember me

ONE-TIME PASSWORD

LOGIN

GO TO SAASPASS    FIDO & Hard Token

Image 42: Hard Token login on SAASPASS SAML Apps.

## Hard Token login with SAASPASS Connectors

Login with hard tokens is supported with Windows SAASPASS Connector. There are two login points where hard tokens can be used for login with the connector. The first is the login in the Desktop SSO, and the second is the login on the SAASPASS protected screens. In order to access, hard token users must first be provisioned by their administrator to the Computer Login company application.

**Important:** The hard token login feature is supported only for the company user accounts for corporate usage and only on domain-bound computers. It is not supported for personal user accounts.

### Hard Token login with Windows SAASPASS Connector

Using the Windows SAASPASS Connector, we enforce protection on: login screen and unlock screen. On each of these screens, login with hard token is supported for the hard token users that have been provisioned for the Computer Login application.

**Important:** Windows SAASPASS Connector only supports login with (HOTP/TOTP) Hard Token and Non-FIDO USB Tokens types (as YubiKey - Yubico OTP and OATH-HOTP). **Currently, login with FIDO U2F is not supported! It is on the roadmap and it will be supported within Q2 2023.**

### Hard Token login on Main and Unlock Login Screens

On Windows systems, the hard token login process for both the login and unlock screens is the same.

### Login from the Other User Tile

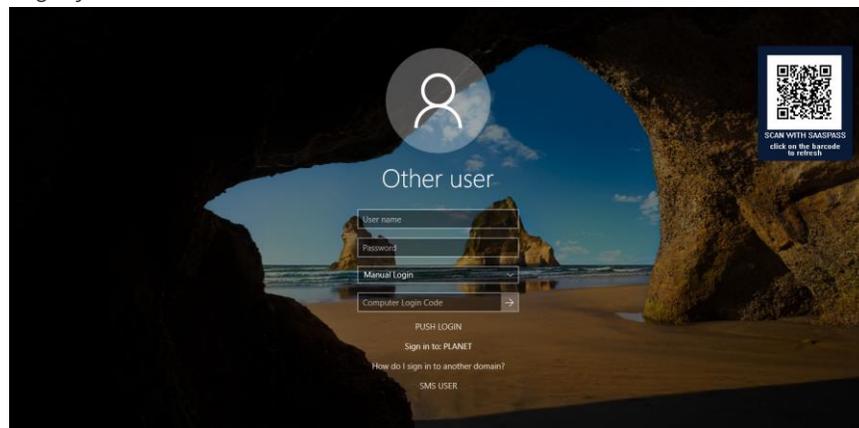


Image 43: Login with Token from Other Tile.

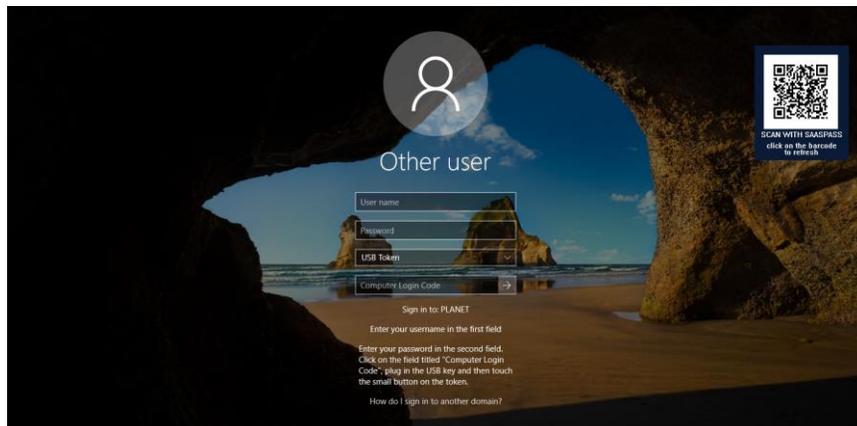
## USB (Non-FIDO U2F) tokens:

### Yubico OTP (non-FIDO U2F)

- Click the Other user tile displayed on the login/unlock screen.
- Enter your username in the first field.
- Enter your computer's password in the second field.
- From the third field click and choose USB Token.
- Click on the fourth field titled "Computer Login Code".
- Plug in the USB key (Yubico OTP), and then press the small button on the token to login.

### USB OATH-HOTP

- Click the Other user tile displayed on the login/unlock screen.
- Enter your username in the first field.
- Enter your computer's password in the second field.
- From the third field click and choose USB Token.
- Click on the fourth field titled "Computer Login Code".
- Plug in the USB key (USB OATH-HOTP), and then press the small button on the token to login.

