YubiKeys for Azure AD Passwordless

Admin Deployment Guide

Copyright

Trademarks

Yubico and YubiKey are registered trademarks of Yubico Inc. All other trademarks are the property of their respective owners.

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

Original Document Release Date

September 22, 2020

Version History

Version	Date	Changes
2.3	May 8, 2023	Added TAP and associated caveats. Reference links to Conditional Access and deployment flows. Status update on mobile support.
2.2	Dec 21, 2022	Small update to the "Combined Security Information" notice
2.1	July 29, 2021	Minor revisions
2.0	March 2, 2021	Updated for general availability
1.0	October 28, 2020	Added Appendix A - Licensing Requirements
0.5	September 22, 2020	Initial Release

Introduction

This document outlines how to enable passwordless (FIDO2) YubiKey security key sign-in within Microsoft Azure Active Directory (AAD) environments. It also includes instructions for enabling access to on-premise resources using kerberos tickets issued from a local Active Directory.

Objectives

- Enable passwordless (FIDO2) security key sign-in for web-based applications using AAD identities
- Enable passwordless (FIDO2) security key sign-in into on-premise resources
- Enable passwordless (FIDO2) security key sign-in into Windows 10 machines

Before you begin

- Make sure you have an AAD tenant with Azure Multi-Factor Authentication (MFA) enabled.
- Microsoft Azure Licensing requirements are outlined in Appendix A. *Note: licensing requirements are subject to change.*
- Yubico recommends identifying a select number of users or a group to test these configurations instead of applying to all users.
    - As Microsoft blocks high privileged users from signing in with a Security Key as default, we recommend test users with lower privileges for testing. To learn more, please refer to FIDO2 security key sign-in isn't working for my Domain Admin or other high privilege accounts. Why?
- Note that Microsoft requires the end user to authenticate with another form of multi-factor authentication prior to enrolling a FIDO2 security key within their account. This can be accomplished via either the Azure AD Temporary Access Pass (TAP) feature or by using a YubiKey 5 Series device as an OATH TOTP token in conjunction with the Yubico Authenticator app. The latter approach is preferable as it does not require the user to enroll an alternate MFA solution prior to enrolling their YubiKey as a FIDO2 token. However, there are some limitations with the TAP solution.
    - After enrollment of the YubiKey as a FIDO2 security key, it can be used as the primary authentication method going forward.

Minimum Requirements

Hardware

- At least one and preferably two of any of these YubiKeys
    - YubiKey 5 Series
    - YubiKey Bio series
    - YubiKey Security Key

Software

- An Azure compatible browser and platform.
    - Note: Android and iOS are not supported, but Microsoft states these platforms are in development. Contact your Microsoft representative for details.
- For web-based applications:
    - Windows 10 version 1903 or later.
- For Azure domain joined Windows log-in
    - Windows 10 version 1909 or later.
- For single sign on (SSO) into on-premise resources and hybrid joined Windows log-in:
    - Windows 10 2004 or later.
    - Azure AD Connect (latest version)
    - Windows Server 2016 or 2019 Domain Controller with the latest patches
        - For Windows Server 2016 - https://support.microsoft.com/help/4534307/windows-10-update-kb4534307
        - For Windows Server 2019 - https://support.microsoft.com/help/4534321/windows-10-update-kb4534321

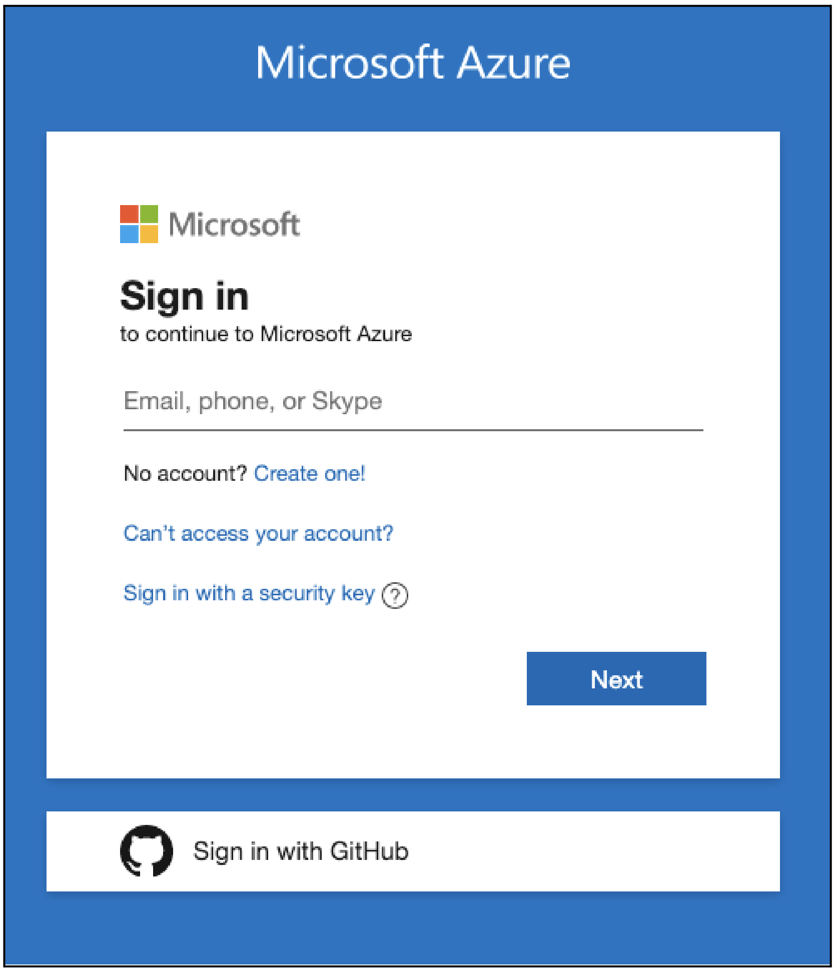
Enabling passwordless (FIDO2) security key sign-in for web-based applications

This section describes how to enable AAD identities to leverage FIDO2 security keys for passwordless authentication into web-based applications. This feature requires that the combined security information registration be enabled.

Enabling combined security information registration

> *Note:* Effective Oct. 1st, 2022, Microsoft will begin to enable combined registration for all users in Azure AD tenants created before August 15th, 2020. Tenants created after this date are enabled with combined registration. This means that the option *"Users can use the combined security information registration experience"* might no longer be visible under *"User settings"* as it is already enabled.

1. Navigate to the Azure Portal (https://portal.azure.com).



Microsoft Azure

Microsoft

Sign in

to continue to Microsoft Azure

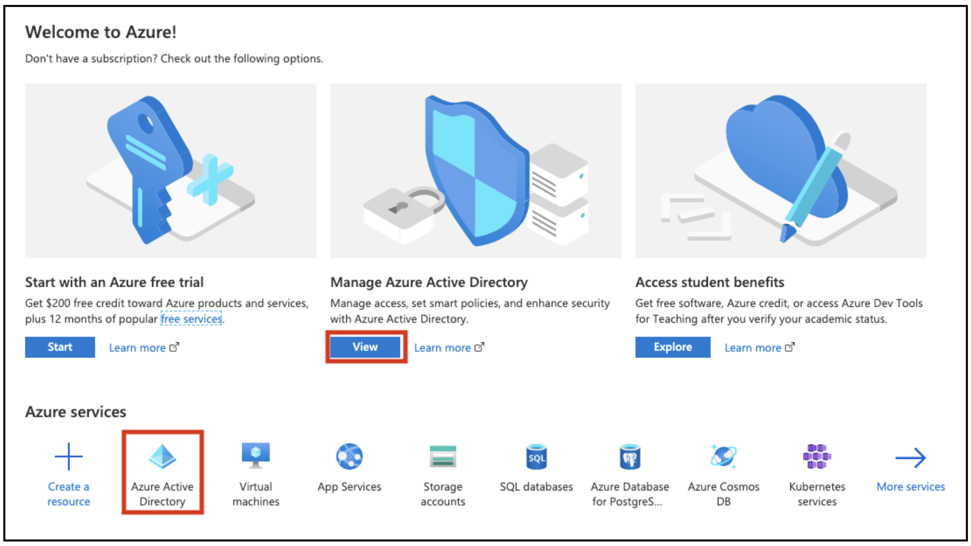
Email, phone, or Skype

No account? Create one!

Can't access your account?

Sign in with a security key ?

