Kensington®

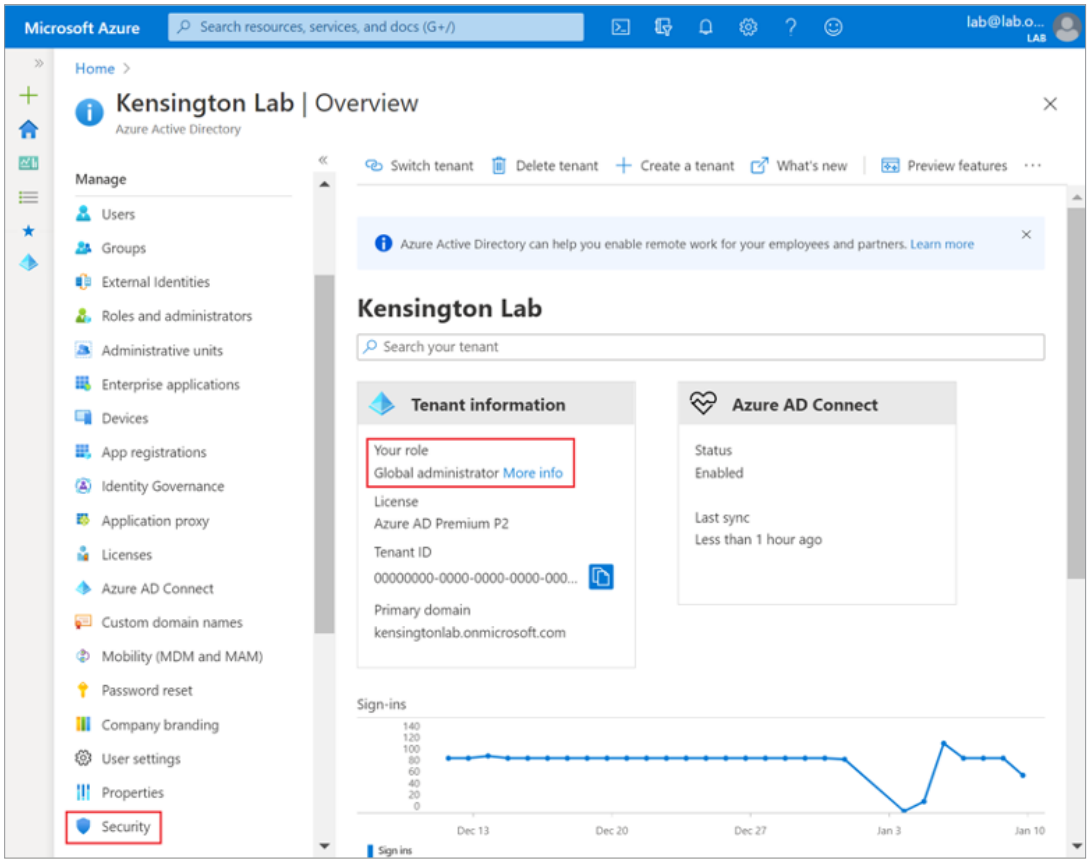
VeriMark™ Guard Setup Guide

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.

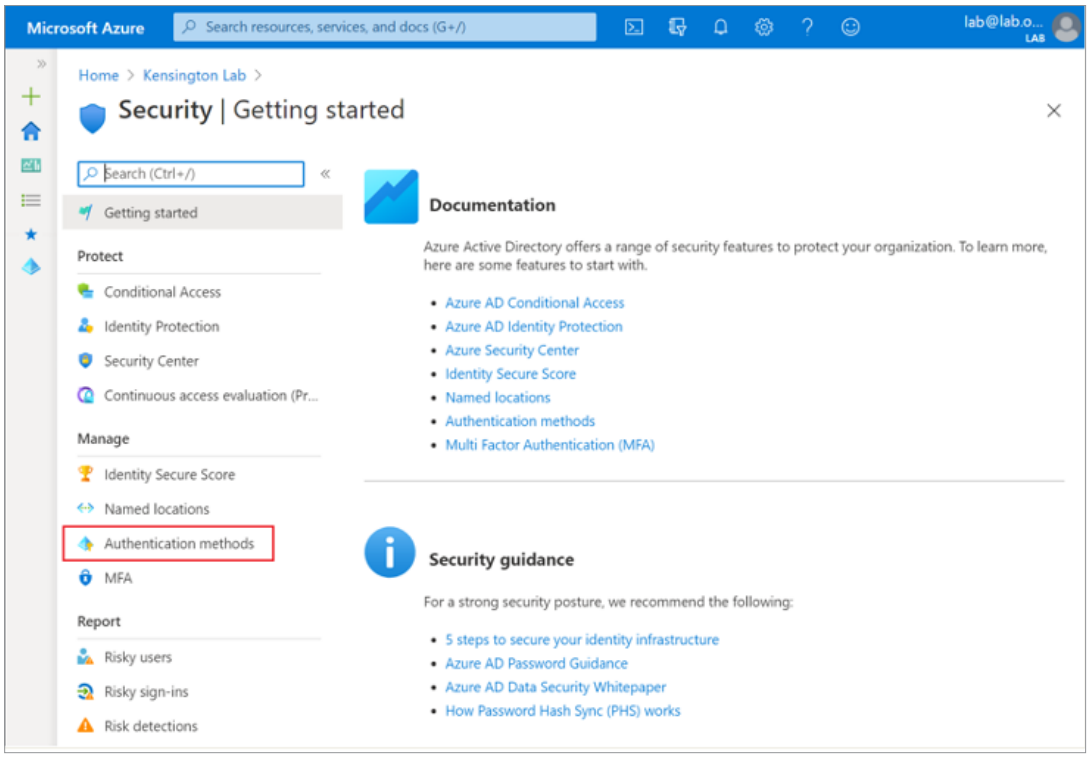
Enabling Support for Fido2 Security Keys

At the time of writing, organizations must enable specific features within their Azure Active Directory (Azure AD) 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 Azure AD implementation.

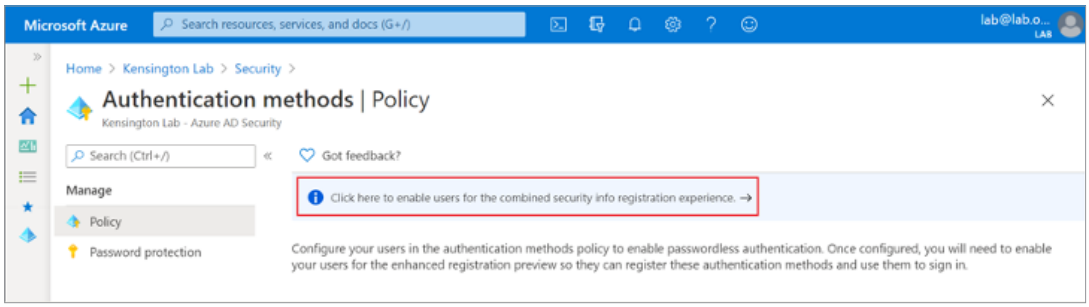
1. Sign in to the Azure portal.
2. Browse to Azure Active Directory with an account that has sufficient permissions to modify security features (**Global Administrator** or **Security Administrator** roles).