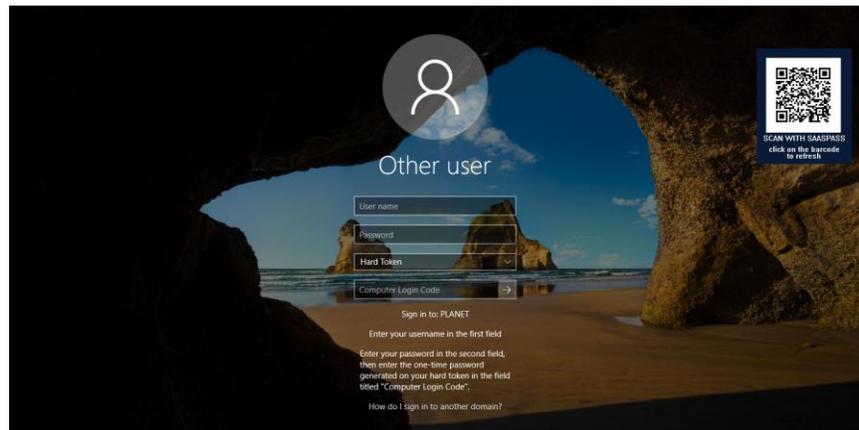


## HOTP/TOTP Hard Token:

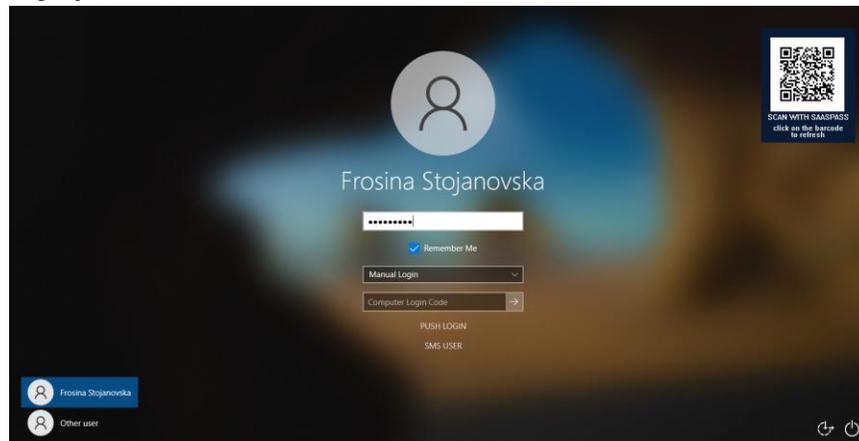
- Click the Other user tile displayed on the login/unlock screen.
- Enter your username in the first field.
- Enter your computer's password in the second field.
- From the third field click and choose Hard Token.
- Enter the one-time password generated on your hard token in the fourth field titled "Computer Login Code".
- Press enter or the login arrow to login.

\*The username in the first entry field in the Other user tile can be written in two formats:

- Enter only the username. Example: Steve.Mills.
- Enter the domain and the username. Example: ROOT\Steve.Mills.



