Kensington

VeriMark[™] Guard Setup Guide

Kensington takes pride in making our comprehensive installation guides easy to follow with simple illustrations and step-by-step instructions. This guide will walk you through setup and help you get to know your VeriMark[™] Guard.



Enabling Support for Fido2 Security Keys	2
Documentation & References	4
Fido2 Security Key Provisioning and Key Management	5
Documentation & References	.0
Configuring Windows 10 Sign-In Using Fido2 Security Keys	
(Modern Management / Microsoft Entra joined)	.1
Enable Manually on an Individual Device	.2
Enable Using Intune Device Configuration Profile	.3
Enable Using Intune Windows 10 Enrollment Policy	.6
Documentation & References	.7
Configuring Windows 10 Sign-In Using Fido2 Security Keys	
(On-Premises Ad / Microsoft Entra hybrid joined)	.8
Documentation & References	.8



Enabling Support for Fido2 Security Keys

At the time of writing, organizations must enable specific features within their Microsoft Entra ID tenant to support the self-service registration of FIDO2 security keys for their enterprise Microsoft 365 accounts. This is not required for personal/consumer Microsoft accounts, which are not subordinated by an organization's Microsoft Entra ID implementation.

- **1.** Sign in to the <u>Microsoft Entra ID portal</u>.
- 2. Browse to <u>Microsoft Entra ID</u> with an account that has sufficient permissions to modify security features (Global Administrator or Security Administrator roles).

Microsoft Anure P. Sta	th museum, servers, and down (Graf)	■ 17 0 0 7 0 Helding
+ Kensingto	n Lab Overview	
	Construction Const	amain 🕂 Create a tenant 📑 What's new 🛛 🔛 Preview features 🧰
Administrative units Toterprise applicatio Devices App regularations App regularations Appleation proxy Loanset Aure AD Connect Castom domain nam Mobility (MOM and	P Search your tenant To Frenant Information Wour rule Global administrator Move into License Adver AD Premium F2 Tenant ID doccosol-docol-docol-doc Premary domain Assuingtoriab premional/License MAM	Azure AD Connect
Password reset Company branding Our settings If Angenties Security	Septima iii iii iii iii iii iii iii	

3. Navigate to Security > Authentication methods.



4. In the Policy pane, select "Click here to enable users for the combined security info registration experience."



5. In the User feature previews pane, enable the "Users can use the combined security information registration experience" setting for either selected groups or all users, then save the configuration.



- 6. In the Policy pane, select FIDO2 Security Key (preview) settings, and configure the following:
 - a. Enable Yes
 - **b.** Target All users or selected users/groups
 - c. General
 - i. Allow self-service set up Yes
 - ii. Enforce attestation Yes

Microsoft Azure	ranch resolutions.	several data tite?		E 6 0 1	0 7 0	septes.
+ Authenti	cation m	ethods Polis	cy			x
D Grant Kitter		Get herback?				
Manage		C can be be a	the same for the same line	and secondly independently	and the second se	
* Billy		0				
Password protects		Cardgare peur anns a your criers for the solu	i the authentication re- socied registration pre-	ethods policy to anable intern to they can register	annetes attendes bes attendes neto	Over configured, pilo all loted to evable chand use them to sign in:
		Method		Terget.	Enabled	
		HDOJ Security Rep ((mexima)	Alues	les.	
		Monort Autoritics	for these of		Ne	
		Text massage (partic	-		No	
		ADD Cleventy Key (previne) settings			
		See 1	nort			
		point	TANGET			CONDIAL
			Aler Select a	1001		Allow set serves set up
		- Ma	Natio	Tor	Registration	100
		· Sejá lá	All units	Gener	Convent	Enforce effectuation
		 Strong authentications 	4			165
						429 RESTRICTION POLICY
						Enloyed key manufation
						700 000

7. Save the configuration.

- Enable passwordless security key sign-in (preview)
 - <u>https://learn.microsoft.com/en-us/entra/identity/authentication/</u> howto-authentication-passwordless-security-key

Fido2 Security Key Provisioning and Key Management

In this section, an eligible Microsoft 365 user within the organizational Microsoft Entra tenant can register their Kensington VeriMark Guard FIDO2 security key. At present, administrators cannot provision or de-provision security keys on a user's behalf. Eligible users will need to perform a self-service registration.