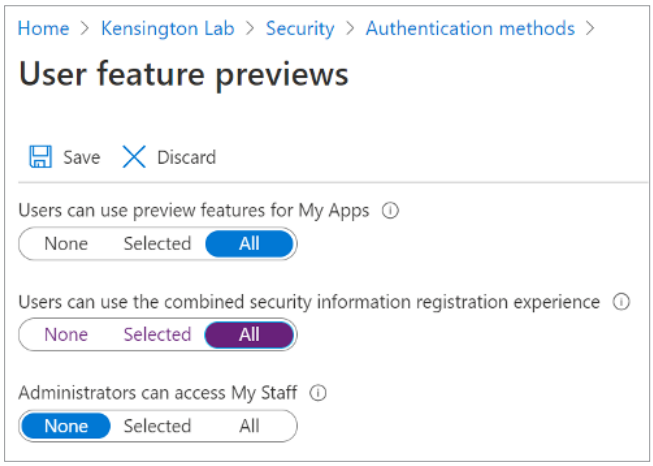
3. Navigate to **Security > Authentication methods**.



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



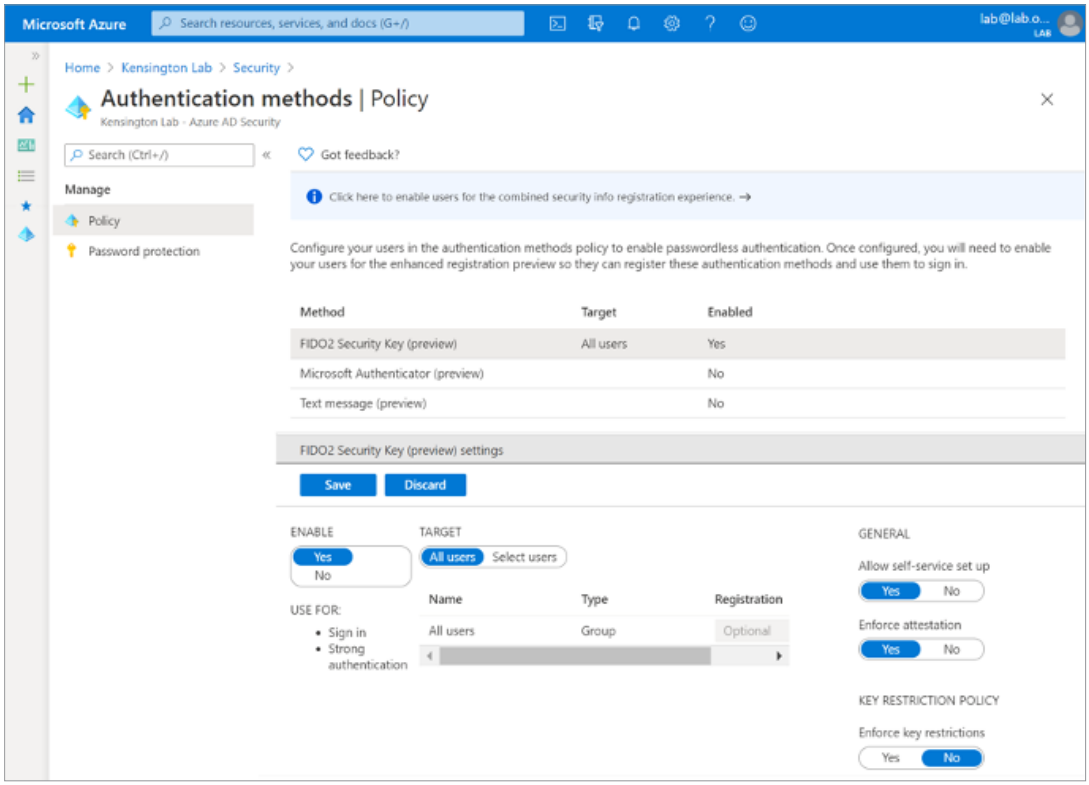
5. In the **User feature previews** pane, enable the "**Users can use the combined security information registration experience**" setting for either selected groups or all users, then save the configuration.



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



7. Save the configuration.

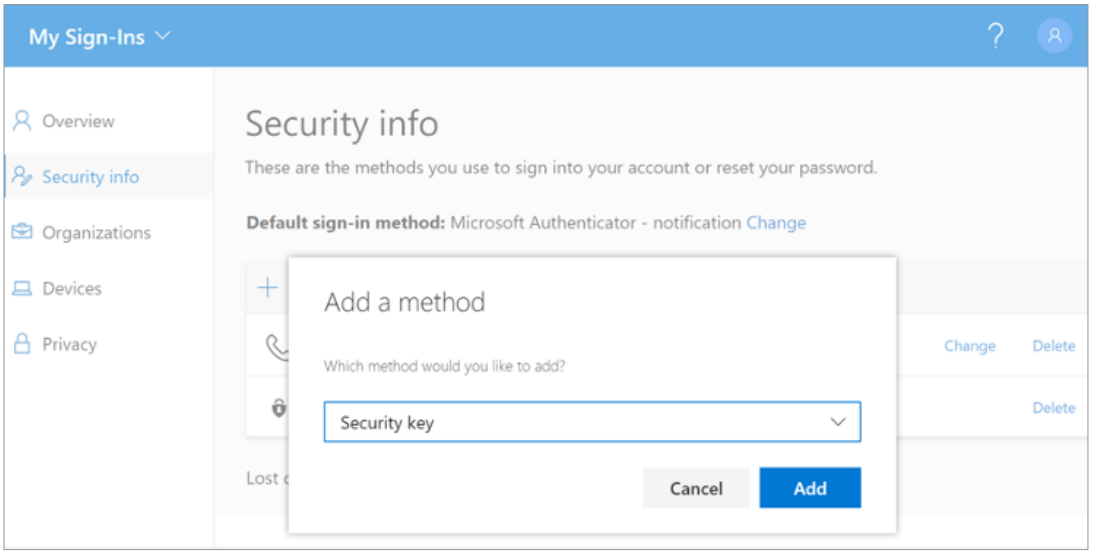
Documentation & References

- Enable passwordless security key sign-in (preview)
  - https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key

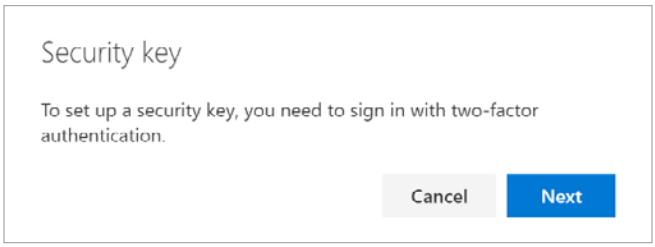
Fido2 Security Key Provisioning and Key Management