2. Sign in as the global administrator.
3. Navigate to Azure Active Directory.



Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

Manage Azure Active Directory

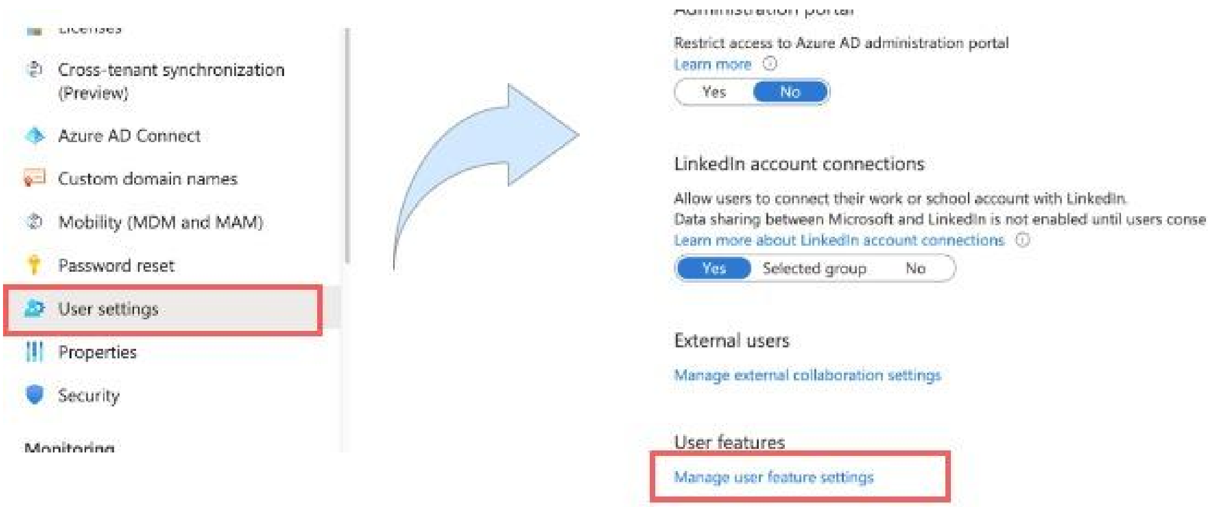
Manage access, set smart policies, and enhance security with Azure Active Directory.

Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

Azure services

4. Under **Manage**, select **User Settings.**
5. Under **User features**, select **Manage user feature settings**



Licenses

Cross-tenant synchronization (Preview)

Azure AD Connect

Custom domain names

Mobility (MDM and MAM)

Password reset

User settings

Properties

Security

Monitoring

Administration portal

Restrict access to Azure AD administration portal
Learn more

Yes [✓ No]

LinkedIn account connections

Allow users to connect their work or school account with LinkedIn.
Data sharing between Microsoft and LinkedIn is not enabled until users conse
Learn more about LinkedIn account connections

[✓ Yes] Selected group No

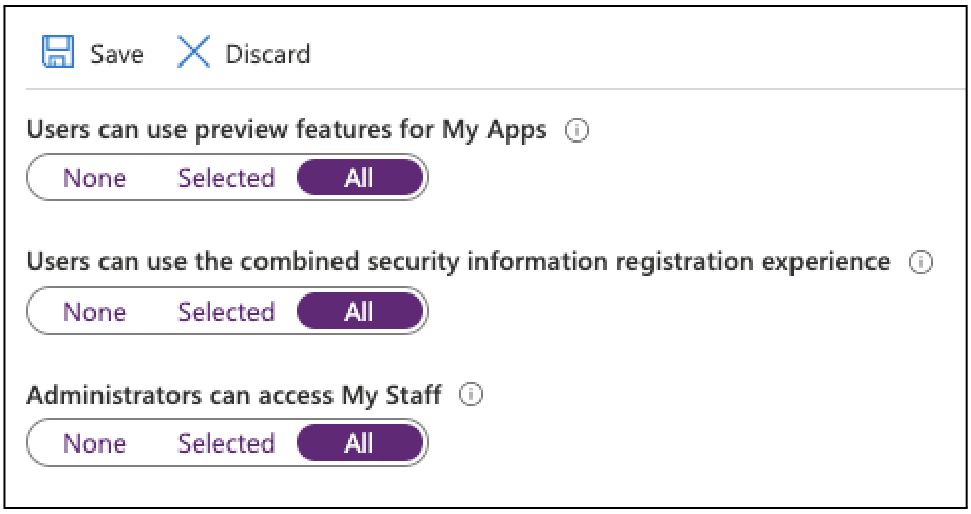
External users

Manage external collaboration settings

User features

Manage user feature settings

6. Under **Users can use the combined security information registration experience**, choose either **Selected** or **All**.



Save Discard

Users can use preview features for My Apps
None Selected [✓ All]

Users can use the combined security information registration experience
None Selected [✓ All]

Administrators can access My Staff
None Selected [✓ All]

As noted above, all new Azure AD tenants as well as tenants created before August 15th 2020 will have combined security information registration enabled automatically from October 1st 2022.

   a. Choosing **Select,** allows an organization to limit this registration feature to specific groups of users.
   b. Choosing **All**, allows all users within this AAD access to this feature.

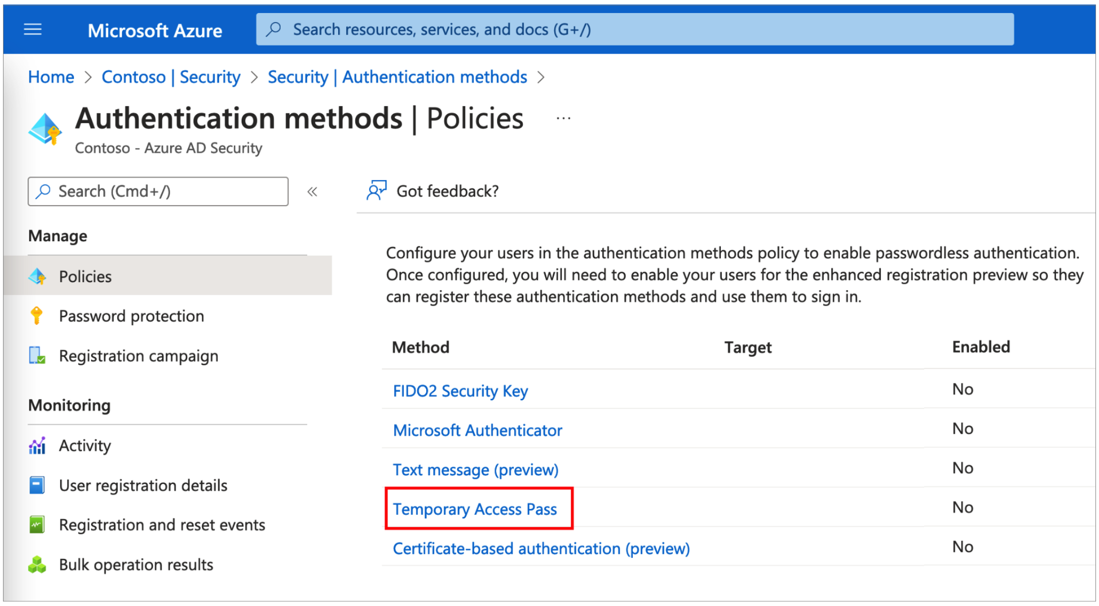
7. Click **Save** to apply changes.

Configure Temporary Access Pass in Azure AD

As noted in the “Before You Begin” section, one option to bootstrap your users to YubiKey-FIDO2 is to enable Temporary Access Pass (TAP). A Temporary Access Pass is a time-limited passcode that can be configured for multi or single use to allow users to onboard other authentication methods including passwordless methods including YubiKey-FIDO2.

Global administrator and Authentication Policy administrator role holders can update the Temporary Access Pass authentication method policy. To configure the Temporary Access Pass authentication method policy:

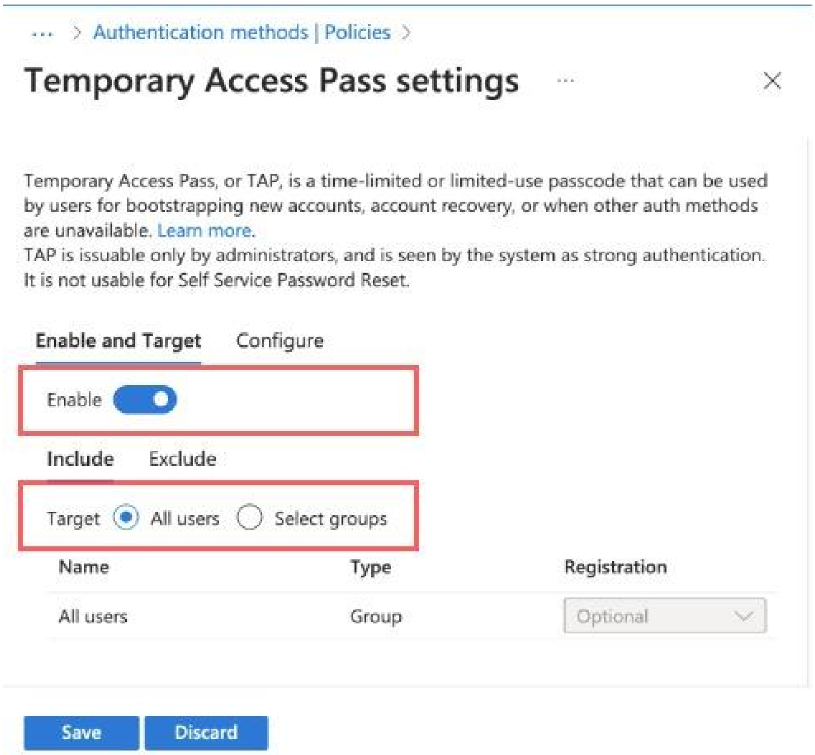
1. Sign in to the Azure portal using an account with global administrator permissions.
2. Search for and select **Azure Active Directory**, then choose **Security** from the menu on the left-hand side.
3. Under the **Manage** menu header, select **Authentication methods > Policies**.
4. From the list of available authentication methods, select **Temporary Access Pass**.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Contoso | Security > Security | Authentication methods >
Authentication methods | Policies
Contoso - Azure AD Security
Search (Cmd+/)
Got feedback?
Manage
Policies
Password protection
Registration campaign
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results

Configure your users in the authentication methods policy to enable passwordless authentication. Once configured, you will need to enable your users for the enhanced registration preview so they can register these authentication methods and use them to sign in.