- **1.** Browse to https://myprofile.microsoft.com.
- 2. Select Security Info. If the user does not currently have any Microsoft Entra Multi-Factor Authentication (MFA) methods registered, they must add a method prior to registering the FIDO2 security key.
- 3. Select Add method and choose Security key.

My Sign-Ins 👻		?	8
R Overview Re Security Mo	Security info These are the methods you use to sign into your account or reset your password. Default sign-in method: Microsoft Authenticator - notification Change		
Devices	+ Add a method Which method would you like to add? Security key	Clerge	Datete Datate
	Lost a Cancel Add		

4. If prompted, click **Next** to sign in with two-factor authentication. In the second screenshot below, the user's default sign-in method is a Microsoft Authenticator notification.



5. Select USB device.



6. Verify that the Kensington VeriMark Guard FIDO2 security key is connected to the device, and click Next.



7. In the Windows Security / Security key setup dialog box, click OK.



8. In the Windows Security / Continue setup dialog box, click OK.

		1
Continue setup		
This will let login.micro- security key	soft.com see the make a	and model of your
login.microsoft.com wa	nts to create a credenti	al on your security
And the second sec	and the second design of the second	
key. This lets you sign it	n without having to type	e your username.
key. This lets you sign in Note: A record of your	n without having to typ visit to this site will be k	e your username. ept on your
key. This lets you sign i Note: A record of your security key.	n without having to typ- visit to this site will be k	e your username. apt on your
key. This lets you sign i Note: A record of your security key.	n without having to typ-	e your username. ept on your
key. This lets you sign in Note: A record of your security key. OK	n without having to typ-	e your username. lept on your Cancel
key. This lets you sign in Note: A record of your security key. OK	n without having to typ- visit to this site will be k	e your username. ept on your Cancel

9. If prompted, create a PIN for the Kensington VeriMark Guard FIDO2 security key. This is only necessary during the initial setup of the security key.

Windows?	Security	new sinn-in	3
Contir	ue setup		
Yo	u'll need to cre securi	eate a PIN for th ty key.	is
Q	New Security Key PIN		
0			

10. When prompted, touch the security key.



11. When prompted, enter a name for the security key.

seconty key		
Name your security key. This v	will help distinguish it from	n other keys
Kensington Guard		

12. Verify that the Kensington VeriMark Guard security key is now a registered MFA method.

My Sign-Ins 🗠				1	?	8
R Overview	Security info					
Py Security info	These are the methods you use to sign	into your account or reset your passwo	rd.			
Crganizations	Default sign-in method: Microsoft Au	/henticator - notification Change				
E Devices	+ Add method					
A Privacy	C Phone	+1 1234567890	Change	Delete		
	Microsoft Authenticator	Phone		Delete		
	Security key	Kensington Guard		Delana		Ŷ
	Lost device? Sign out everywhere					

13. Test the security key by signing out (or opening a separate browser session) and navigating to <u>https://myprofile.microsoft.com</u> again. At the logon screen, select **Sign in with a security key**.

Sign in	
Email or phone	
Can't access your account?	
Sign in with a security key 🕥	
	Must

14. When prompted, provide the security key PIN.

ished by Google LLC.
urity key PIN.
curity key PIN.
curity key PIN.

15. When prompted, touch the security key.



16. If prompted, click **Yes** to stay signed in.



At this point, the Kensington VeriMark Guard FIDO2 security key is successfully associated with the registered user and is not specific to the device that was used during the initial registration. The security key is fully portable and can be connected to other devices to log on as the same registered user account.