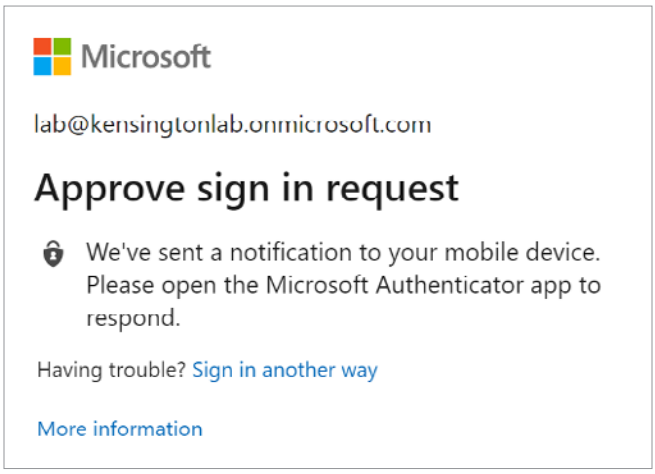
In this section, an eligible Microsoft 365 user within the organizational Azure AD tenant can register their Kensington VeriMark Guard FIDO2 security key. At present, administrators cannot provision or de-provision security keys on a user's behalf. Eligible users will need to perform a self-service registration.

1. Browse to https://myprofile.microsoft.com.
2. Select **Security Info**. If the user does not currently have any Azure AD 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**.

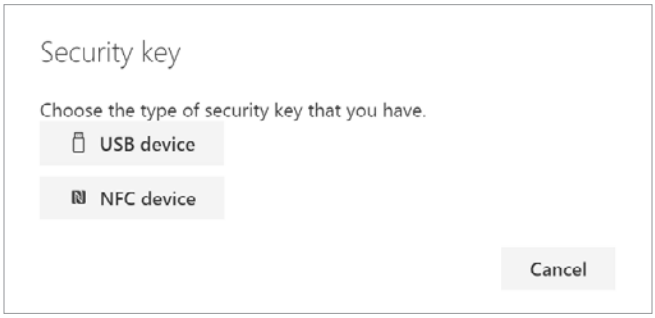


4. If prompted, click **Next** to sign in with two-factor authentication. In the second screenshot below, the user's default sign-in method is a Microsoft Authenticator notification.

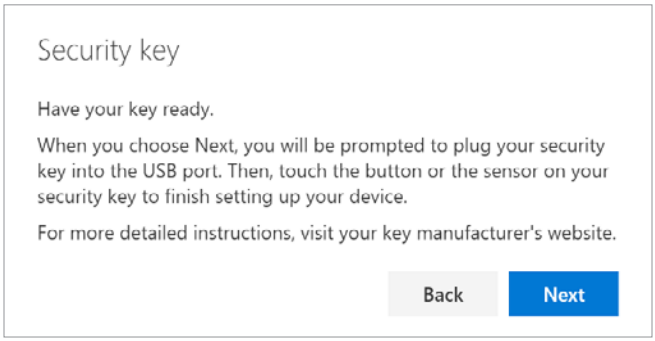


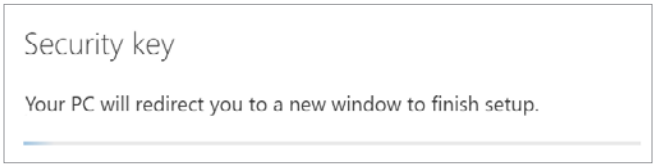


5. Select **USB device**.

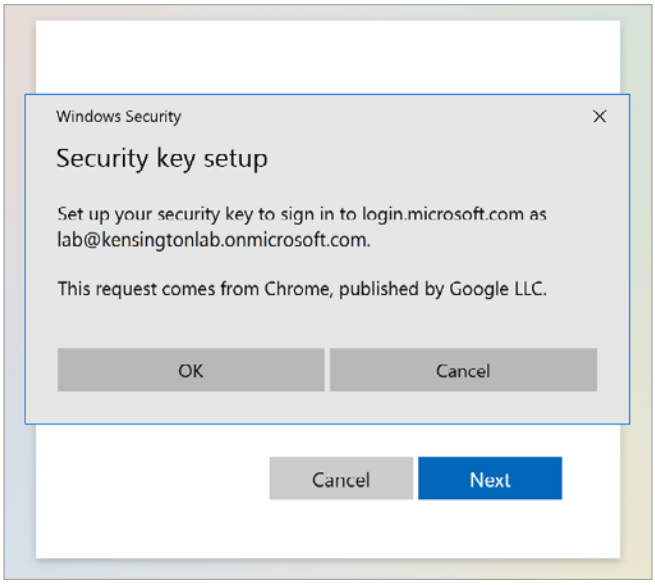


6. Verify that the Kensington VeriMark Guard FIDO2 security key is connected to the device, and click **Next**.

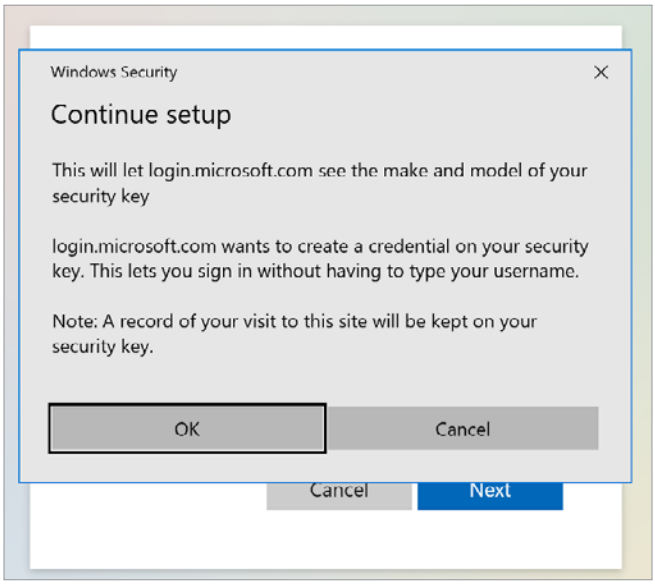




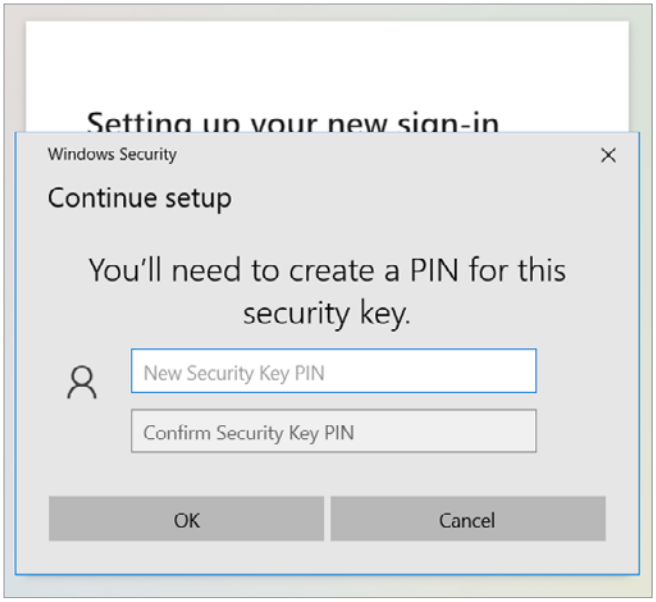
7. In the **Windows Security / Security key setup** dialog box, click **OK**.



