FIDO2 Entering PIN Incorrectly

The process around a user's PIN being blocked due to too many incorrect attempts varies when using a FIDO2 token. This article aims to address these scenarios and provide additional guidance on the following topics to Local Administrators:

- Incorrect PIN entry
- Restarting a login session without removing the security key
- Managing blocked security keys

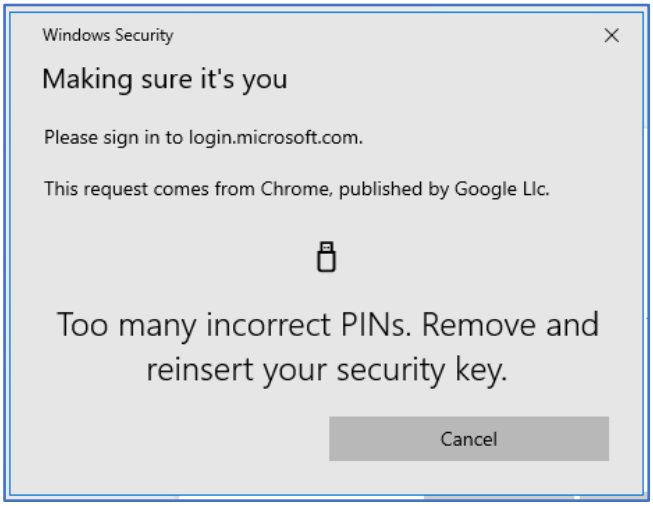
There is also some useful guidance around Help & Support Channels available below.

IMPORTANT NOTE: users can only enter an incorrect PIN for a maximum of **eight** times before the authenticator is blocked and they get locked out.

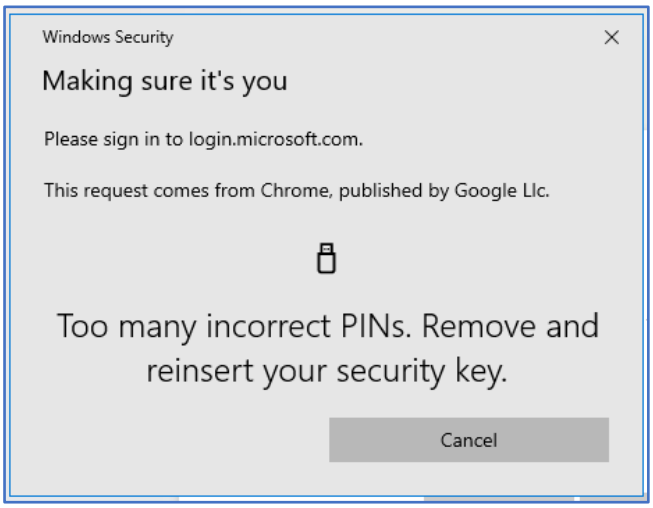
Incorrect PIN Entry

If a user enters the incorrect PIN, they will see the following:

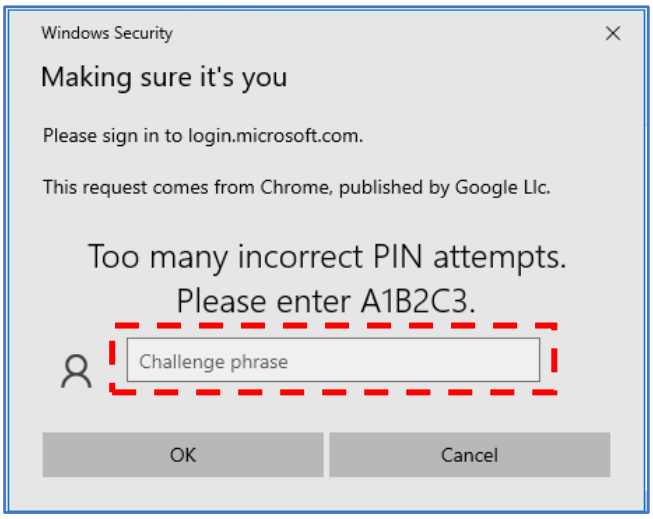
1. After 4 incorrect attempts the user will be presented with a prompt to remove and reinsert the security key