- Enable passwordless security key sign-in (preview)
 - <u>https://learn.microsoft.com/en-us/entra/identity/authentication/</u> howto-authentication-passwordless-security-key
- Set up a security key as your verification method
 - <u>https://support.microsoft.com/en-us/account-billing/</u> set-up-a-security-key-as-your-verification-method-2911cacd-efa5-4593-ae22-e09ae14c6698

Configuring Windows 10 Sign-In Using Fido2 Security Keys (Modern Management / Microsoft Entra joined)

Microsoft Entra joined Windows 10 devices support the ability to use FIDO2 security keys at the logon screen for a fully passwordless experience. This scenario is supported if the following requirements are met:

- Microsoft Entra ID Multi-Factor Authentication (e.g., licensed and enabled in tenant)
- Combined security information registration preview
- Compatible FIDO2 security keys (e.g., Kensington VeriMark Guard)
- Microsoft Entra joined devices require Windows 10 version 1909 or higher



Microsoft offers a variety of broader deployment methods in their documentation; however, we will provide the following examples:

- **1.** Enable manually on an individual device
- 2. Enable using Intune device configuration profile (targeted devices)
- 3. Enable using Intune Windows 10 enrollment policy (all eligible users/devices)

Enable Manually on an Individual Device

To manually enable on an individual device for testing, choose a Windows 10 device running 20H1 or greater and launch the Local Group Policy Editor. Navigate to Computer Configuration > Administrative Templates > System > Logon, and configure the Turn on security key sign-in setting as Enabled.



If it is necessary to manually test on an older build of Windows 10 without the latest ADMX templates, the **Registry Editor** can be used as a workaround.

Registry Editor				-		×
Eile Edit View Favorites Help						
Computer/HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Policies/Pa	sspo	rtForWork/SecurityKey				
Policies COMMS DM PassportForWork Biometrics Code510-549d-4ed4-8953-a697d9866c07 SecureAted		Name (#)(Default) U(DeSecultyKeyForSignin	Type REG_SZ REG_DWORD	Dat (val Ox0	ta lue not si ioccocci	et) (1)
Balla Adaptat	-W.	4	(

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Policies\PassportForWork\SecurityKey] "UseSecurityKeyForSignin"=dword:0000001

Enable Using Intune Device Configuration Profile

To target specific device groups to enable the credential provider, use the following custom settings via Intune:

1. Browse to Microsoft Endpoint Manager admin center > Devices > Configuration profiles > Create profile.



- 2. Configure the new profile with the following settings:
- Name: Security Keys for Windows Sign-In
- Description: Enables FIDO Security Keys to be used during Windows Sign In
- Platform: Windows 10 and later
- Profile type: Custom
- Custom OMA-URI Settings:
 - Name: Turn on FIDO Security Keys for Windows Sign-In
 - OMA-URI: ./Device/Vendor/MSFT/PassportForWork/SecurityKey/UseSecurityKeyForSignin
 - Data Type: Integer
 - Value: 1

Create a profile	×
Platform	
Windows 10 and later	Ŷ
Profile	
Custom	~
Custom	
Create	

Name *	Security Keys for Windows Sign-In	2
Description	Enables FIDO Security Keys to be used during Windows Sign	in 🗸
	Woolcourt Warrel Inter	
Nation	Cistore	
Nation Notice type	Custom	
Provious Next	Cistors	
Provious Next	Cirstons Cirstons Add Row Cottotit Sering	
Provious Next Provious I Use > Desires I use to and lase	Customs Customs Customs Customs Customs	D. Security Kays for Windows Tag
Provious Next Provious Next Provious Configuration united No. 10 and late Mark 10 and late Mark 10 and late	Custore Custore Add Row Coloutific Serrege Name* Televent 10 National Serrege Name* Televent 10 Desciption National Serrege	D Selanty Keys for Windows Say
Providus Next Providus Next Providus Configuration unities Providus Configuration unities Providuo Providuo Configuration unities Providuo Providuo Configuration unities Providuo Prov	Custors Custors Custors Add Row December Same* Ten on Re Same* Ten on Re	O Security Kays for Windows Sig- red GrowtSPT Perspection Work Sec