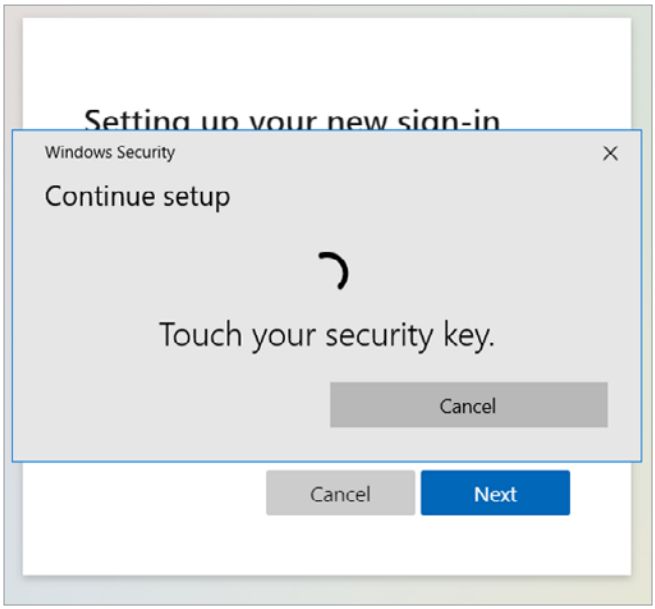
8. In the **Windows Security / Continue setup** dialog box, click **OK**.



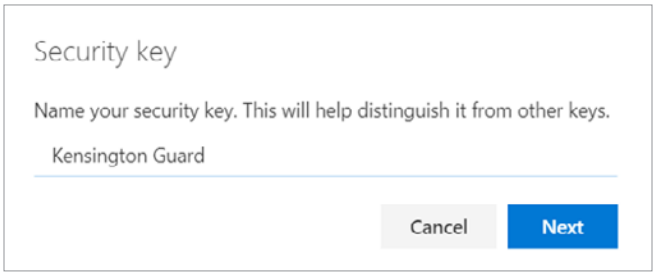
9. If prompted, create a PIN for the Kensington VeriMark Guard FIDO2 security key. This is only necessary during the initial setup of the security key.



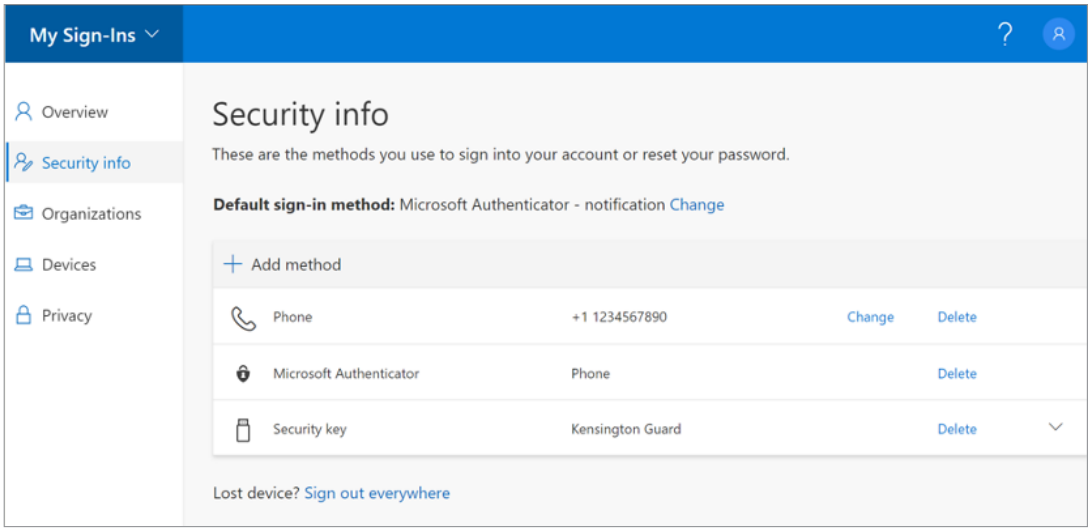
10. When prompted, touch the security key.



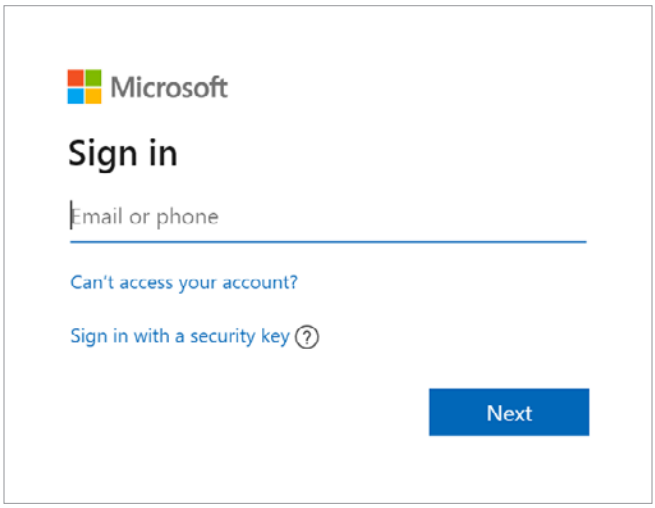
11. When prompted, enter a name for the security key.



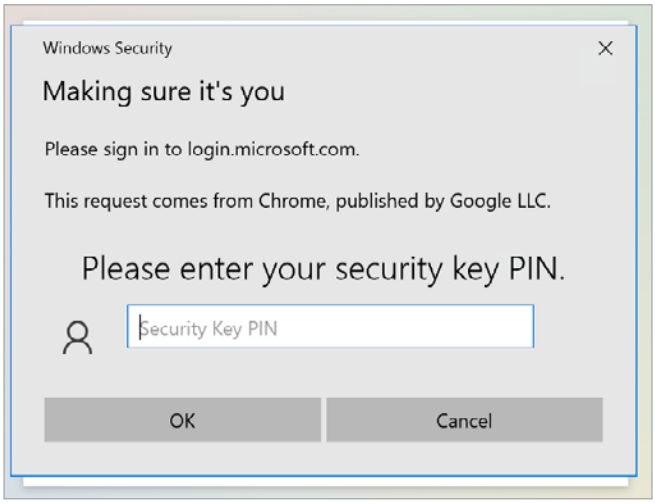
12. Verify that the **Kensington VeriMark Guard** security key is now a registered MFA method.