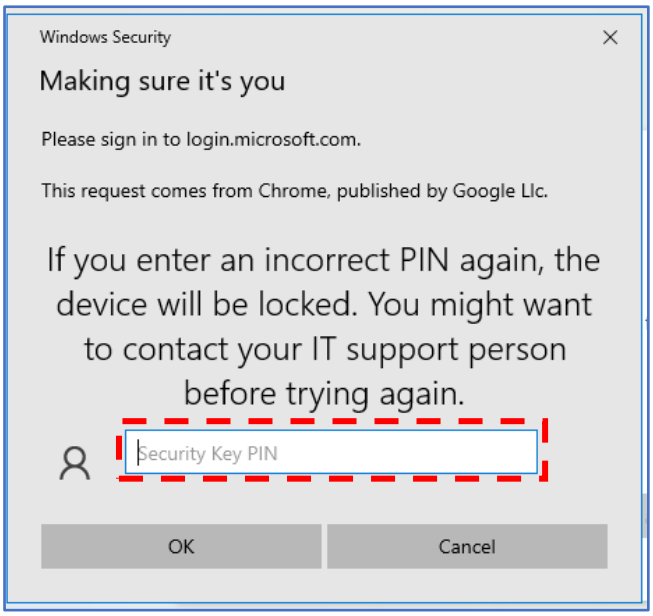
2. After a further 3 incorrect attempts the user will again be presented with a prompt to remove and reinsert the security key



3. The user will then be presented with a Captcha, which they type into the box that reads **Challenge phrase**.



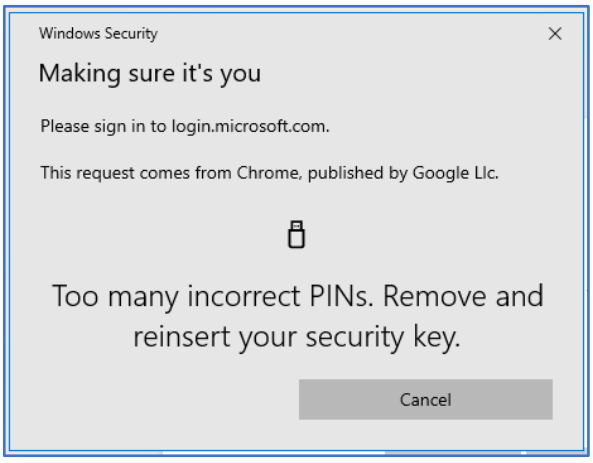
4. If the correct passphrase is entered, the user will be allowed one last attempt to enter the correct PIN with a warning informing them their security key will be locked if the PIN entered is incorrect.



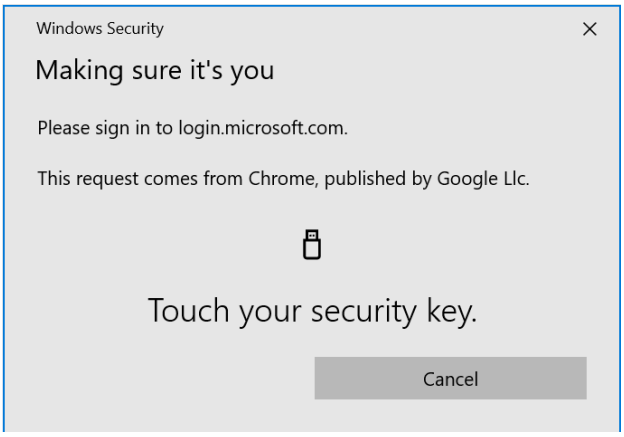
Important Note

During Step 1 or Step 2**,** if the user inputs the correct PIN on the last attempt (i.e on their 4th attempt in Step 1 or 3rd attempt in Step 2), the system will still inform the user that they have entered too many incorrect PINs and will tell them to remove and reinsert their security key before confirming their presence again. See below for how this would look.

a) User enters correct PIN on their last attempt so is prompted with a security message (even though the PIN attempt is correct).



b) After user removes and reinserts the security key, they are required to verify their presence before access is granted.