Method	Target	Enabled
FIDO2 Security Key		No
Microsoft Authenticator		No
Text message (preview)		No
Temporary Access Pass		No
Certificate-based authentication (preview)		No

5. Set the **Enable** to **Yes** to enable the policy. Then select the **Target** users.



... > Authentication methods | Policies >

Temporary Access Pass settings

Temporary Access Pass, or TAP, is a time-limited or limited-use passcode that can be used by users for bootstrapping new accounts, account recovery, or when other auth methods are unavailable. Learn more.
TAP is issuable only by administrators, and is seen by the system as strong authentication. It is not usable for Self Service Password Reset.

Enable and Target | Configure

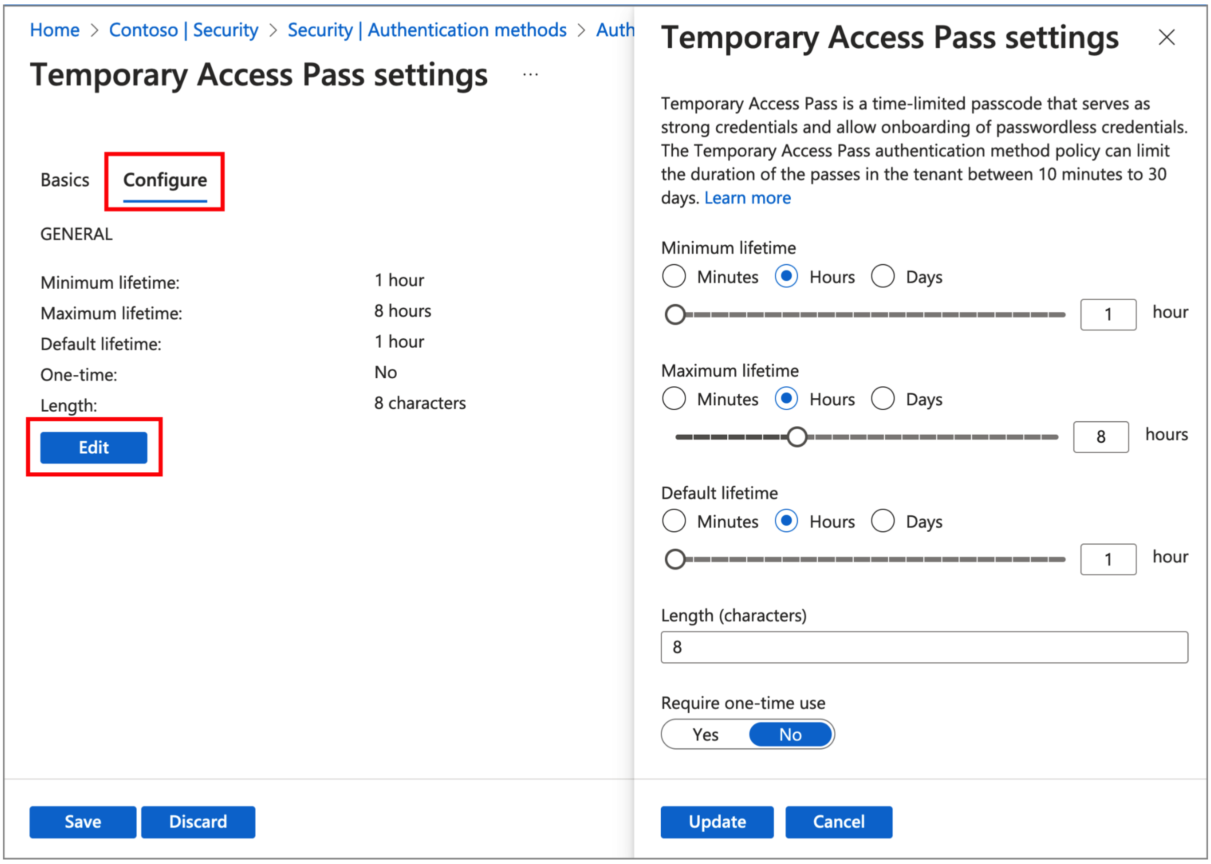
Enable: On

Include | Exclude

Target ● All users ○ Select groups

Name	Type	Registration
All users	Group	Optional

6. (Optional) Select **Configure** and modify the default Temporary Access Pass settings, such as setting maximum lifetime, or length.



Home > Contoso | Security > Security | Authentication methods > Auth

Temporary Access Pass settings

Basics | Configure

GENERAL

Minimum lifetime:	1 hour
Maximum lifetime:	8 hours
Default lifetime:	1 hour
One-time:	No
Length:	8 characters

Temporary Access Pass settings

Temporary Access Pass is a time-limited passcode that serves as strong credentials and allow onboarding of passwordless credentials. The Temporary Access Pass authentication method policy can limit the duration of the passes in the tenant between 10 minutes to 30 days. Learn more

Minimum lifetime
○ Minutes ● Hours ○ Days
1 hour

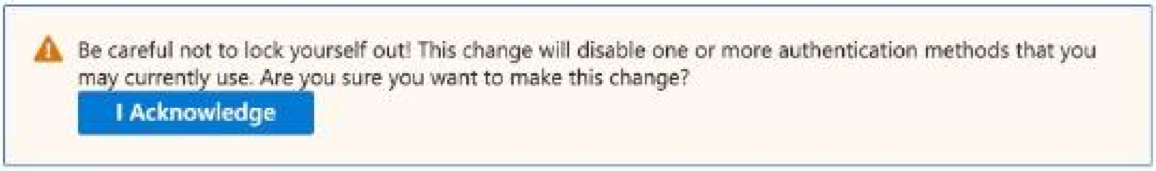
Maximum lifetime
○ Minutes ● Hours ○ Days
8 hours

Default lifetime
○ Minutes ● Hours ○ Days
1 hour

Length (characters)
8

Require one-time use
Yes [✓ No]

NOTE: Use Caution - changes to Access/Authentication policies will impact user access. Be careful not to lock out admin users. Microsoft may display messages as a reminder.



Be careful not to lock yourself out! This change will disable one or more authentication methods that you may currently use. Are you sure you want to make this change?

7. Select **Save** to apply the policy.

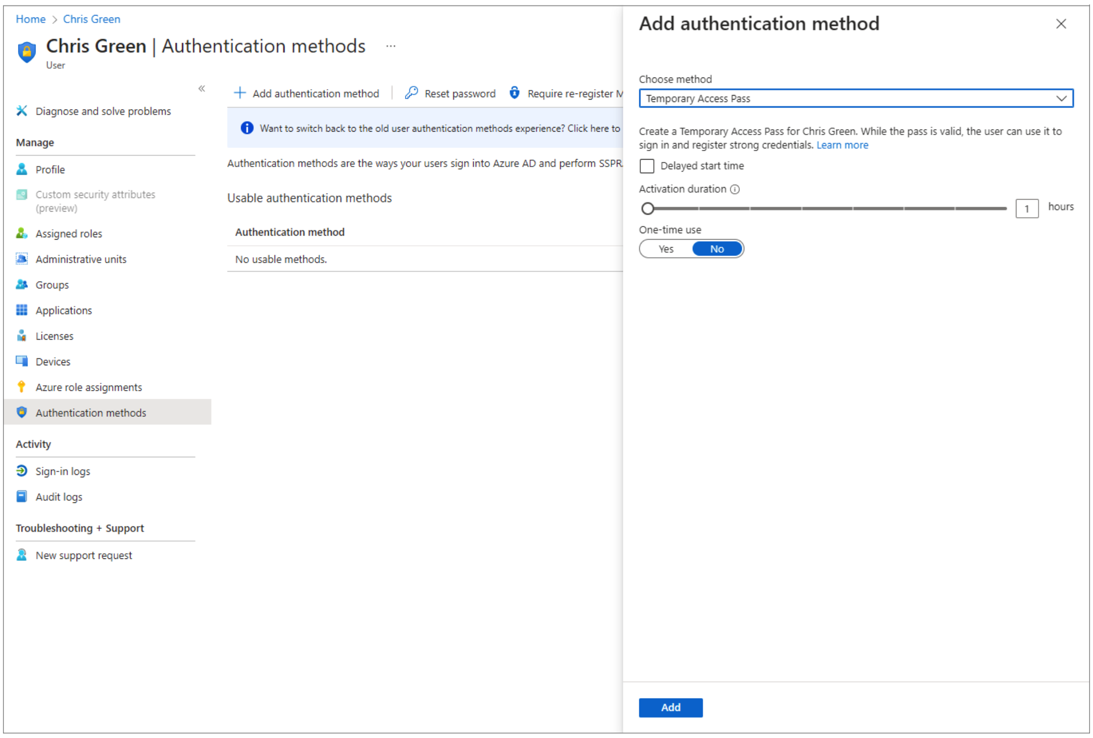
Create a Temporary Access Pass

After you enable a policy, you can create a Temporary Access Pass for a user in Azure AD. These roles can perform the following actions related to a Temporary Access Pass.