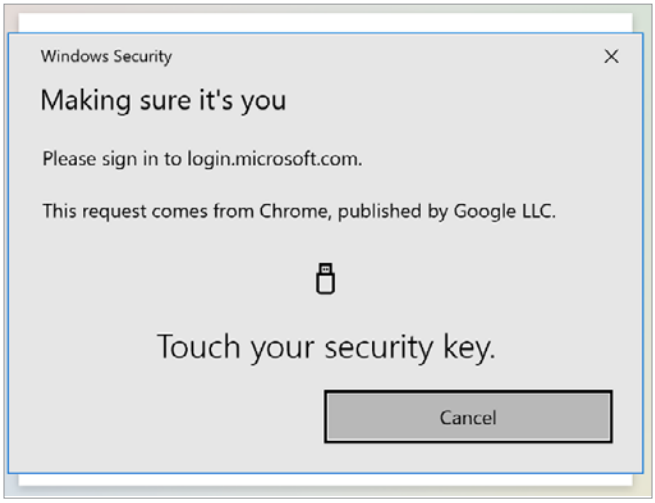
13. Test the security key by signing out (or opening a separate browser session) and navigating to https://myprofile.microsoft.com again. At the logon screen, select **Sign in with a security key**.



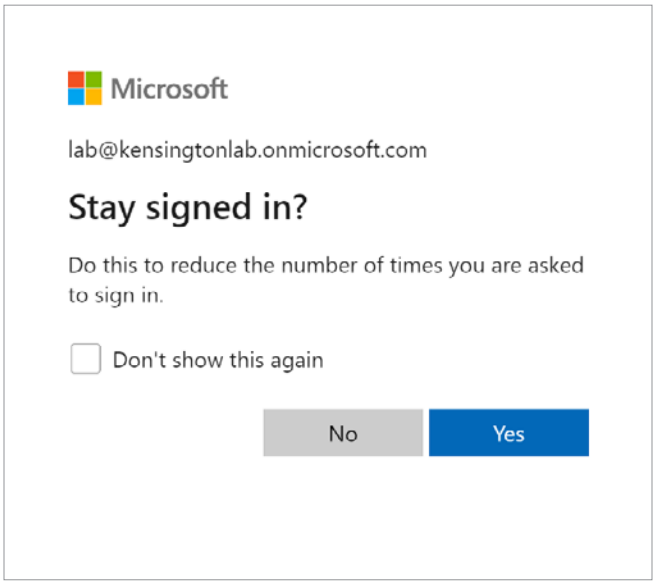
14. When prompted, provide the security key PIN.



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.

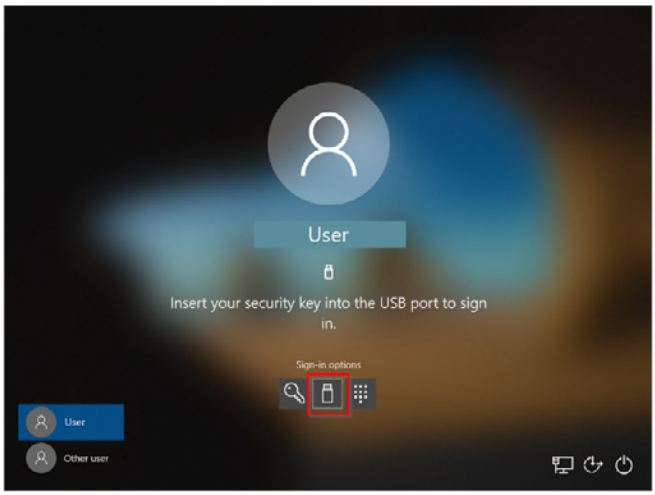
Documentation & References

- Enable passwordless security key sign-in (preview)
  - https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key
- Set up a security key as your verification method
  - https://docs.microsoft.com/en-us/azure/active-directory/user-help/security-info-setup-security-key

Configuring Windows 10 Sign-In Using Fido2 Security Keys (Modern Management / Azure Ad–Joined)

Azure AD–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:

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

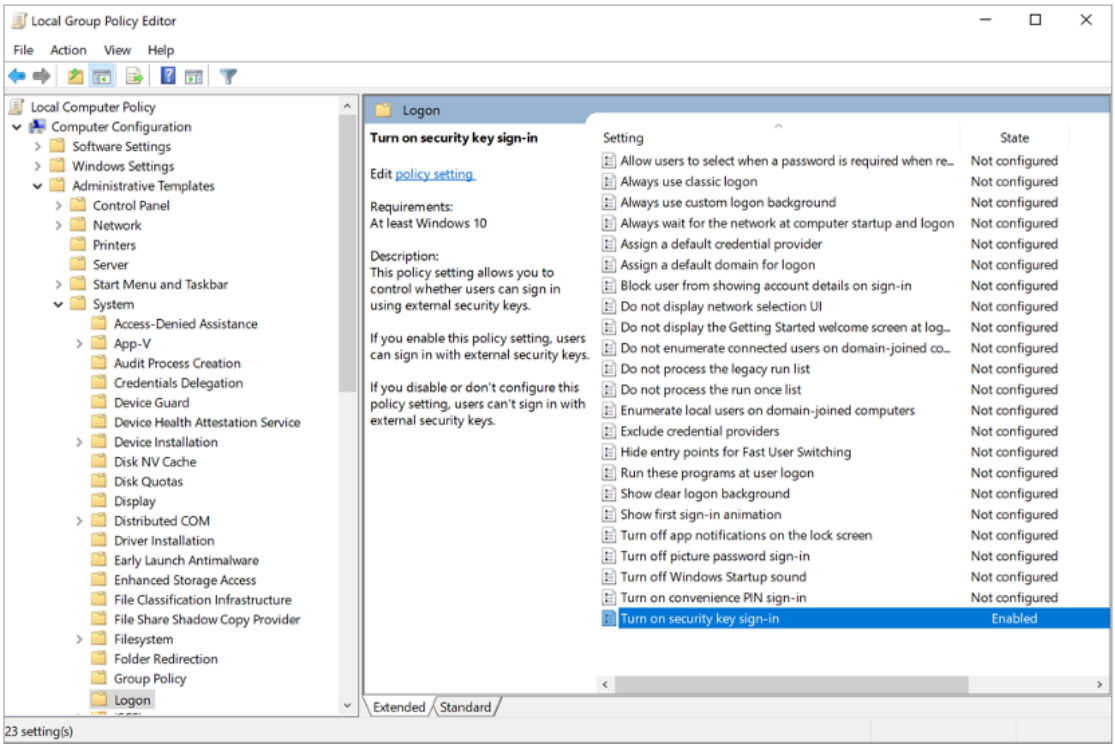


Microsoft offers a variety of broader deployment methods in their documentation; however, we will provide the following examples:

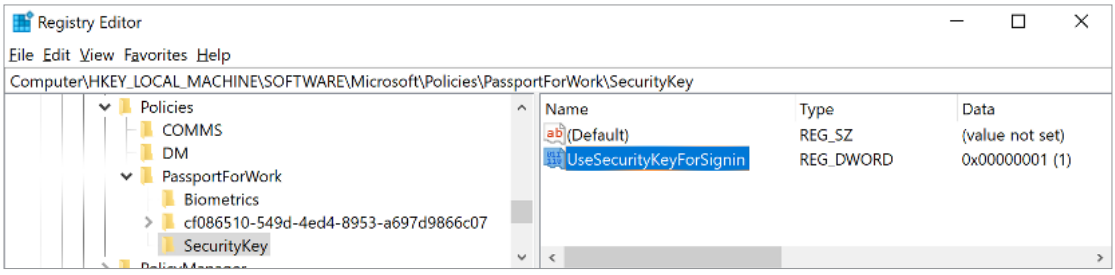
1. Enable manually on an individual device
2. Enable using Intune device configuration profile (targeted devices)
3. Enable using Intune Windows 10 enrollment policy (all eligible users/devices)

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.