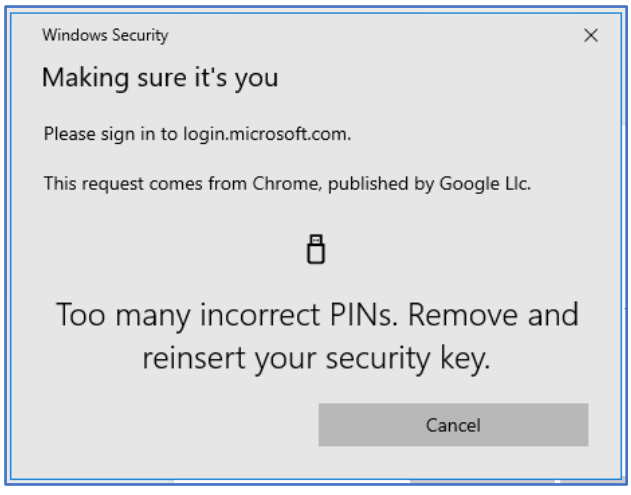


Restarting a Login Session without removing the Security Key

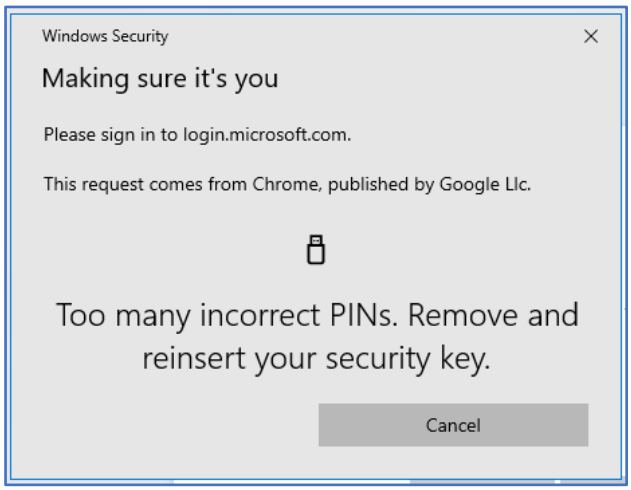
This section provides guidance on what happens if a user enters their PIN incorrectly 4 times, or closes the login session and tries again without removing the security key.

Users should be advised against the practice of closing their login session during an authentication attempt unless there is a genuine reason. If a user does not remove their security key from the USB port when they shut the webpage during an authentication attempt, the following will happen when they reload the session with the FIDO2 token still in place:

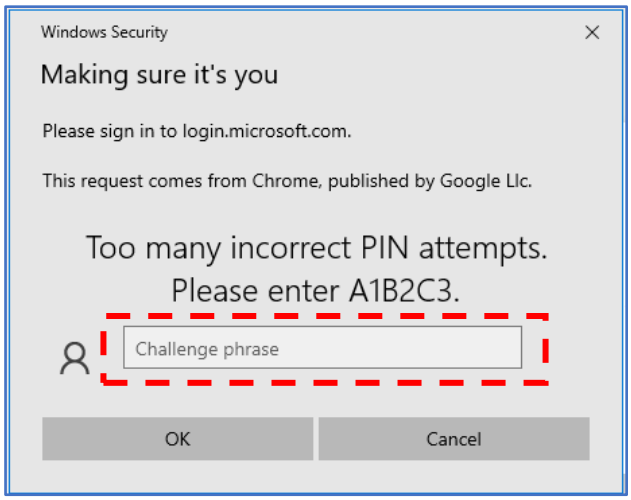
1. The user will get 2 PIN entry attempts. If both are entered incorrectly, they will be presented with a prompt to remove and reinsert the security key.



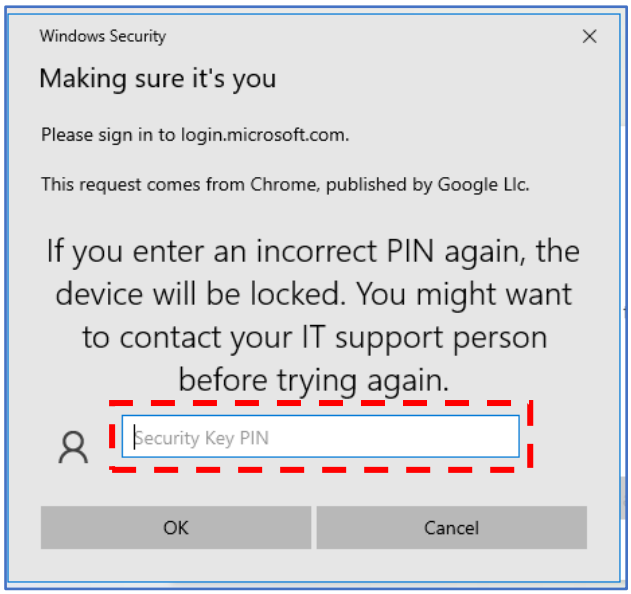
2. After a further 3 incorrect attempts the user will be presented with a prompt to remove and reinsert the security key