3. Assign the new device configuration policy to the appropriate users or devices.

Custom Kindows 10 and later		
✓ Basics ✓ Configuration settings	Assignments Applicabil	ty Rules (1) Review + creat
included groups		
Assign to	Selected groups	Ŷ
Selected groups		
No groups selected		
Select groups to include		
Excluded groups		
When excluding groups, you cannot mi	user and device groups across include and ex	dude. Click here to learn more.
Selected groups		
No groups selected		
+ Select groups to exclude		

4. Customize any required applicability rules and create the policy.

Enable Using Intune Windows 10 Enrollment Policy

If a targeted deployment is not necessary, the following method enables security keys for sign-in for all users on eligible Windows 10 devices.

- 1. Browse to Microsoft Intune > Device enrollment > Windows enrollment > Windows Hello for Business.
- 2. Under Settings, set Use security keys for sign-in to Enabled.

Microsoft Endpoint Manager	admin center		a (٥	lubdiab.o. 🧶
 France Deutoisand All services Uncontrol Devices Ange Devices Ange Endpoint security Reports Usen Groups Tenant administration Tenablebiccolog + support 	Hume I Devices Overview Search (Cri+c) * Conview Monitar By plantures Monitar By plantures Windows Windows Windows Windows Windows Monitar By conview Convice enrollment Paricy Compliance pathons Conditional access Conditional access Conditional access	Envollment status Inture envolled Lar unutto you Plaffarm Windows Android Cot/Paulos macOS Windows Mobile Tetal Coroliment failure III III III III III III III III III	Erestiment alerts devices to seam res Devices 10 10 10 10 10 10 10 10 10 10 10	Compile 3	ance vi	abat.	×



- Enable passwordless security key sign-in to Windows 10 devices with Microsoft Entra ID (preview)
 - <u>https://learn.microsoft.com/en-us/entra/identity/authentication/</u> howto-authentication-passwordless-security-key-windows

Configuring Windows 10 Sign-In Using Fido2 Security Keys (On-Premises Ad / Microsoft Entra hybrid joined)

Microsoft Entra hybrid joined Windows 10 devices support the ability to use FIDO2 security keys at the logon screen for a passwordless experience to both on-premises and Microsoft Entra ID—integrated resources. This scenario is supported if the following requirements are met:

- Microsoft Entra ID Multi-Factor Authentication (e.g., licensed and enabled in tenant)
- Combined security information registration preview
- Compatible FIDO2 security keys (e.g., Kensington VeriMark Guard)
- Microsoft Entra hybrid joined devices require Windows 10 version 2004 or higher
- Fully patched Windows Server 2016/2019 domain controllers
- Microsoft Entra ID Connect version 1.4.32.0 or later

For more information on how to prepare a hybrid environment for supporting FIDO2 security keys at the Windows 10 logon screen, please refer directly to the following Microsoft documentation.

- Enable passwordless security key sign-in to Windows 10 devices with Microsoft Entra ID (preview)
 - <u>https://learn.microsoft.com/en-us/entra/identity/authentication/</u> howto-authentication-passwordless-security-key-windows
- Enable passwordless security key sign-in to on-premises resources with Microsoft Entra ID (preview)
 - https://learn.microsoft.com/en-us/entra/identity/authentication/ howto-authentication-passwordless-security-key-on-premises
- Deployment frequently asked questions (FAQs) for hybrid FIDO2 security keys in Microsoft Entra ID (preview)
 - <u>https://learn.microsoft.com/en-us/entra/identity/authentication/</u> howto-authentication-passwordless-fags
- Troubleshooting for hybrid deployments of FIDO2 security keys in Microsoft Entra ID (preview)
 - <u>https://learn.microsoft.com/en-us/entra/identity/authentication/</u> howto-authentication-passwordless-troubleshoot