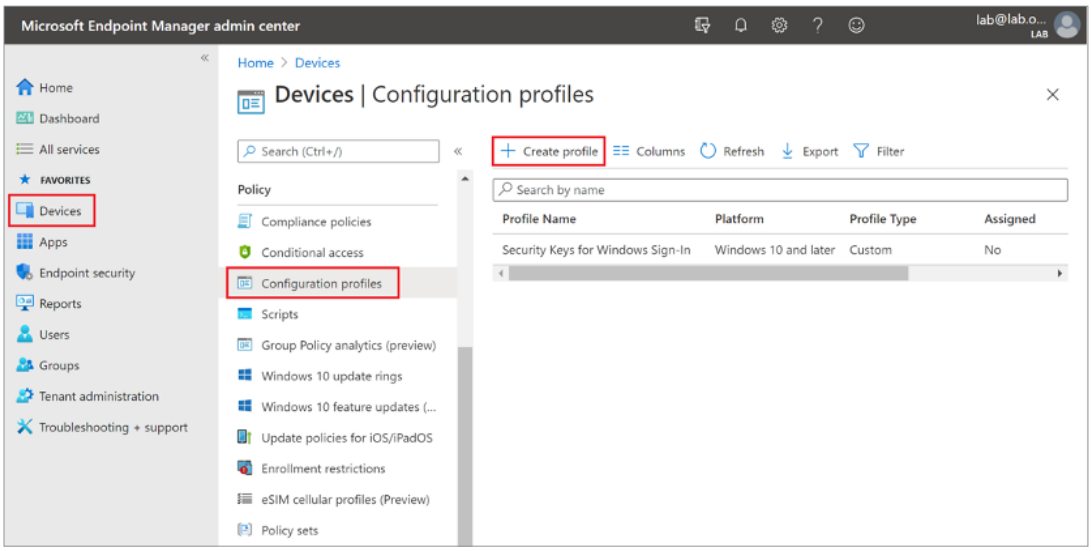



```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Policies\PassportForWork\SecurityKey]
“UseSecurityKeyForSignin”=dword:00000001
```

Enable Using Intune Device Configuration Profile

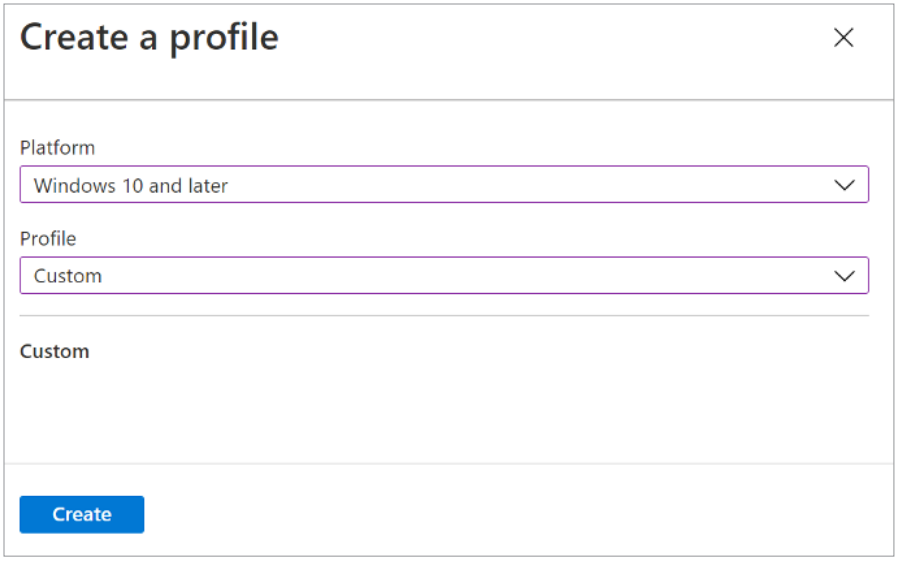
To target specific device groups to enable the credential provider, use the following custom settings via Intune:

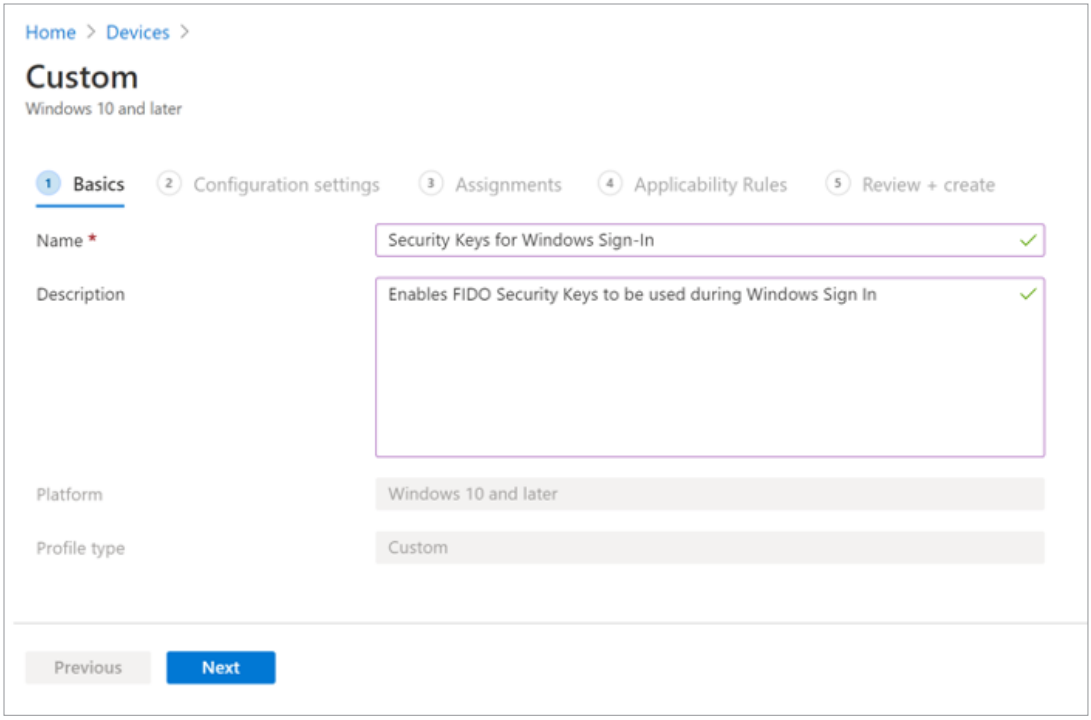
1. Browse to **Microsoft Endpoint Manager admin center > Devices > Configuration profiles > Create profile**.

