



**Advanced Card Systems Ltd.**  
Card & Reader Technologies

# ACS PocketKey Series

## FIDO2 Windows Passwordless Logon

Application Note V1.03



## Table of Contents

- 1.0. Introduction ..... 3**
- 1.1. Overview ..... 3
- 1.2. Background ..... 3
- 2.0. Preparation ..... 4**
- 3.0. Join a Windows Device to Entra ID ..... 5**
- 4.0. Configure Setting on Entra Admin Center ..... 7**
- 4.1. Device Settings ..... 7
- 4.2. Passkey Settings ..... 7
- 5.0. Set up a security key ..... 8**
- 5.1. Register a security key ..... 8
- 6.0. Windows Logon ..... 10**

## List of Figures

No table of figures entries found.

## List of Tables

No table of figures entries found.



## **1.0. Introduction**

### **1.1. Overview**

ACS PocketKey Series provides users the experience of secure and swift passwordless online login. It allows individuals, enterprises, and government-scaled agencies to substitute passwords or increase account security with multi-factor authentication or two-factor authentication, reducing reliance on static passwords.

The devices are certified by the FIDO Alliance [FIDO®] and are compliant with FIDO2 and FIDO® U2F protocols. Its cryptographic security model terminates any likelihood of phishing, password/identity theft and repetitive attacks. User tracking can also be prevented by storing FIDO® cryptographic keys on-device and creating unique keys for each website.

### **1.2. Background**

The ACS PocketKey Series integrates FIDO functionality, enabling users to sign in to Microsoft Entra ID without the need for passwords.

This document provides a comprehensive guide on configuring the PocketKey Series (hereafter referred to as the "security key") as the default sign-in method for Windows logon. By following the steps outlined, users can enjoy a seamless authentication experience that combines robust security with intuitive, user-friendly features.



## 2.0. Preparation

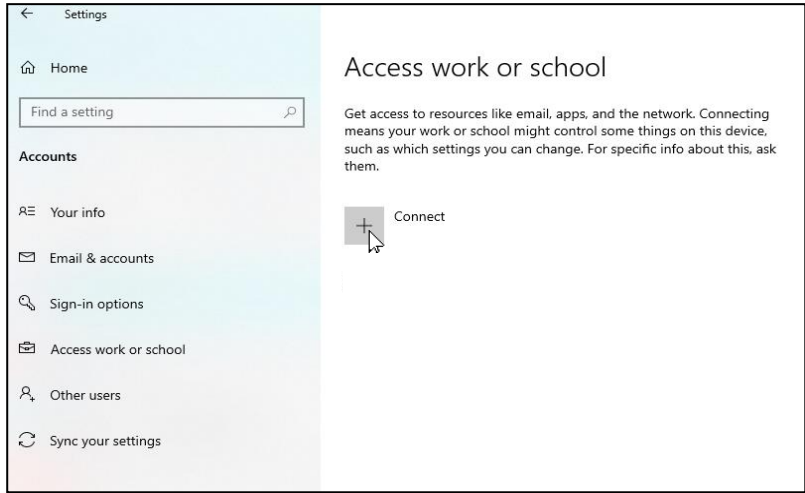
1. Microsoft Entra ID P1 license
  1. The pricing of Entra: [Microsoft Entra Plans and Pricing | Microsoft Security](#)
2. Windows 10 and Windows 11

For more information, refer to the link: [Plan your Microsoft Entra join deployment – Microsoft Entra ID | Microsoft Learn](#).

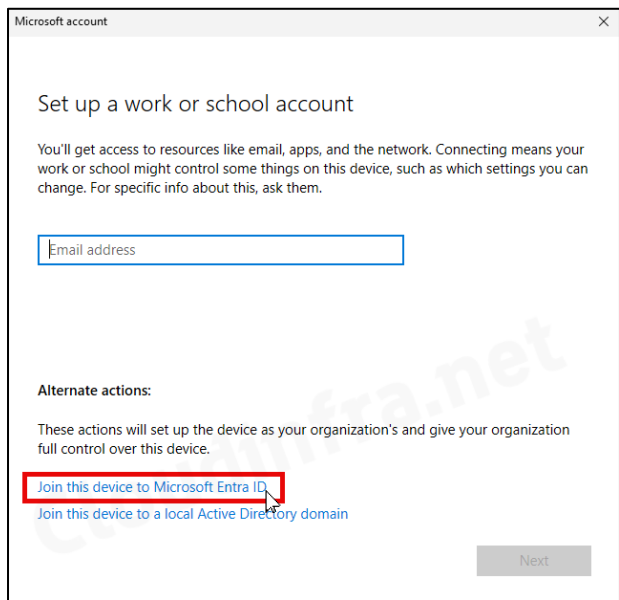
### 3.0. Join a Windows Device to Entra ID