- Global Administrators can create, delete, and view a Temporary Access Pass on any user (except themselves)
- Privileged Authentication Administrators can create, delete, and view a Temporary Access Pass on admins and members (except themselves)
- Authentication Administrators can create, delete, and view a Temporary Access Pass on members (except themselves)
- Global Reader can view the Temporary Access Pass details on the user (without reading the code itself).

1. Sign in to the Azure portal as either a Global administrator, Privileged Authentication administrator, or Authentication administrator.
2. Select **Azure Active Directory**, browse to Users, select a user, such as Chris Green, then choose **Authentication methods**.
3. If needed, select the option to **Try the new user authentication methods experience**.
4. Select the option to **Add authentication methods**.
5. Below **Choose method**, select **Temporary Access Pass**.

6. Define a custom activation time or duration and select **Add**.



Want to switch back to the old user authentication methods experience? Click here to

Authentication methods are the ways your users sign into Azure AD and perform SSPR.

Usable authentication methods

Authentication method
No usable methods.

Add authentication method

Choose method: Temporary Access Pass

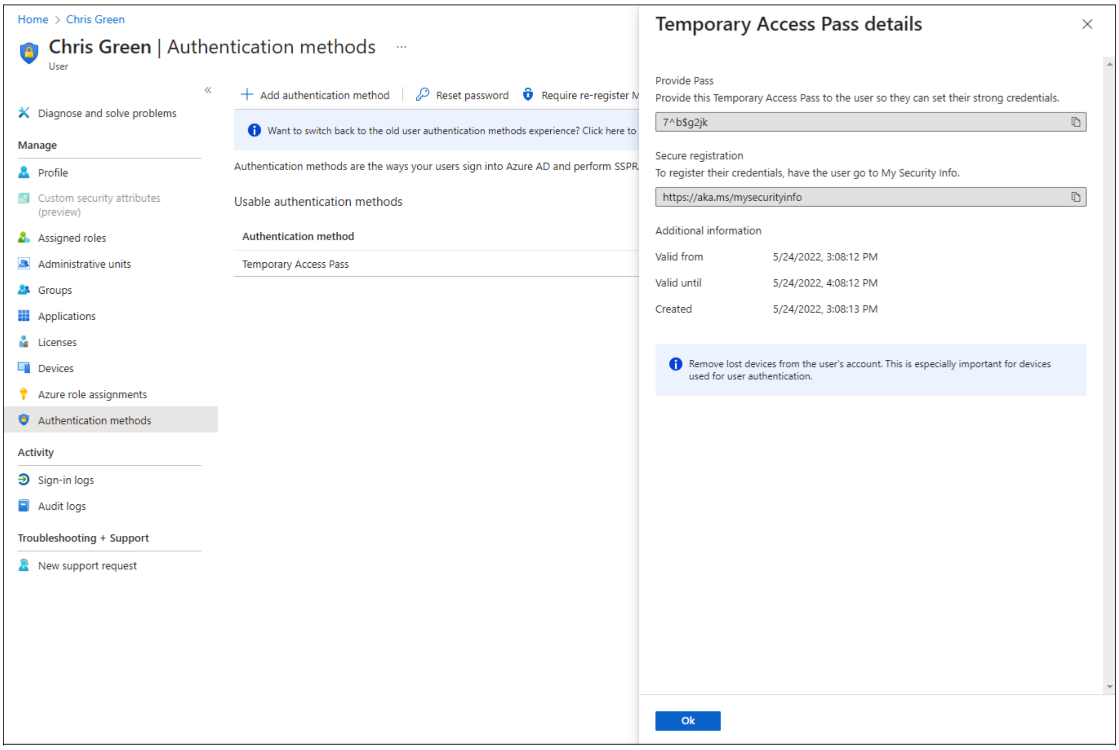
Create a Temporary Access Pass for Chris Green. While the pass is valid, the user can use it to sign in and register strong credentials. Learn more

□ Delayed start time

Activation duration ⓘ 1 hours

One-time use: Yes [✓ No]

7. Once added, the details of the Temporary Access Pass are shown. Make a note of the actual Temporary Access Pass value. You provide this value to the user. You can't view this value after you select Ok.



Want to switch back to the old user authentication methods experience? Click here to

Authentication methods are the ways your users sign into Azure AD and perform SSPR.

Usable authentication methods

Authentication method
Temporary Access Pass

Temporary Access Pass details

Provide Pass

Provide this Temporary Access Pass to the user so they can set their strong credentials.

7^b$g2jk

Secure registration

To register their credentials, have the user go to My Security Info.

https://aka.ms/mysecurityinfo

Additional information

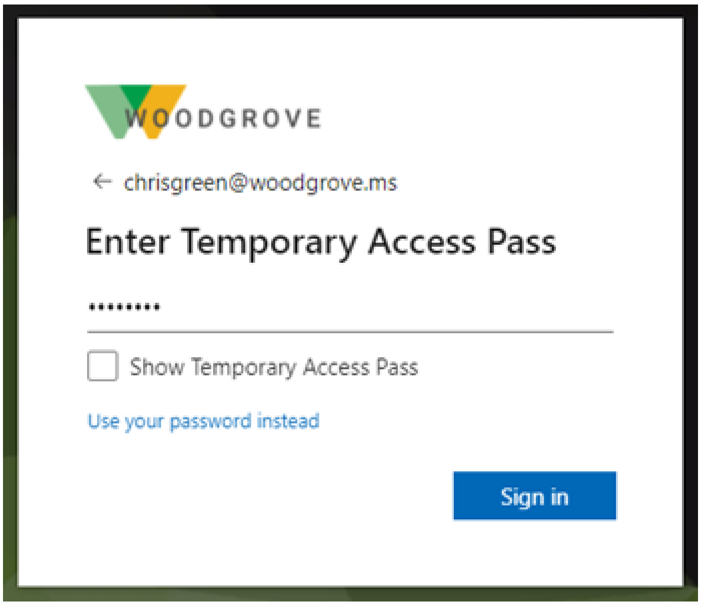
Valid from	5/24/2022, 3:08:12 PM
Valid until	5/24/2022, 4:08:12 PM
Created	5/24/2022, 3:08:13 PM

Remove lost devices from the user's account. This is especially important for devices used for user authentication.

Use a Temporary Access Pass

The most common use for a Temporary Access Pass is for a user to register authentication details during the first sign-in or device setup, without the need to complete extra security prompts. Authentication methods are registered at ***https://aka.ms/mysecurityinfo***. Users can also update existing authentication methods here.

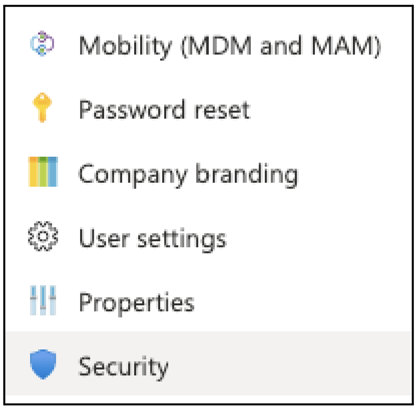
1. Open a web browser to https://aka.ms/mysecurityinfo
2. Enter the UPN of the account you created the Temporary Access Pass for, such as tapuser@contoso.com.
3. If the user is included in the Temporary Access Pass policy, they'll see a screen to enter their Temporary Access Pass.
4. Enter the Temporary Access Pass that was displayed in the Azure portal.


WOODGROVE
← chrisgreen@woodgrove.ms
Enter Temporary Access Pass
••••••••
□ Show Temporary Access Pass
Use your password instead
Sign in

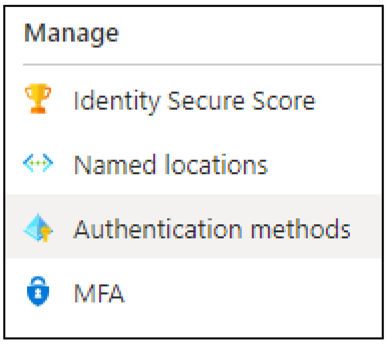
The user is now signed in and can update or register a method such as FIDO2 security key (i.e. YubiKey). Users who update their authentication methods due to losing their credentials or device should make sure they remove the old authentication methods. Users can also continue to sign-in by using their password; a TAP doesn't replace a user's password.