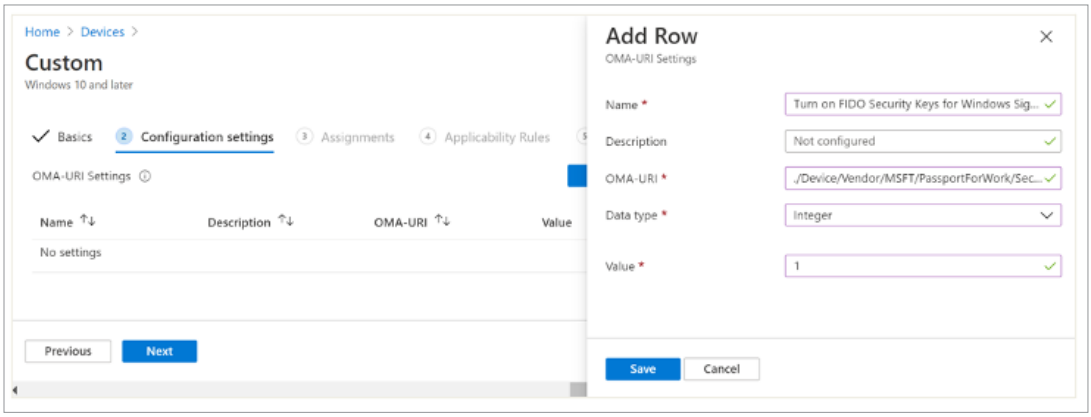


2. Configure the new profile with the following settings:

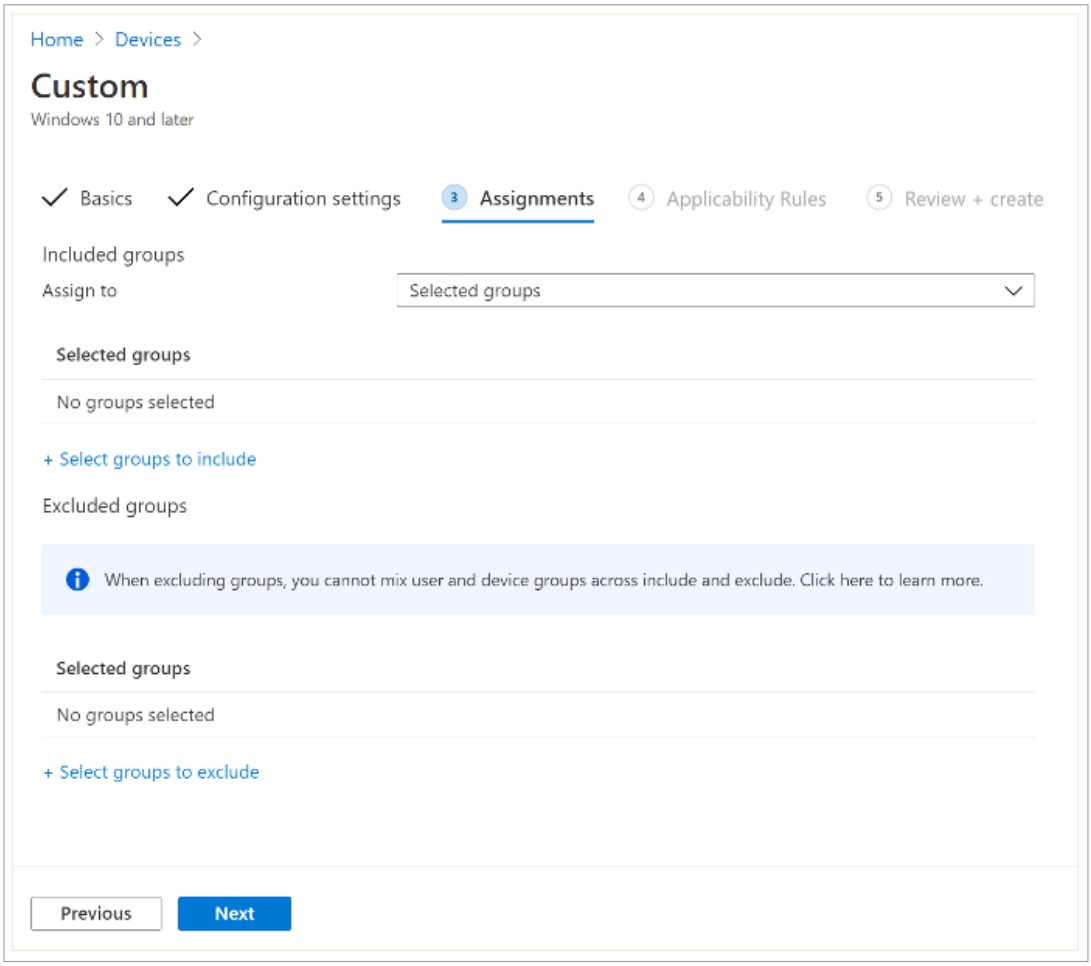
- Name: **Security Keys for Windows Sign-In**
- Description: **Enables FIDO Security Keys to be used during Windows Sign In**
- Platform: **Windows 10 and later**
- Profile type: **Custom**
- Custom OMA-URI Settings:
  - Name: **Turn on FIDO Security Keys for Windows Sign-**In
  - OMA-URI: **./Device/Vendor/MSFT/PassportForWork/SecurityKey/UseSecurityKeyForSigni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




Home > Devices >
Custom
Windows 10 and later
1 Basics
2 Configuration settings
3 Assignments
4 Applicability Rules
5 Review + create
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
Previous
Next


Home > Devices >
Custom
Windows 10 and later
Basics
2 Configuration settings
3 Assignments
4 Applicability Rules
OMA-URI Settings
Name
Description
OMA-URI
Value
No settings
Previous
Next
Add Row
OMA-URI Settings
Name *
Turn on FIDO Security Keys for Windows Sig...
Description
Not configured
OMA-URI *
./Device/Vendor/MSFT/PassportForWork/Sec...
Data type *
Integer
Value *
1
Save
Cancel

