Implementing VeroCard – High Security Module – with FIDO2

Guide

VeroGuard Systems

VeroGuard Systems – Melbourne, Australia – Phone: +61 3 9558 3090

Email: - info@veroguard.com.au

Table of Contents

Table of Figures

1 Introduction

1.1 Purpose

This document was written to provide an overview of the setup requirements for integrating a Windows 10 environment authenticating via Azure AD with VeroID and VeroCard running FIDO2.

1.2 Scope and intended reading audience

This version is intended for technical / IT personnel and includes both the back-end setup changes as well as the end user/end user device tasks. Relevant sections of Microsoft technical articles and references are also added to the end of the document for context and further reading.

1.3 Preconditions

All end users must be in possession of a VeroCard and have been onboarded with a VeroID.

1.4 Definitions

Word/Acronym	Meaning
AAD	Azure Active Directory
AD	Active Directory
BT	Bluetooth
FIDO	Fast Identity Online
PRT	Primary refresh token
WebAuthn	Web authentication

2 VeroGuard integration instructions

2.1 Azure AD (AAD) setup

1. Sign into the Azure portal as an administrator.
2. Browse to **Azure Active Directory** > **Security** > **Authentication methods** > **FIDO2 Security Key (Preview)**) (see **Figure 1.**
3. Under the method **FIDO2 Security Key**, choose the following options:
    a. **Enable** - Yes or No
    b. **Target** - All users or Select users
    c. **Enforce attestation** – set to No
4. **Save** the configuration.

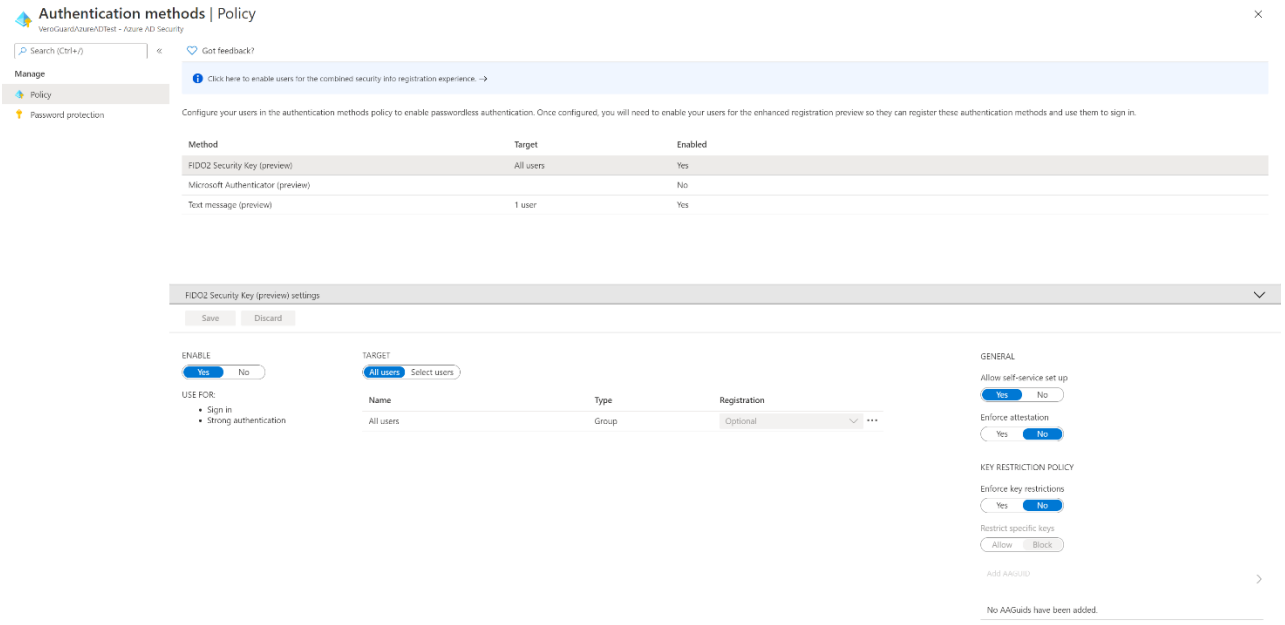

Figure 1. *AAD setup screen*

2.2 Prepare end user devices

2.2.1 Setting up user devices

End user devices require the latest Microsoft operating system and VeroGuard's Serenity Companion Service. If the device you are preparing does not have Bluetooth, please install the USB BT adaptor provided with the VeroCard when completing end user set-up.