Enabling FIDO2 Security Keys

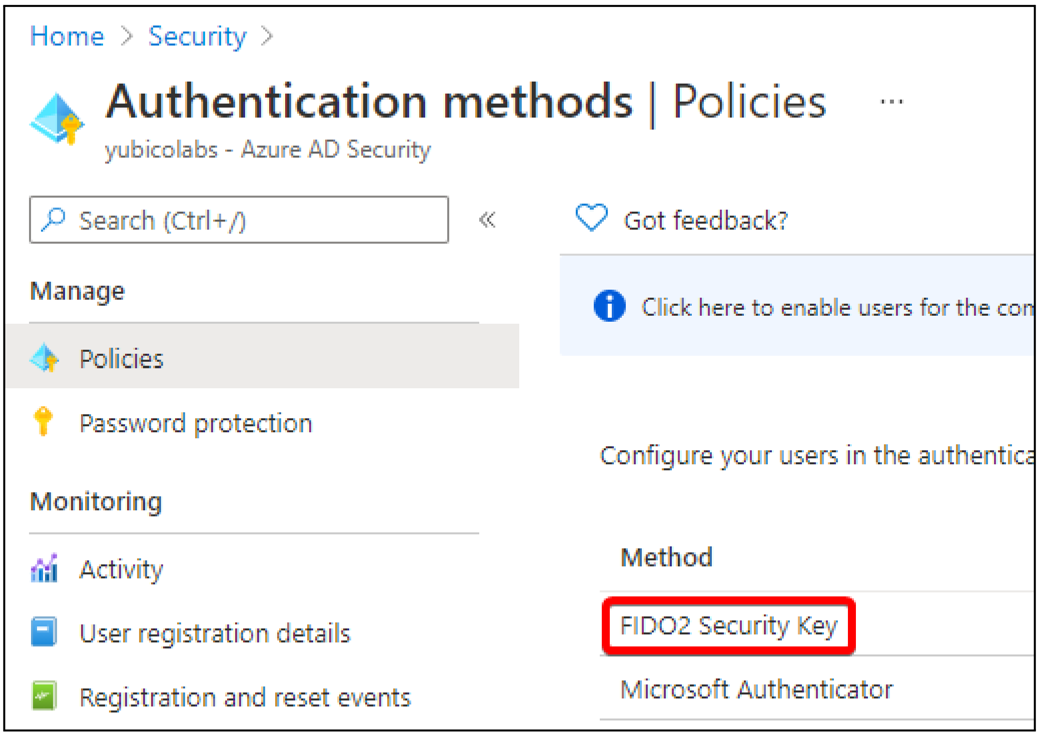
1. From the Azure portal, navigate to **Azure Active Directory.**
2. Navigate to **Security.**



3. Under **Manage**, select **Authentication Methods.**



4. If not auto-directed, navigate to **Authentication method policy** from the left hand menu.
5. From the **Authentication method policy** section, click **FIDO2 Security Keys** under methods.



Click here to enable users for the con

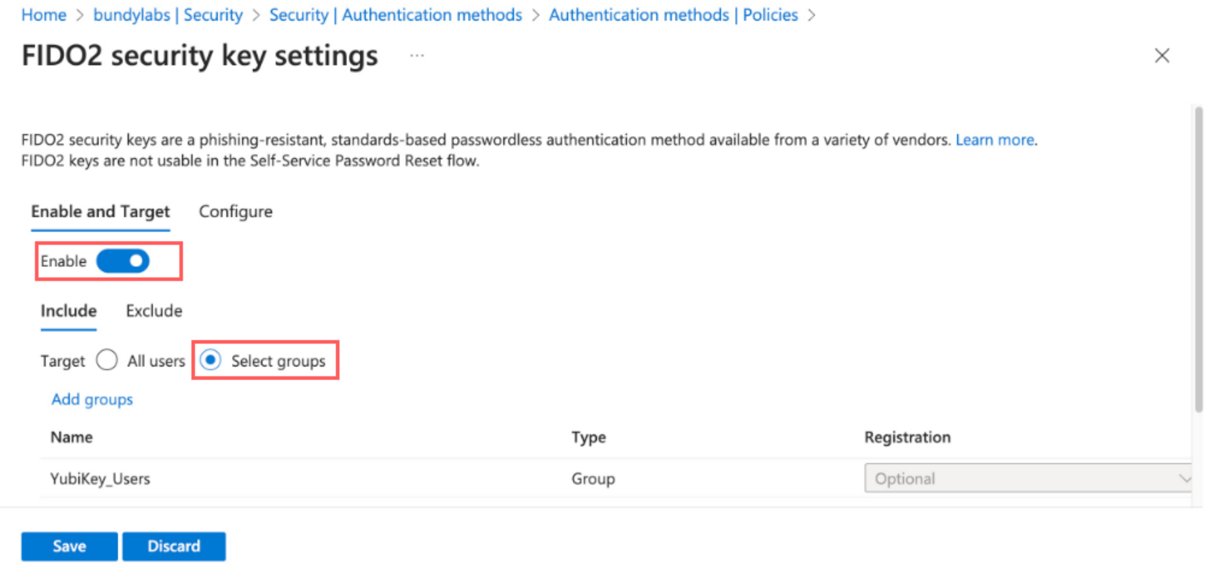
Configure your users in the authentica

6. In the **FIDO2 Security Key settings** section:

a. Under **Enable and Target,** toggle **Enable**.
b. Under **Include,** select either **All Users** or **Select users.**

> *Note:* Yubico recommends only enabling this feature for a select group of test users.

c. Under General, the following configurations are optional:
   - i. Allow self-service set up
     1. Recommended configuration: **Yes**
   - ii. Enforce attestation
     1. Recommended configuration: **No**
   - iii. Enforce key restrictions
     1. Recommended configuration: **No**
   - iv. Restrict Specific Keys
     1. Recommended configuration: **Block**
   - v. Add AAGUID (if Restrict Specific Keys are set to *Allow*)
     1. YubiKey specific AAGUIDs can be found here: https://support.yubico.com/hc/en-us/articles/360016648959



Home > bundylabs | Security > Security | Authentication methods > Authentication methods | Policies >

FIDO2 security key settings

FIDO2 security keys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. Learn more.
FIDO2 keys are not usable in the Self-Service Password Reset flow.

Enable and Target | Configure

Enable ●

Include | Exclude

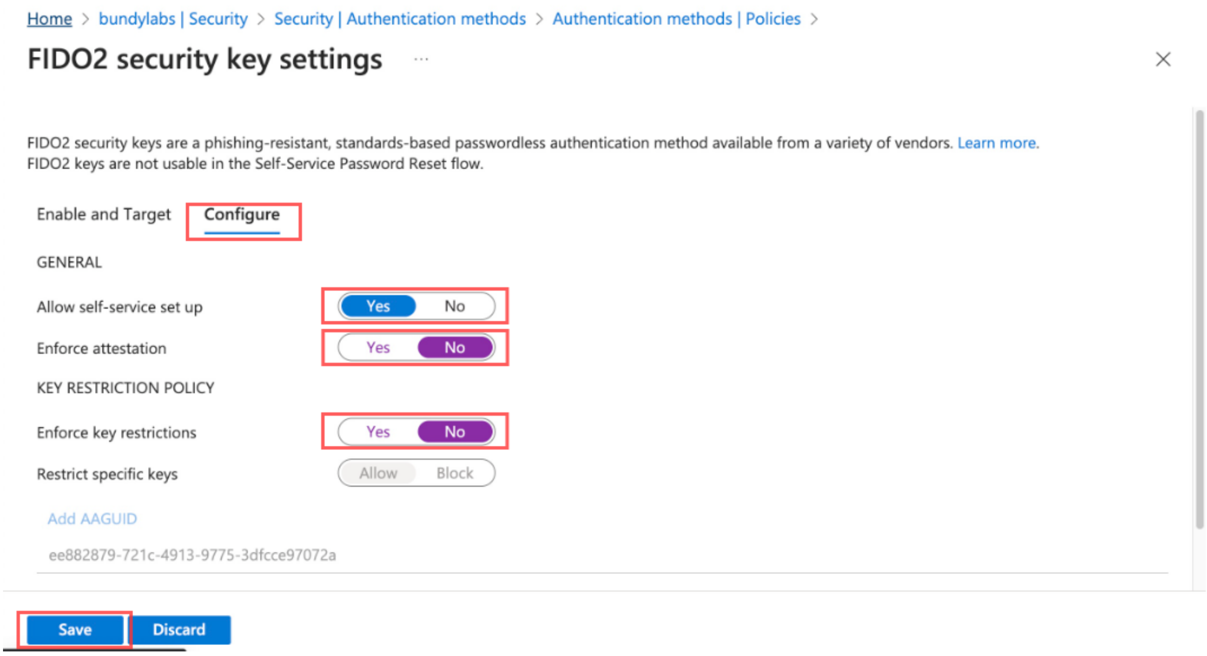
Target ○ All users ● Select groups

Add groups

Name	Type	Registration
YubiKey_Users	Group	Optional

d. Under **Configure**, the following configurations are optional:
   - i. Allow self-service set up
     1. Recommended configuration: **Yes**
   - ii. Enforce attestation
     1. Recommended configuration: **No**
   - iii. Enforce key restrictions
     1. Recommended configuration: **No**
   - iv. Restrict Specific Keys
     1. Recommended configuration: **Block**
   - v. Add AAGUID (if Restrict Specific Keys are set to *Allow*)

1. YubiKey specific AAGUIDs can be found here: https://support.yubico.com/hc/en-us/articles/360016648959



Home > bundylabs | Security > Security | Authentication methods > Authentication methods | Policies >

FIDO2 security key settings ...