*Login from User Tile*

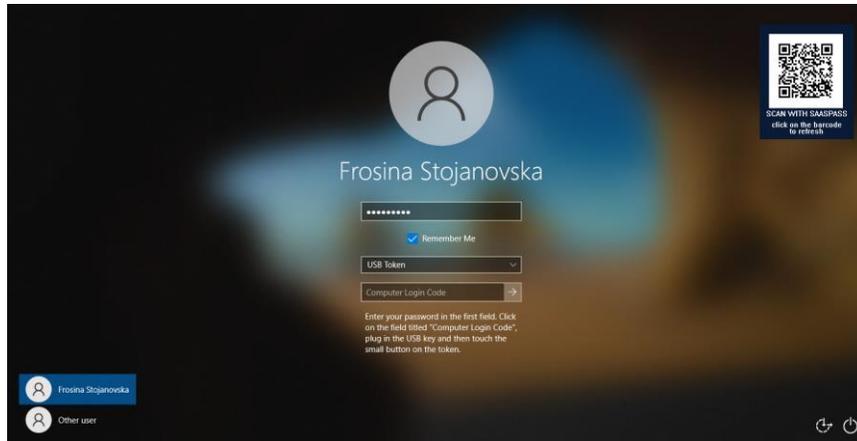


*Image 44: Login with Token from User Tile.*

## **USB (Non-FIDO U2F) tokens:**

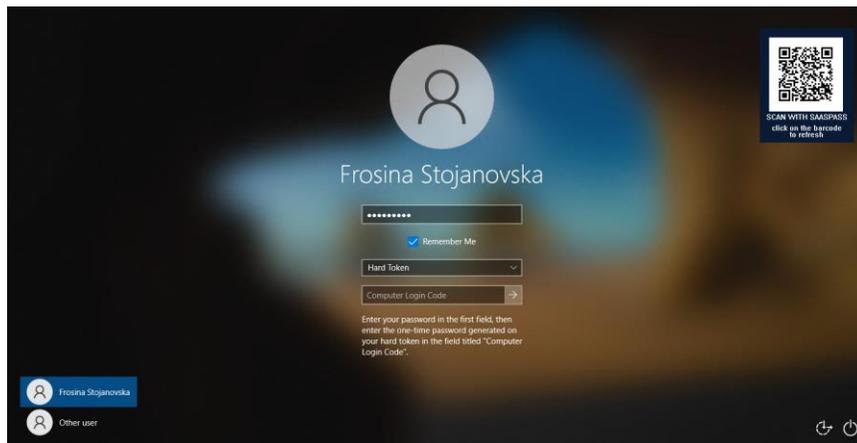
### **Yubico OTP (non-FIDO U2F)**

- Click the User tile displayed on the login/unlock screen.
- Enter your computer's password in the second field.
- From the third field click and choose USB Token.
- Click on the fourth field titled "Computer Login Code".
- Plug in the USB key (Yubico OTP), and then press the small button on the token to login.



### USB OATH-HOTP

- Click the User tile displayed on the login/unlock screen.
- Enter your computer's password in the second field.
- From the third field click and choose USB Token.
- Click on the fourth field titled "Computer Login Code".
- Plug in the USB key (USB OATH-HOTP), and then press the small button on the token to login.



### HOTP/TOTP Hard Token:

- Click the User tile displayed on the login/unlock screen.
- Enter your computer's password in the second field.
- From the third field click and choose Hard Token.
- Enter the one-time password generated on your hard token in the third field titled "Computer Login Code".
- Press enter or the login arrow to login.

### Hard Token login on Windows Desktop SSO App

On the Windows Desktop SSO app, users can login by filling out the SAASSPASS ID or Email in the first entry field and for the OTP field, if you

have a USB token then you need to click in the OTP field, plug the token and touch its button so it will auto fill that field or if you are (TOTP/HOTP) hard token user fill out the OTP manually.

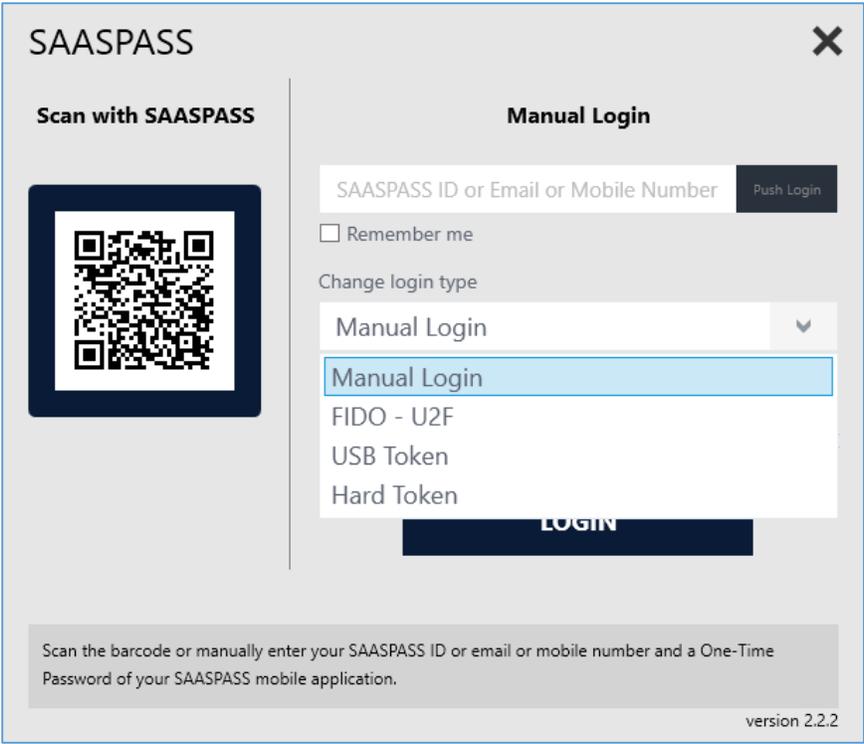


Image 45: Login with Token from Win Desktop SSO App.

---

For any questions, you can always contact us at:  
[support@saaspass.com](mailto:support@saaspass.com)