1. **Update all devices to 20H2 (minimum)**

Hybrid Azure AD joined devices must run Windows 10 version 2004 or newer.

2. **Serenity Companion Service**

Run the Serenity Companion installer package which will set the service to run in the background, enabling the VeroCard to securely communicate with VeroGuard via the PC's Bluetooth connection. You can find the installer at https://www.support.veroguard.com.au/downloads.

If Windows defender or your AntiVirus software show an alert, please select the option to "install anyway"

The Serenity Companion installer will enable security keys for Windows sign-in as described in the Microsoft technical articles by adding the following key to the registry during installation: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Policies\PassportForWork\SecurityKey - UseSecurityKeyForSignin – REG_DWORD = 0x00000001

2.3 Connecting and Activating VeroCard

The following sections can all be completed by end users – however some parts e.g., setting a PIN **MUST** be completed by the end user only. Users can access the VeroCard user guide at https://www.support.veroguard.com.au/user-manual.

VeroCards require pairing with any PC before they can be used for authentication to user accounts. Pairing a VeroCard uses the same procedure as pairing any other Bluetooth device and requires confirmation of the passcode for added security.

Activation is the process used by VeroGuard to link the device to the VeroGuard Platform, confirm its status remains secure and then enables the end user to set their secret PIN.

When you initially turn on your VeroCard it will display the message "Ready for Activation" below the VeroCard number.

Please note that the keypad on the VeroCard is deactivated when on the charger. Please ensure your VeroCard is removed from the charger when completing any necessary activities. The VeroCard can be returned to the charger in between if necessary

2.3.1 Pairing a VeroCard with the PC

1. Go to Windows **Settings** > **Bluetooth**.
2. Turn on your VeroCard.
3. Click "Add Device" and the first option "Bluetooth" to initiate a search for available Bluetooth devices.
4. In the results view look for a 16-digit number in the list e.g., 1002000000009643 and click on the device name with your mouse (see **Figure 2**).
5. The screen on both devices will now display a "compare passcodes and confirm" message. Click "Connect" on the PC and touch the green "tick" on the VeroCard.

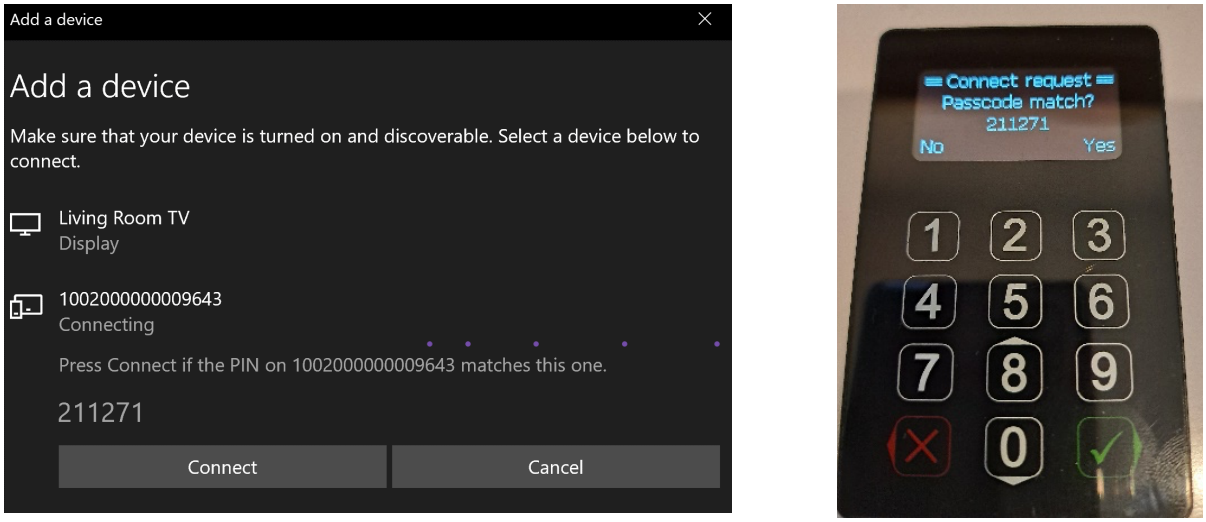

Figure 2. *Add a device screen and VeroCard compare passwords confirmation screen*