FIDO2 security keys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. Learn more.
FIDO2 keys are not usable in the Self-Service Password Reset flow.

Enable and Target | Configure

GENERAL

Allow self-service set up: [✓ Yes] No

Enforce attestation: Yes [✓ No]

KEY RESTRICTION POLICY

Enforce key restrictions: Yes [✓ No]

Restrict specific keys: Allow Block

Add AAGUID

ee882879-721c-4913-9775-3dfcce97072a

7. Click **Save**

Users can now register and use YubiKeys for passwordless authentication. For end user instructions, please see the **YubiKeys for Azure AD Passwordless User Enablement Guide** companion doc, available via https://support.yubico.com/hc/en-us/articles/360016913619.

Enabling passwordless (FIDO2) security key sign-in into on-premises resources (AAD joined or AAD hybrid joined)

This section outlines the administrative steps to enable passwordless single-sign on to on-premise resources from Azure AD joined or hybrid Azure AD joined Windows 10 machines. This requires Azure AD Connect to be installed and configured joining an on-premise AD to AAD. Additionally, the steps in the previous section must be completed (enabling FIDO2 in Azure AD).

Create a Kerberos server object in your Azure AD tenant

1. Login to the Windows Server with Azure AD Connect running with an enterprise administrator account.
2. Run Powershell as an administrator.
3. Within Powershell, navigate to C:\Program Files\Microsoft Azure Active Directory Connect\AzureADKerberos\

   Example Command:

   ```
   cd “C:\Program Files\Microsoft Azure Active Directory Connect\AzureADKerberos\”
   ```

4. Run the following PowerShell command to create a new Azure AD Kerberos server object in both your on-premises Active Directory domain and Azure Active Directory tenant.

> *Note: Replace **contoso.corp.com** in the following example with your on-premises Active Directory domain name.*

```
Import-Module ".\AzureAdKerberos.psd1"

# Specify the on-premises Active Directory domain. A new Azure AD
# Kerberos Server object will be created in this Active Directory domain.
$domain = "contoso.corp.com"

# Enter in the Azure Active Directory global administrator username and password.
$cloudCred = Get-Credential

# Enter in the domain administrator username and password.
$domainCred = Get-Credential

# Create the new Azure AD Kerberos Server object in Active Directory
# and then publish it to Azure Active Directory.
Set-AzureADKerberosServer -Domain $domain -CloudCredential
$cloudCred -DomainCredential $domainCred
```

Viewing and verifying the Azure AD Kerberos Server

1. Run Powershell as an administrator.
2. Execute the following PowerShell command to view and verify the newly created Azure AD Kerberos server

```
Get-AzureADKerberosServer -Domain $domain -CloudCredential $cloudCred
-DomainCredential $domainCred
```

This command outputs the properties of the Azure AD Kerberos Server. Review the properties to validate the properties accurately match the environment.

Enabling passwordless (FIDO2) security key sign-in into Windows 10 machines

This section outlines how to enable passwordless (FIDO2) security key sign-in into Windows 10 machines in either a Azure-only or Hybrid environment. You must first enable FIDO2 in Azure AD first as described in the previous sections. There are three methods that can be used to enable the FIDO2 security key sign-in option on the Windows 10 lock screen.

- Create and apply a provisioning package to a Windows 10 device
- Use Intune
- Use Group Policy

While this document outlines each of these options, only one option is required. Yubico recommends choosing the option that aligns with the organization’s current processes to manage devices.

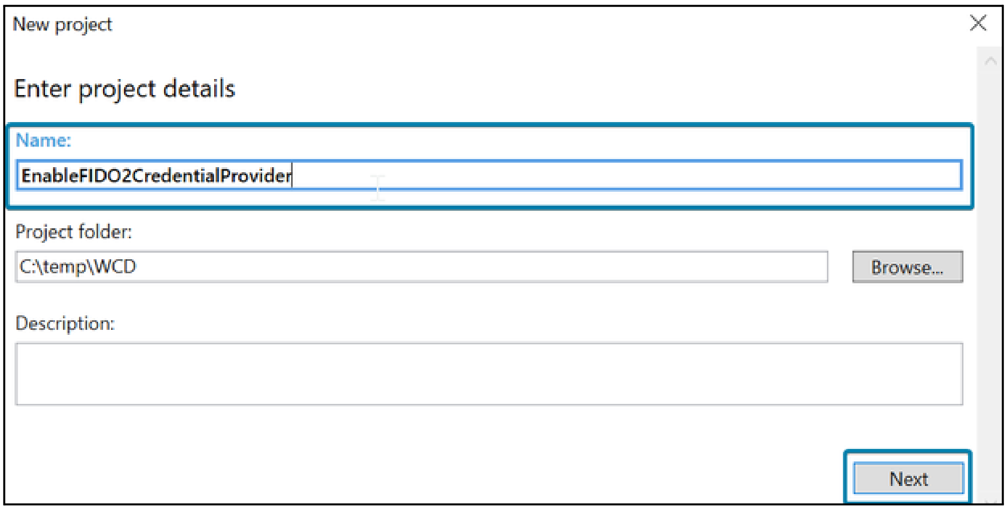
Option 1. Using a Provisioning package method

A provisioning package can be installed on the Windows 10 device to enable the FIDO2 security key sign-in option.

Create a provisioning package

The Windows Configuration Designer app can be installed from the Microsoft Store. Complete the following steps to create a provisioning package:

1. Launch the Windows Configuration Designer.
2. Select **File > New project**.
3. Give your project a name and take note of the path where your project is created, then select **Next**.


New project

Enter project details

Name:

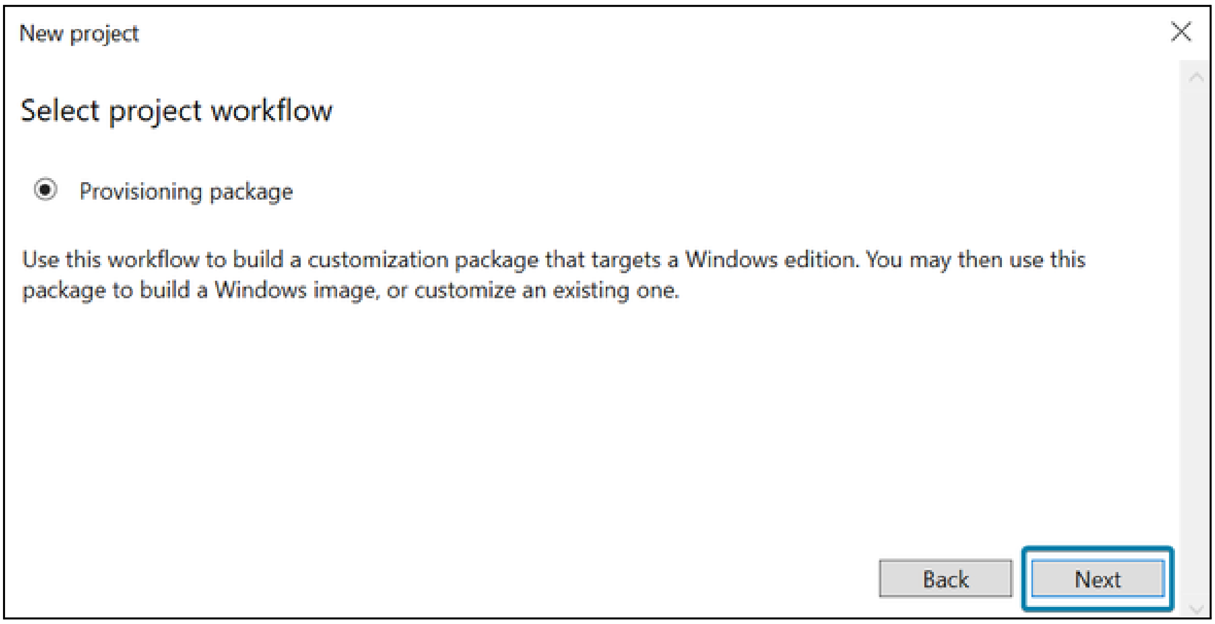
EnableFIDO2CredentialProvider

Project folder:

C:\temp\WCD

Description:

4. Leave **Provisioning package** selected as the Selected project workflow and select **Next**.


New project

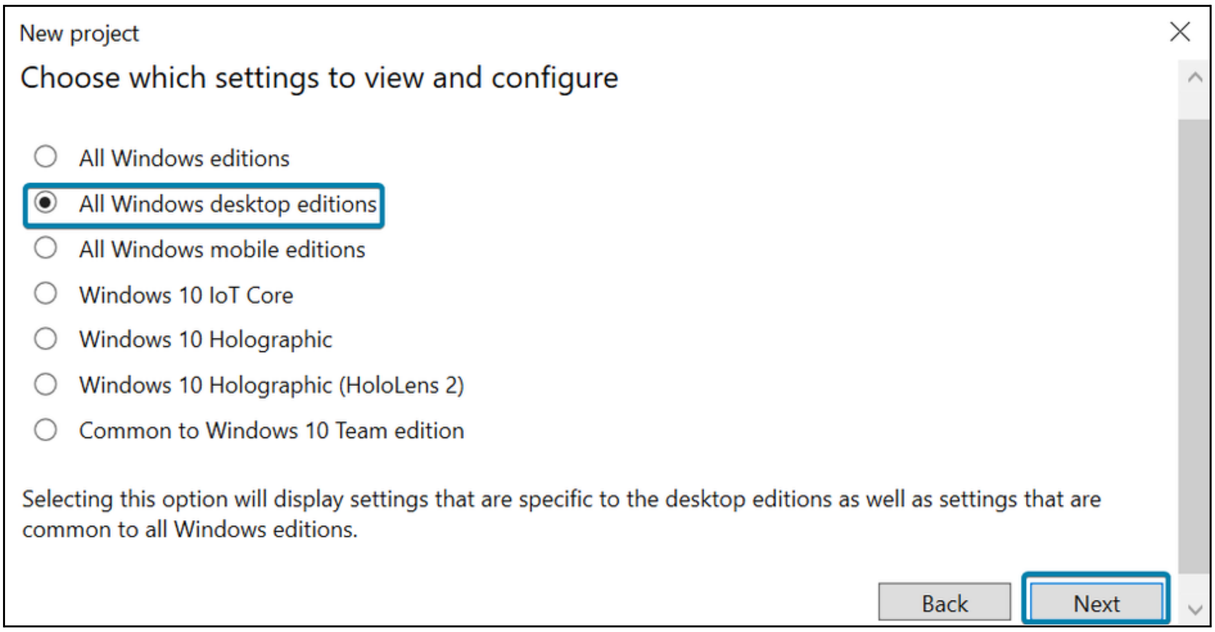
Select project workflow

● Provisioning package

Use this workflow to build a customization package that targets a Windows edition. You may then use this package to build a Windows image, or customize an existing one.

5. Select **All Windows desktop editions** under Choose which settings to view and configure, then select **Next**.

   Please verify that you selected ‘All Windows desktop editions’, or the following menus may not provide the correct options.



New project

Choose which settings to view and configure

○ All Windows editions

● All Windows desktop editions

○ All Windows mobile editions

○ Windows 10 IoT Core

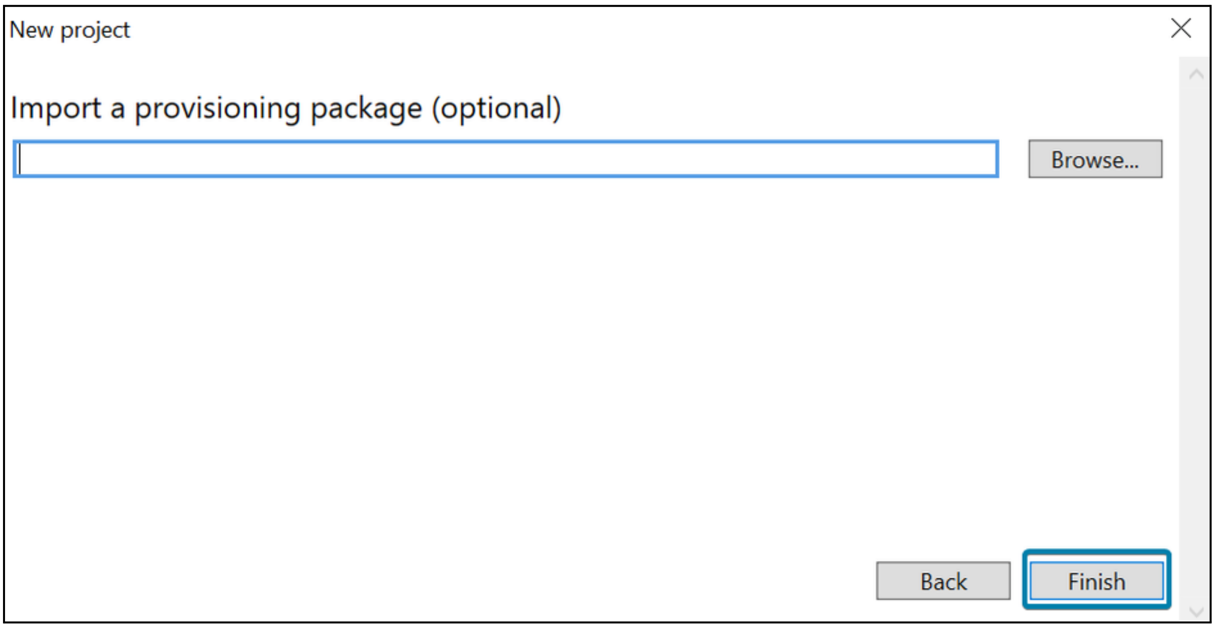
○ Windows 10 Holographic

○ Windows 10 Holographic (HoloLens 2)

○ Common to Windows 10 Team edition

Selecting this option will display settings that are specific to the desktop editions as well as settings that are common to all Windows editions.

6. Select **Finish**.

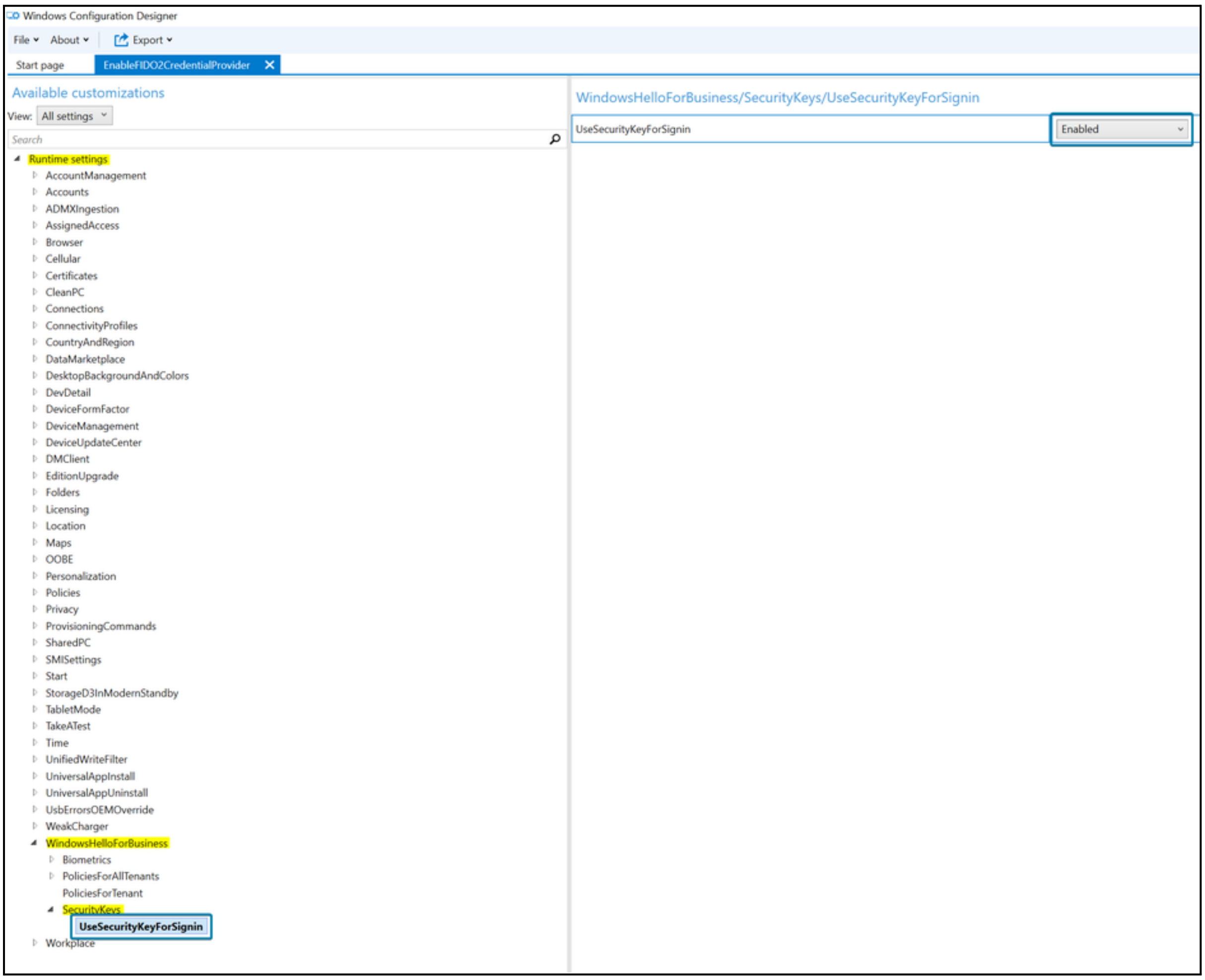


New project

Import a provisioning package (optional)

7. In your newly created project, in the left panel, browse to: **Runtime settings** > **WindowsHelloForBusiness** > **SecurityKeys** > **UseSecurityKeyForSignIn**.

