Troubleshooting Azure passwordless security key sign in for Windows

Introduction

This guide is intended to help troubleshoot devices that have been configured, or are being configured, but are having issues with Azure Passwordless security key sign in. This guide is specifically for Azure Active Directory (AAD) joined Windows machines, or hybrid Azure AD joined (HAADJ) Windows machines. If you would like to use a local account with a Yubikey, please follow the Yubico Login for Windows Configuration Guide.

Baseline configuration check

The Azure AD tenant must be configured to support FIDO2 authentication. When encountering issues with a deployment it is common that one one of the configuration steps was skipped. Please review the environment and ensure all configurations were completed as outlined in the deployment guide: YubiKeys for Microsoft Azure AD Passwordless Sign In Guide – Yubico.

Quick checks

- Azure AD joined Windows 10 devices must be at version 1909 or higher.
- Hybrid Azure AD joined Windows 10 devices must be at version 2004 or higher.
- Windows 10 must be enabled for security key sign in. This is checked by looking at Window registry keys. Ensure that one of the following are set:
    - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Policies\PassportForWork\SecurityKey]
        - "UseSecurityKeyForSignin"=dword:00000001
    - [HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\FIDO]
        - "EnableFIDODeviceLogon"=dword:00000001

No security key icon on the sign in screen

The feature to sign in with a security key, turning on the security key icon on the sign in screen, is controlled by a registry key. There are several ways this is managed, please see the appropriate section according to how it was deployed:

Enabled by Intune

1. Ensure that the registry key **UseSecurityKeyForSignin** is set to **1** by Intune policy
    a. [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Policies\PassportForWork\SecurityKey]
        i. "**UseSecurityKeyForSignin**"=dword:00000001

Enabled by GPO

1. Ensure that the registry key **EnableFIDODeviceLogon** is set to **1**
    a. [HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\FIDO]
        i. "**EnableFIDODeviceLogon**"=dword:00000001
2. You can find this setting in the group policy in the following location
    a. Configure the setting Computer Configuration > Administrative Templates > System > Logon > Turn on security key sign-in
    b. Set to **Enabled** and link GPO accordingly
3. Validate that Intune isn't applying settings by checking **UseSecurityKeyForSignin** registry key and ensure it is set to **1**
    a. [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Policies\PassportForWork\SecurityKey]
        i. "UseSecurityKeyForSignin"=dword:00000001

Enabled by provisioning package

1. Ensure that the provisioning package is configured to enable UseSecurityKeyForSignin
2. Launch Windows Configuration Designer
3. Select **File > Open Project**
4. Navigate to directory where Provisioning Package was exported and open the .icdproj file
5. in the left panel, browse to: **Runtime settings > WindowsHelloForBusiness > SecurityKeys > UseSecurityKeyForSignIn**.
6. In the middle panel, change the **UseSecurityKeyForSignIn** to **Enabled**
7. Export the Provisioning Package and install on the machine
8. Validate that Intune isn't applying settings by checking **UseSecurityKeyForSignin** registry key and ensure it is set to **1**
    a. [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Policies\PassportForWork\SecurityKey]
        i. "UseSecurityKeyForSignin"=dword:00000001

Security key icon should not be on sign in screen

This is typically caused by conflicting security configurations on the Windows 10 client. There are two registry keys used by Windows to enable and disable the security key icon on the sign in screen. The registry key UseSecurityKeyForSignin, usually set by Intune, will take precedence over EnableFIDODeviceLogon, usually set by GPO. If there are multiple configurations being applied be aware that UseSecurityKeyForSignin will always take precedence.

There have been reports from customers that have also found other GPOs in their environment that have caused issues with passwordless sign in. Depending on the link order

of GPOs, conflicting security settings can cause Windows to act differently than expected. Review your GPO configurations if after following this documentation you are still experiencing problems.

Managed by Intune

1. Ensure that the registry key **UseSecurityKeyForSignin** is set to **0** by Intune policy
    a. [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Policies\PassportForWork\SecurityKey]
        i. "**UseSecurityKeyForSignin**"=dword:00000000

Managed by GPO

1. Ensure that the registry key **EnableFIDODeviceLogon** is set to **0**
    a. [HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\FIDO]
        i. "**EnableFIDODeviceLogon**"=dword:00000000
2. You can find this setting in the group policy in the following location
    a. Configure the setting Computer Configuration > Administrative Templates > System > Logon > Turn on security key sign-in
    b. Set to **Disabled** and link GPO accordingly
3. Validate that Intune isn't applying settings by checking **UseSecurityKeyForSignin** registry key and ensure it is set to **0**
    a. [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Policies\PassportForWork\SecurityKey]
        i. "UseSecurityKeyForSignin"=dword:00000000

Configured through provisioning package

Ensure that the provisioning package is configured to enable UseSecurityKeyForSignin

1. Launch Windows Configuration Designer
2. Select **File > Open Project**
3. Navigate to directory where Provisioning Package was exported and open the .icdproj file
4. in the left panel, browse to: **Runtime settings > WindowsHelloForBusiness > SecurityKeys > UseSecurityKeyForSignIn**.
5. In the middle panel, change the **UseSecurityKeyForSignIn** to **Disabled**
6. Export the Provisioning Package and install on the machine
7. Validate that Intune isn't applying settings by checking **UseSecurityKeyForSignin** registry key and ensure it is set to **0**

a. [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Policies\PassportForWork\SecurityKey]
    i. "UseSecurityKeyForSignin"=dword:00000000

Windows Configuration Designer setting not available

When configuring the Provisioning Package you may run into a situation where you do not see the option to enable **UseSecurityKeyForSignin**. This occurs when the incorrect Windows edition is selected while creating your project for the Provisioning Package. To resolve this issue follow the steps below:

1. Close your current project in Windows Configuration Designer
2. Select **File > Open Project**
3. Select the directory for the project you originally created and delete it
4. Close the navigation window
5. Select **File > New Project**
6. Give your project a name and take note of the path where your project is created, then select **Next**.
7. Leave Provisioning package selected as the Selected project workflow and select **Next**.
8. At this step ensure that you select **All Windows Desktop editions**
9. At the next window you will now be able to follow the steps outlined in the Admin Deployment Guide to enable **UseSecurityKeyForSignin**

First sign in with a security key requires Windows to be online

The first time a user signs into Windows with a security key it is required that Windows is online and able to contact Azure AD. This is by design to authenticate the user and their machine to Azure AD. After this initial sign in the user can sign in using a security key offline.

Privileged users are unable to sign in with a security key

This is a default security policy to prevent Azure AD high privileged accounts from signing into on-premises resources. This is outlined in Microsoft's FAQ FIDO2 security documentation.

To unblock the accounts, use Active Directory Users and Computers to modify the msDS-NeverRevealGroup property of the Azure AD Kerberos Computer object (CN=AzureADKerberos,OU=Domain Controllers,<domain-DN>).