To join a Windows Devices:

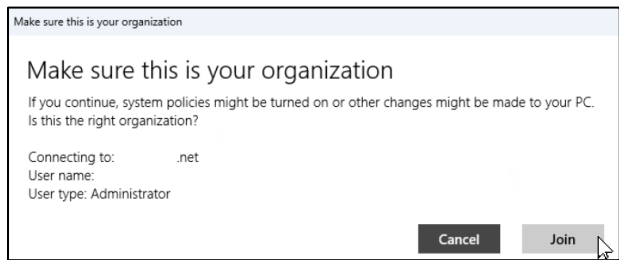
1. Go to **Settings**, select **Accounts**, then enter to **Access work or school**
2. Click **Connect** to enroll the device to Microsoft Entra ID



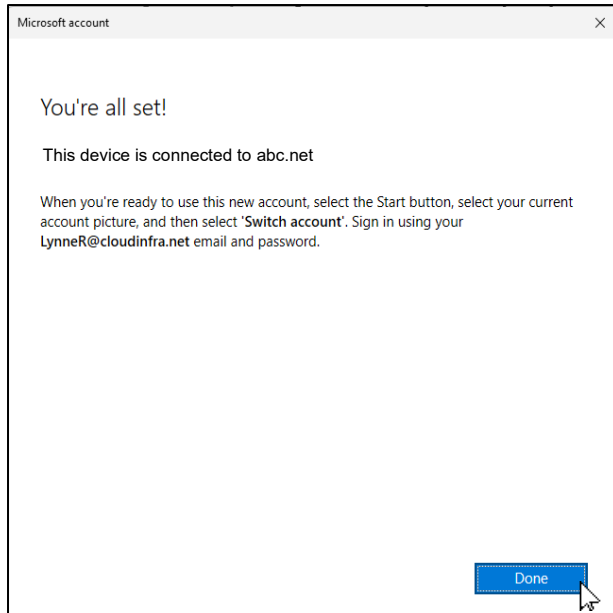
3. Select **Join this device to Microsoft Entra ID**, then sign in to your Microsoft Entra ID account (or AzureAD account, if you prefer)



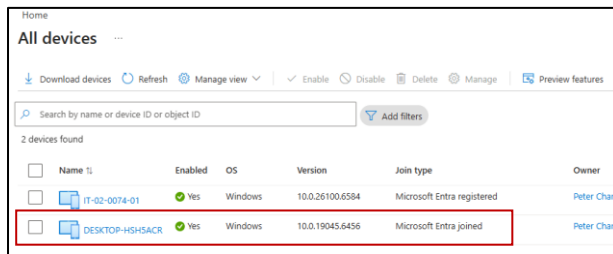
4. Click "Join" button to confirm the action to finish the set up



5. Once completed then click **Done**



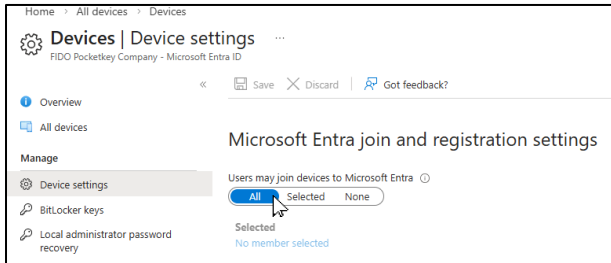
6. Go back to **Access work or school** to confirm the connection.
7. You may go to **Entra Admin Center**, expand **Entra ID**, select **Devices**, then open **See all devices** to search for the device you just joined to Entra ID to confirm if the Join type is showing as **Microsoft Entra joined**



## 4.0. Configure Setting on Entra Admin Center

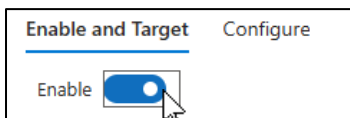
### 4.1. Device Settings

1. Login to the **Microsoft Entra Admin Center**
2. Expand **Entra ID**, select **Devices**, then open **Device settings**
3. Configure the Users may join devices to Microsoft Entra setting and set it to **All**  
*Alternatively, you can select **Selected** and specify individual users or an Entra group that is allowed to join devices to Microsoft Entra.*