3. The user will then be presented with a Captcha, which they type into the box that reads **Challenge phrase.**



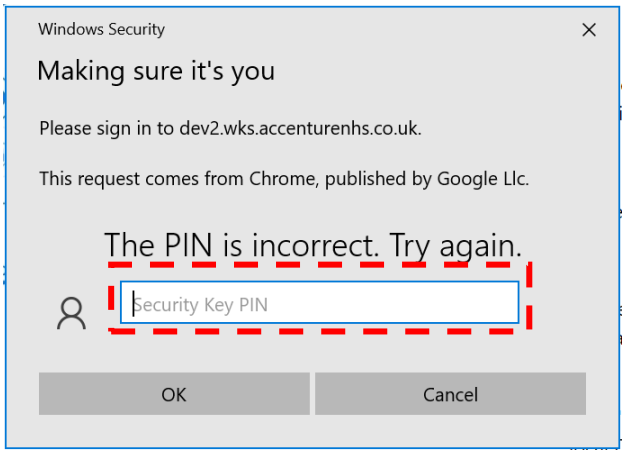
4. If the correct passphrase is entered, the user will be allowed one last attempt to enter the correct PIN with a warning informing them their security key will be locked if the PIN entered is incorrect.



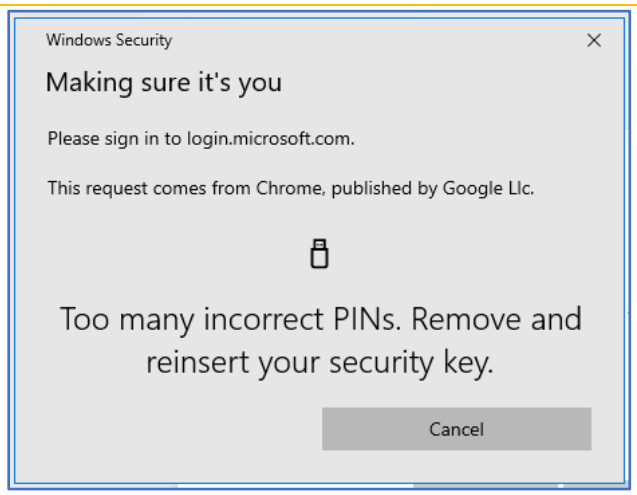
Important Note

Even if the user enters the correct PIN in the first attempt after closing and reloading the session, they will still be required to complete <u>both</u> entry attempts. This is to ensure it is not someone randomly trying to guess the PIN. See below for how this would look.

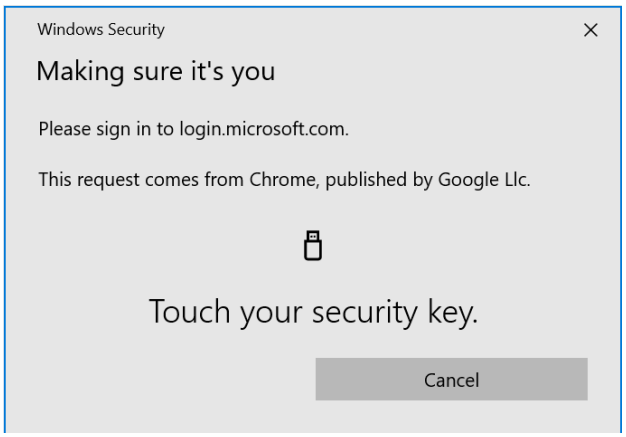
a) After the user enters the correct PIN on their first attempt, they will be prompted to **enter the correct PIN again** (even though the first attempt was correct)



b) The user enters the correct PIN a second time after which they will be instructed to remove and reinsert their security key



c) After the user removes and reinserts their security key, they need to touch their key to verify their presence before access is granted



Managing Blocked Security Keys

In the event that a FIDO2 security key becomes blocked after too many incorrect PIN entries, the following steps should be taken:

- Reset the security key to factory settings
- Remove the security token from relevant user account(s)
- Re-register the security token with a new PIN

Help & Support

Local Administrators can contact the NHSmail Helpdesk via helpdesk@nhs.net or 0333 200 1133 for further assistance.