If the end user device does not have Bluetooth, please install the USB BT adaptor provided with the VeroCard.

2.3.2 Activating a VeroCard

Until it is activated your VeroCard will display the message “Ready for Activation” below the VeroCard number. Once Serenity Companion is installed and your VeroCard paired, the PC will connect to the paired device whenever they are in range and switched on. This is indicated on the VeroCard by the Bluetooth icon (indicates Bluetooth connection is present) and the “V” icon showing connection to VeroGuard (see

Figure 3).

1. Confirm the VeroCard is connected correctly by viewing the BT and V icons.
2. Navigate to the “Activate” command by pressing 0-6-3 (for more information on using your VeroCard and navigation see article and https://www.support.veroguard.com.au/user-manual).
3. The VeroCard will display “Activating”. Follow the prompts on the VeroCard to complete the process and create and confirm your PIN.
4. Once successfully activated the VeroCard will display “Ready to Vero”.

To activate a VeroCard you must be connected to VeroGuard. If you do not see the “V” icon, check your internet connection.

See more information on setting a secure PIN in our article "A Better PIN"

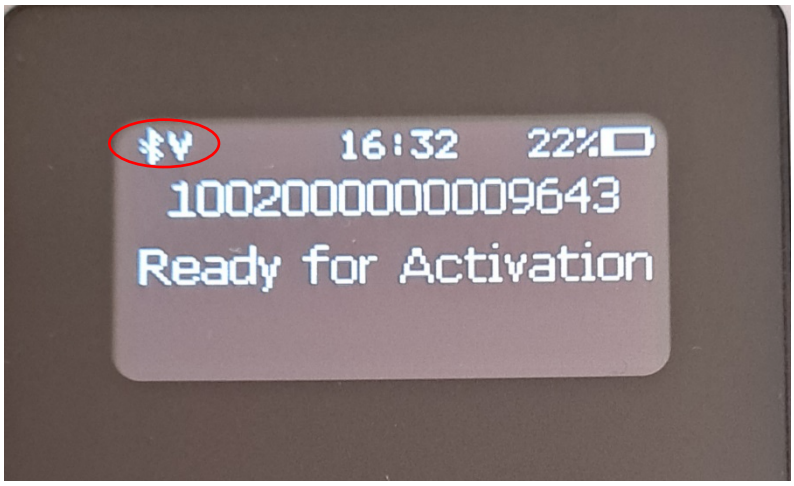

Figure 3. *VeroCard "Ready for Activation" screen*

2.3.3 Register your VeroCard to your "Sign in" Account

This final setting requires the end user to login to their Microsoft account online and add the VeroCard as a security device to their profile.

1. End users need to browse to https://mysignins.microsoft.com and sign-in (if not already) with their Windows username and password.
2. Click **Security Info** (see **Figure 4**).

If the user already has at least one Azure AD Multi-Factor Authentication method registered, they can immediately register a FIDO2 security key. If they do not have at least one Azure AD Multi-Factor Authentication method registered, they must add one.