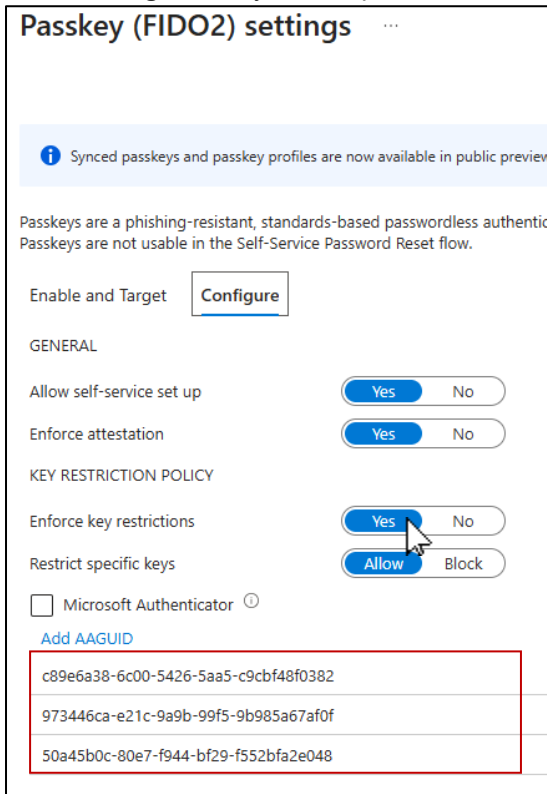


### 4.2. Passkey Settings

1. Login to the **Microsoft Entra Admin Center**
2. Expand **Entra ID**, select **Authentication methods**, open **Policies**, then select **Paskey**
3. Toggle on the Passkey Authentication Method



4. Go to **Configure**, if try to set up the **KEY RESTRICTION POLICY**



For more information about AAGUID of ACS PocketKey Series, refer to the link: [AAGUIDs](#)

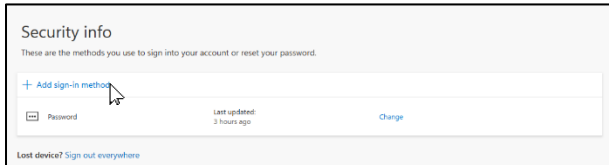
## 5.0. Set up a security key

Please ensure that the configuration in the Entra Admin Center is complete before proceeding with the following steps.

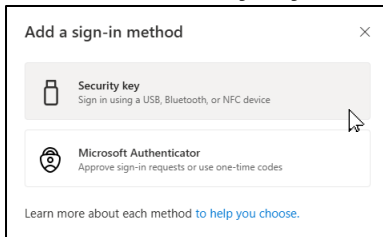
### 5.1. Register a security key

To use the PocketKey series device for sign-in, please ensure it is set up with a PIN. Note that you can register up to 10 keys with your account.

1. Go to the My Profile page at [My Account](#)  
*Please note you may need to sign-in with password in first time*
2. Select **Security Info**, select **Add sign-in method**

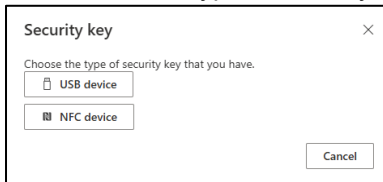


3. Then select **Security key\***.



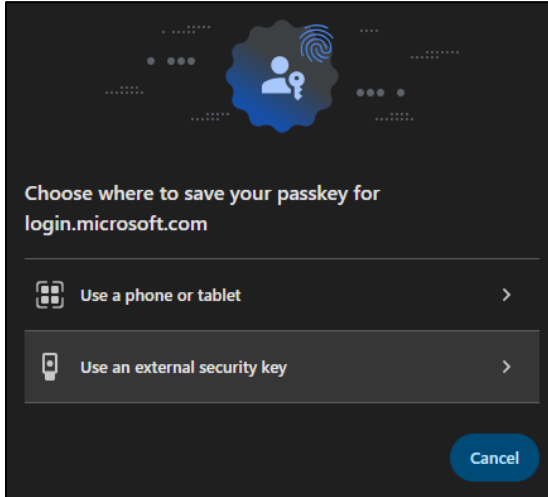
*\*Please note: Microsoft may ask you to set up “Microsoft Authenticator” as sign-in method in first time.*

