Troubleshooting Entra ID passwordless security key sign in for Windows

Copyright

Trademarks

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

Contact Information

Yubico Inc
5201 Great America Pkwy #122
Santa Clara, CA 95054
USA
yubi.co/contact

Version History

Version	Date	Changes
1.0	May 20, 2025	• Initial Release

Introduction

This guide is intended to help troubleshoot devices that have been configured, or are being configured, but are having issues with Entra ID passkey (FIDO2) security key sign in. This guide is specifically for Entra joined Windows devices, or Entra hybrid joined Windows devices.

Baseline configuration check

The Entra ID 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 **Admin Deployment Guide**.

Quick Checks

- Entra joined Windows 10 devices must be at version 1909 or higher.
- Entra hybrid joined Windows 10 devices must be at version 2004 or higher.
- Windows 10/11 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
    a. Select **File** > **Open Project**
3. Navigate to directory where Provisioning Package was exported and open the .icdproj file
    a. In the left panel, browse to: **Runtime settings > WindowsHelloForBusiness > SecurityKeys > UseSecurityKeyForSignIn**.
4. In the middle panel, change the **UseSecurityKeyForSignIn** to **Enabled**
5. Export the Provisioning Package and install on the machine
6. 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 10/11 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
4. .icdproj file 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
8. select Next.
9. At this step ensure that you select **All Windows Desktop editions**
10. At the next window you will now be able to follow the steps outlined in the
11. 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 Entra ID. When a user signs in to their Microsoft Entra joined or hybrid joined device while connected to the internet, Microsoft Entra ID issues a Primary Refresh Token (PRT) to the device.The PRT is valid for 14-days and renewed continuously every 4-hours as long as the device is in use. If the device remains offline for more than 14 days, the cached PRT will likely expire. When the user attempts to sign in after this 14-day period without an internet connection, the device will no longer be able to verify the cached PRT. As a result, the user will likely be unable to sign in to the device using their Microsoft Entra credentials until the device is connected to the internet again and can re-authenticate with Microsoft Entra ID to obtain a new PRT.

Privileged users are unable to sign-in with a security key

The default security policy doesn't grant Microsoft Entra permission to sign high privilege accounts on to on-premises resources. Due to possible attack vectors from Microsoft Entra ID to Active Directory, it's not recommended to unblock these accounts by relaxing the Password Replication Policy of the computer object CN=AzureADKerberos,OU=Domain Controllers,<domain-DN>

Sign-in with a security key containing multiple passkeys

When signing in or unlocking a Windows device using a security key that contains multiple Microsoft Entra accounts, the device defaults to the last account added to the key.

Users aren't able to use FIDO2 security keys immediately after they create a Microsoft Entra hybrid joined machine

After the domain-join and restart process on a clean install of a Microsoft Entra hybrid joined machine, you must sign in with a password and wait for policy to synchronize before you can use a FIDO2 security key to sign in.

This behavior is a known limitation for domain-joined devices, and isn't specific to FIDO2 security keys.

To check the current status, use the **dsregcmd /status** command. Check that both **AzureAdJoined** and **DomainJoined** show **YES**.

Users unable to get SSO to NTLM network resources after signing in with a FIDO2 security key are receiving a credential prompt

Make sure that enough DCs are patched to respond in time to service your resource request. To check if you can see a server that is running the feature, review the output of **nltest /dsgetdc:<dc name> /keylist /kdc**

If you're able to see a DC with this feature, the user's password may have changed since they signed in, or there's another issue.

Users are unable to sign-in using a security key even when online in a hybrid environment

Verify that the Entra Kerberos Server object has been created in the on-premises Active Directory Domain and has been published to the Entra tenant

Viewing and verifying the Entra ID Kerberos Server

1. Launch **Powershell** as an **Administrator**.
2. Execute the following PowerShell command to view and verify the newly created Entra ID Kerberos server object.

```
# When prompted to provide domain credentials use the
userprincipalname format for the username instead of domain\username

Get-AzureADKerberosServer -Domain $domain -UserPrincipalName
$userPrincipalName -DomainCredential (get-credential)
```

This command returns the properties of the Entra ID Kerberos Server object. Review the output to ensure the values align with your environment. The following is an example showing a subset of the output. Ensure that the kerberos user and computer account objects have been created successfully:

Property	Value
ID	****
UserAccount	CN=krbtgt_AzureAD,CN=Users,DC=contoso,DC=corp,DC=com
ComputerAccount	CN=AzureADKerberos,OU=Domain Controllers, DC=contoso, DC=corp,DC=com
DisplayName	krbtgt_****
DomainDnsName	Contoso.corp.com
KeyVersion	1364170
KeyUpdatedFrom	dc.contoso.corp.com
CloudDisplayName	krbtgt_****
CloudDomainDnsName	contoso.corp.com

FIDO2 sign-in is blocked due to expired password

If your password has expired, signing in with FIDO is blocked. The expectation is that users reset their passwords before they can log in by using FIDO. This behavior applies to hybrid on-premises synced user sign-in with cloud kerberos trust.