



# FIDO2 Security Tokens Admin Guide

Instructions for Local Administrators on the use and management of FIDO2 security keys through the NHSmail portal.

# FIDO2 Security Keys Admin Guide

Step by step instructions for Local Administrators on the use and management of FIDO2 security keys through the NHSmail portal.

## CONTENTS



**01**

### FIDO2 OVERVIEW

Introduction to FIDO2 security keys

**02**

### MANAGING SECURITY KEYS

This section provides instructions on how to manage security keys for a user

**03**

### FAQ

This section provides answers to common questions and scenarios.



\*\*\*\*\*





## What is FIDO2

FIDO2 is an open authentication standard developed by the FIDO2 Alliance in collaboration with the World Wide Web Consortium (W3C).

FIDO2 uses public-key cryptography to provide secure and convenient authentication technology. For every account that uses a FIDO2 security key, there is a public and private key that enable services to validate the identity of users and their security key.

Prior to being able to use a FIDO2-enabled security key, users must register their key with the NHSmail platform.

When users then authenticate, their identity can then be verified with a simple action, such as scanning a fingerprint or touching the security key. The NHSmail platform and the user's authenticator conduct a challenge-response to verify that the user is in possession of the correct private key. Each registration uses a unique key pair, and the private key never leaves the user's security key.

For further information, read this [FIDO2 Overview](#) article.

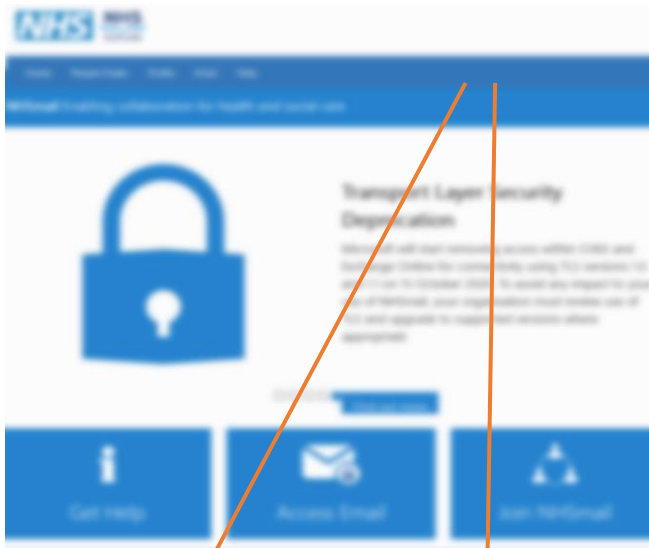


## Navigate to User's FIDO tokens

In order to register a new token for a user, first login to the [NHSmile Portal](#) with your Local Administrator account.

Navigate to the Admin tab, select **User Management** and search for the user that requires security token registration or management. Select the relevant user then click on the **Manage FIDO2 Tokens** button.

This will take you to the FIDO2 management page where you will be able to [register](#), [edit](#) and [remove](#) any FIDO2 security keys for this user.



Manage FIDO2 Tokens

## Register a new token

On the user's FIDO2 token management page, click on the **Register New Token** button.

Insert the token you wish to register for this user and create a PIN for this token (minimum 4 numbers). The user may be prompted for this PIN at a later date, it is therefore important that you share the PIN with the end user in a secure manner.

Once you have registered a PIN you will be asked to tap the security key and provide a valid nickname for the security key. This nickname is used to identify the correct security key during the login process so be sure to give it a recognisable name.

## Edit a token nickname

On the user's FIDO2 token management page, you will see a list of security tokens registered for this user. Click on the **Edit** button next to the security key you wish to change.

Provide a new valid nickname for the security key and click **Save Changes**.

Note that this nickname is used to identify the correct security key during the login process so be sure to give it a recognisable name.

## Remove a token

On the user's FIDO2 token management page, you will see a list of security tokens registered for this user. Click on the **Remove** button next to the specific security key you wish to remove. A new window will pop up to confirm you wish to remove this security key for the user.

Once you have removed a security key, that user will no longer be able to login using that specific security key. This will be effective immediately. Any existing sessions the user may have will last until their next login attempt.

For further guidance, there is a [How-To-Video](#) available to watch with step-by-step instructions on registering and managing a user's FIDO2 token.

## My token is not working

If a user is not able to login with their FIDO2 security token, please ask the user to try the following:

- Check if they have internet connectivity
- Check if it works to login with their token from a different browser (see this further guidance for a [list of supported browsers](#))

You may be able to help by removing the FIDO2 security token from the user's registered tokens and re-registering this again on behalf of the user.

If none of the above resolves the issue, then it may be a problem with the hardware and will need to be investigated further.



## I have forgotten my PIN

If a user needs help resetting their PIN, you will need to have access to the hardware token. A Local Administrator can then reset the security token back to factory settings on a Windows 10 device.

The security token also needs to be removed from the user's registered tokens in the NHSmail Portal and subsequently re-registered with a new PIN. It is important that you share this new PIN with the end user in a secure manner.

## My token has been misplaced / stolen

If a user's token has been stolen, misplaced, or otherwise lost, please make sure to remove the security token from the user's registered tokens in the NHSmail Portal. This is critical as an attacker may attempt to use the token to gain unwarranted access to systems.

It is also advised that you follow local procedures to report this as appropriate. You may also wish to instruct users on how to store tokens securely to prevent a similar incident from occurring again.