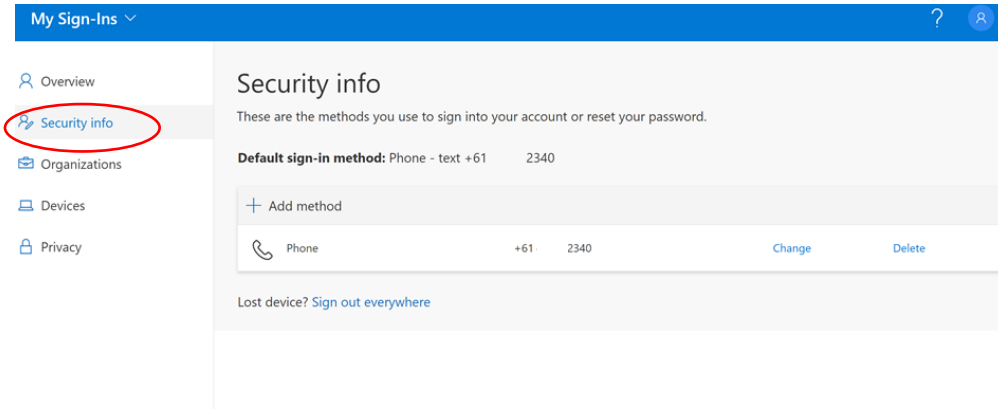

Figure 4. *Security info link*

3. Add a FIDO2 Security key by clicking **Add a method** and choosing **Security Key** (see **Figure 5**).

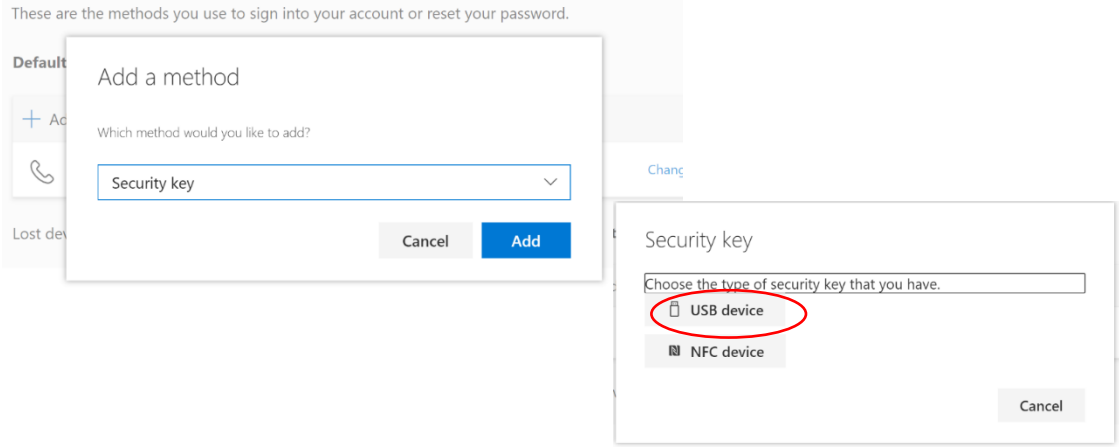

Figure 5. *Add a FIDO2 Security*

4. Choose **USB device** [NOTE – This will try both USB and Bluetooth BLE that supports VeroCard].
5. Make sure your VeroCard is turned on and ready and choose **Next.** The browser will connect with and register the device against your account.
6. The user will be returned to the combined registration experience and asked to provide a meaningful name for the key so the user can identify each if they have multiple. Click **Next** (see **Figure 6**).
7. Click **Done** to complete the process.

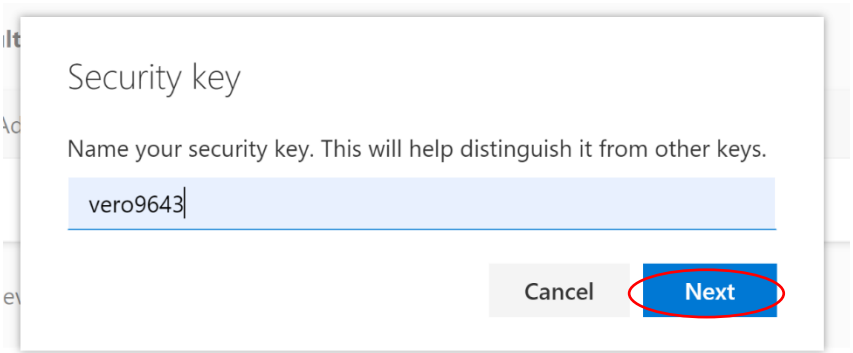

Figure 6. *Security key screen*

2.4 Login to your Device

1. Power up, log out of your device or return to the lock screen (WIN+L).
2. On the screen select “Sign-in Options” or if already displayed click the “FIDO security key” icon, and the message will change to request you to “Turn on your Bluetooth security key or insert it into the USB port” (see **Figure 7**).