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

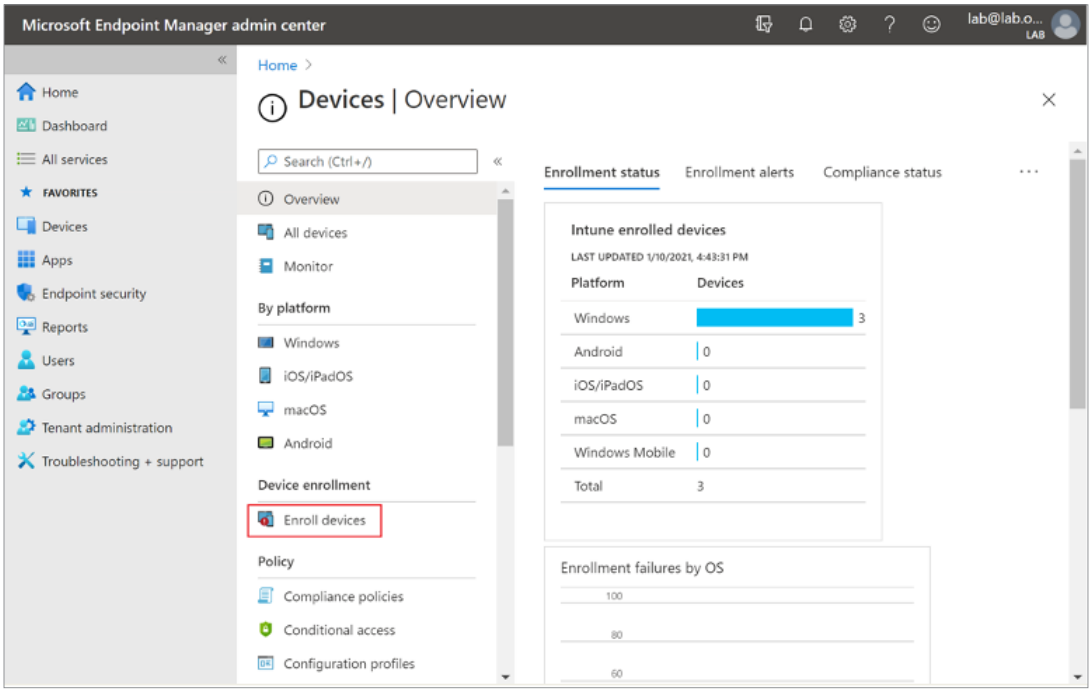


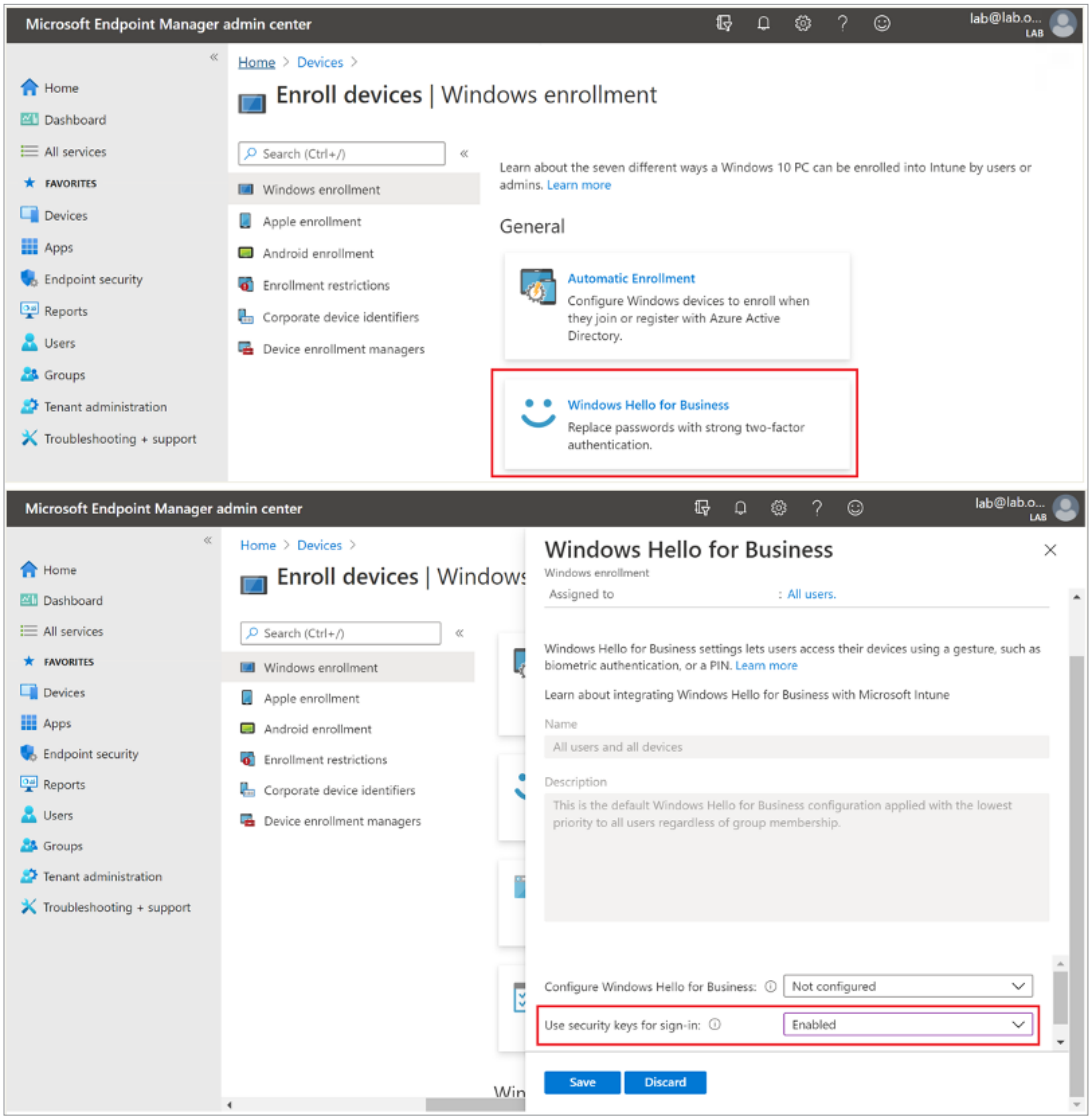
4. Customize any required applicability rules and create the policy.

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**.





Documentation & References

- Enable passwordless security key sign-in to Windows 10 devices with Azure Active Directory (preview)
  - https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key-windows

Configuring Windows 10 Sign-In Using Fido2 Security Keys (On-Premises Ad / Hybrid Azure Ad–Joined)

Hybrid Azure AD–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 Azure AD–integrated resources. This scenario is supported if the following requirements are met:

- Azure AD Multi-Factor Authentication (e.g., licensed and enabled in tenant)
- Combined security information registration preview
- Compatible FIDO2 security keys (e.g., Kensington VeriMark Guard)
- Hybrid Azure AD–joined devices require Windows 10 version 2004 or higher
- Fully patched Windows Server 2016/2019 domain controllers
- Azure AD 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.

Documentation & References

- Enable passwordless security key sign-in to Windows 10 devices with Azure Active Directory (preview)
  - https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key-windows
- Enable passwordless security key sign-in to on-premises resources with Azure Active Directory (preview)
  - https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key-on-premises
- Deployment frequently asked questions (FAQs) for hybrid FIDO2 security keys in Azure AD (preview)
  - https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-faqs
- Troubleshooting for hybrid deployments of FIDO2 security keys in Azure AD (preview)
  - https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-troubleshoot