4. Then select the type of security key you have, either **USB device** or **NFC device**.

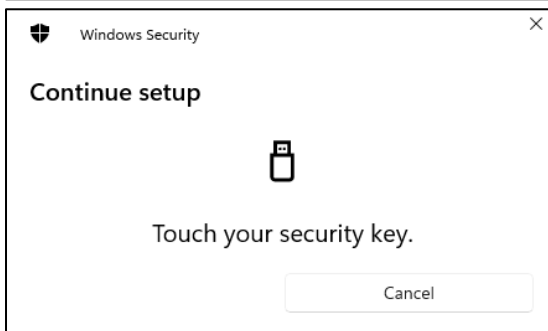
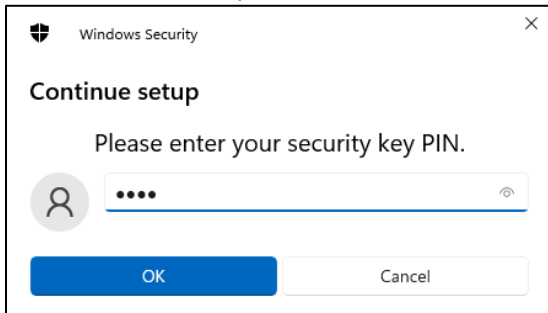


- a. **USB device:** Insert your security key into the USB port of your device.
  - PocketKey
  - PocketKey+ II
  - PocketKey+ Bio
- b. **NFC device:** Tap the security key against your NFC reader.
  - PocketKey NFC Card
  - PocketKey+ II
  - PocketKey+ Bio

5. Then choose **Use an external security key**



6. Enter the **PIN**, then press the built-in button or fingerprint sensor or tap for authenticate.

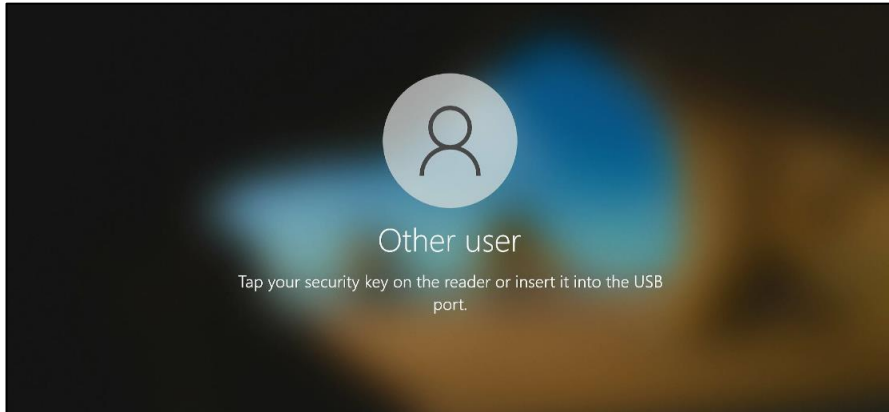


7. The registration is done.

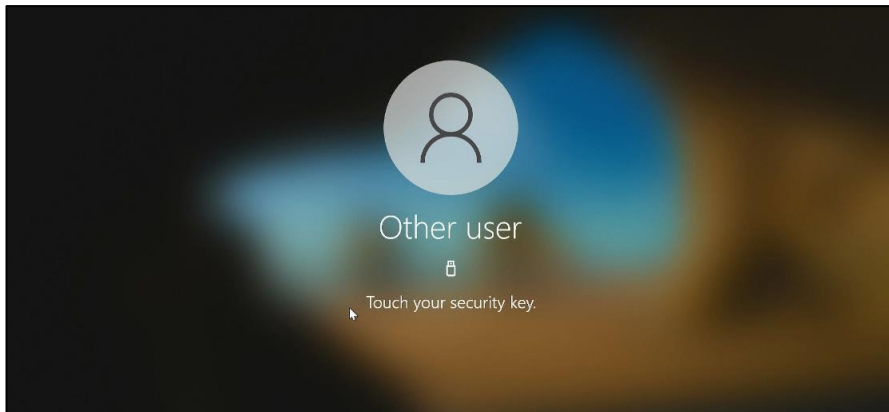
## 6.0. Windows Logon

To login Windows work account:

1. On the Windows sign-in screen, select **Other User**,
  - a. Insert the **PocketKey/ NFC card/ PocketKey+ II** into the USB port or tap it via NFC.



- b. If the **PocketKey+ Bio** is used, touch the sensor when prompted\*.



*\*Windows will typically require the user to enter an alternative sign-in method (e.g., PocketKey PIN) after three consecutive failed attempts.*

2. Enter the **PIN**, the login will complete successfully.