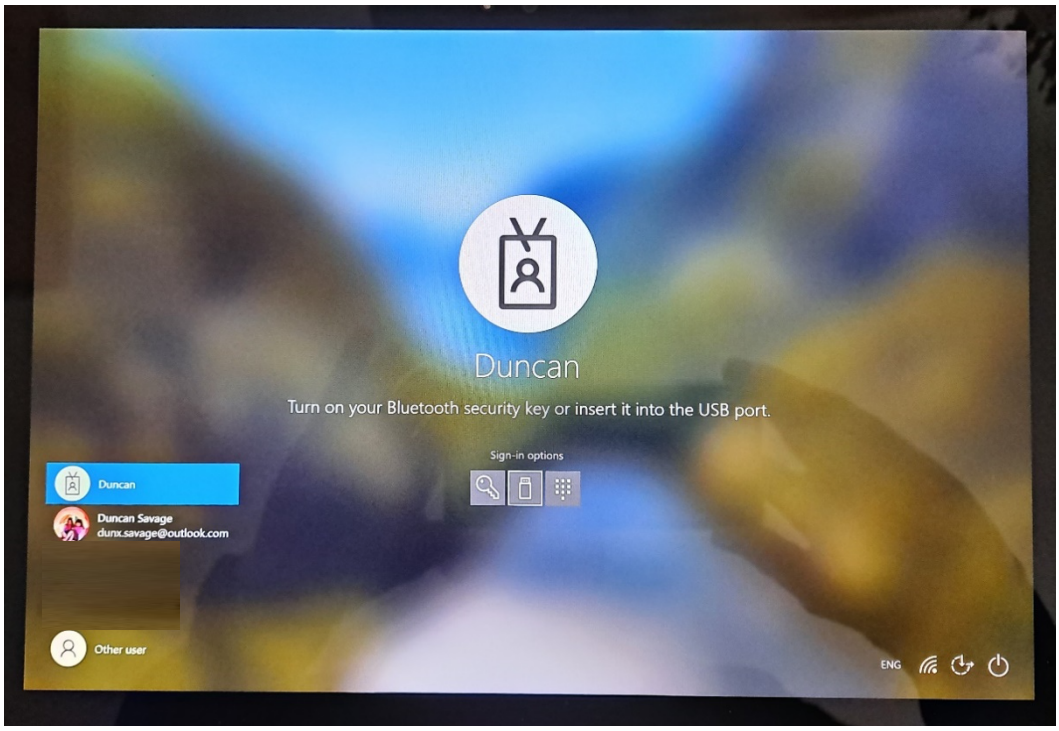

Figure 7. *Turn on your Bluetooth security key or insert in into the USB port screen*

3. Turn on your VeroCard and once connected it will display available accounts.
4. Select your account (see **Figure 8**).
    a. If multiple accounts exist, select account using up/down (8/0).
    b. Click the green tick to select.
    c. Enter your PIN on the VeroCard when prompted.

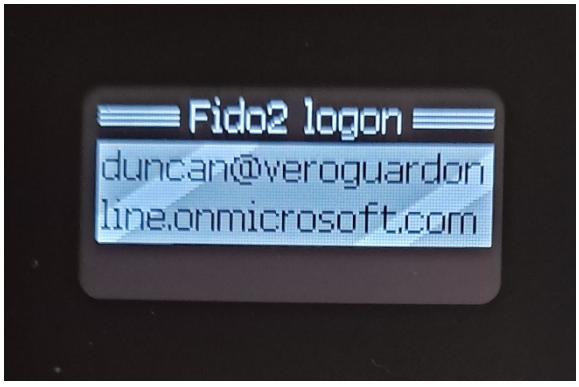

Figure 8. *Selecting account to login in with*

Once a user has completed an online login, the same login process can be used when offline