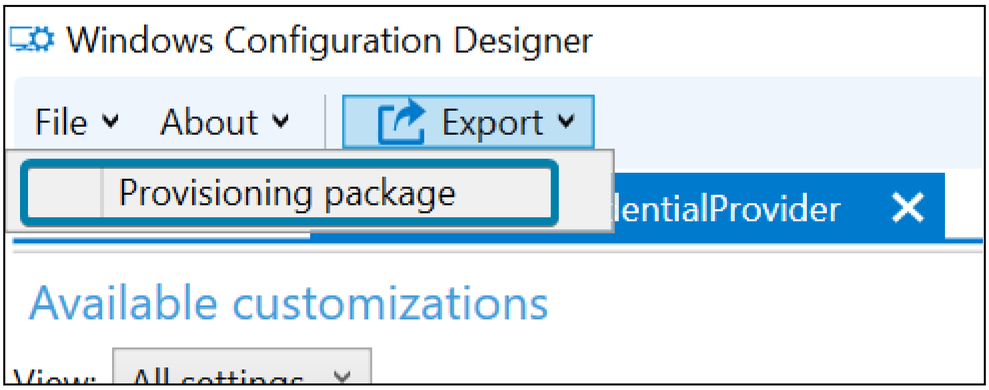
   In the middle panel, change the **UseSecurityKeyForSignIn** to **Enabled**.



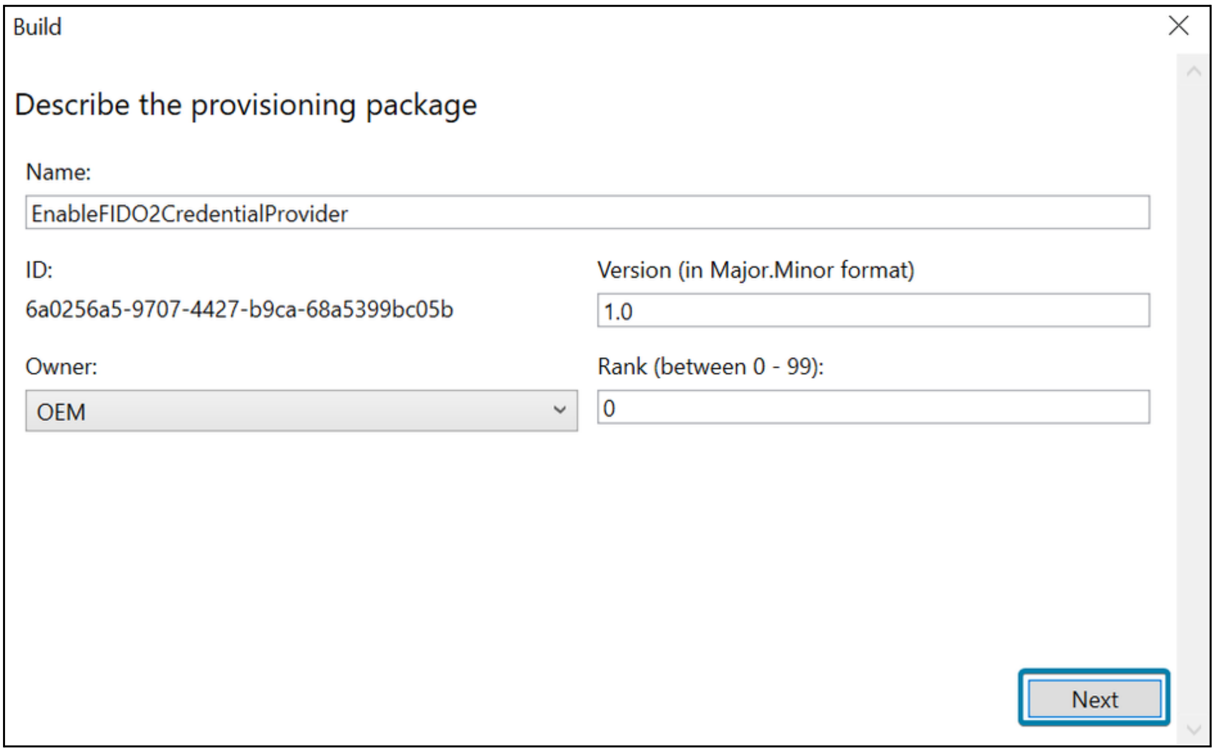
WindowsHelloForBusiness/SecurityKeys/UseSecurityKeyForSignin

UseSecurityKeyForSignin: Enabled

8. In the top left menus of the Configuration Designer, select **Export** > **Provisioning package**.



9. Leave the defaults in the **Build** window under **Describe the provisioning package**, then select **Next**.



Build

Describe the provisioning package

Name: EnableFIDO2CredentialProvider

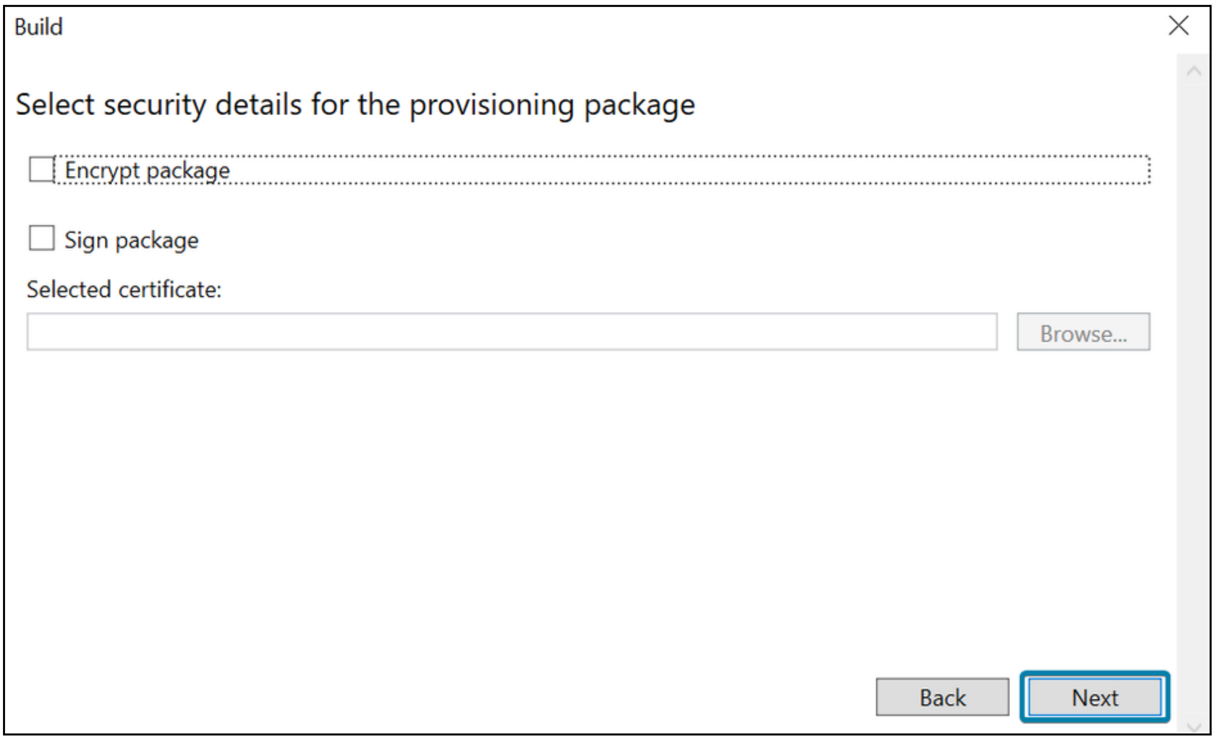
ID: 6a0256a5-9707-4427-b9ca-68a5399bc05b

Version (in Major.Minor format): 1.0

Owner: OEM

Rank (between 0 - 99): 0

10. Leave the defaults in the **Build** window under **Select security details for the provisioning package** and select **Next**.



Build

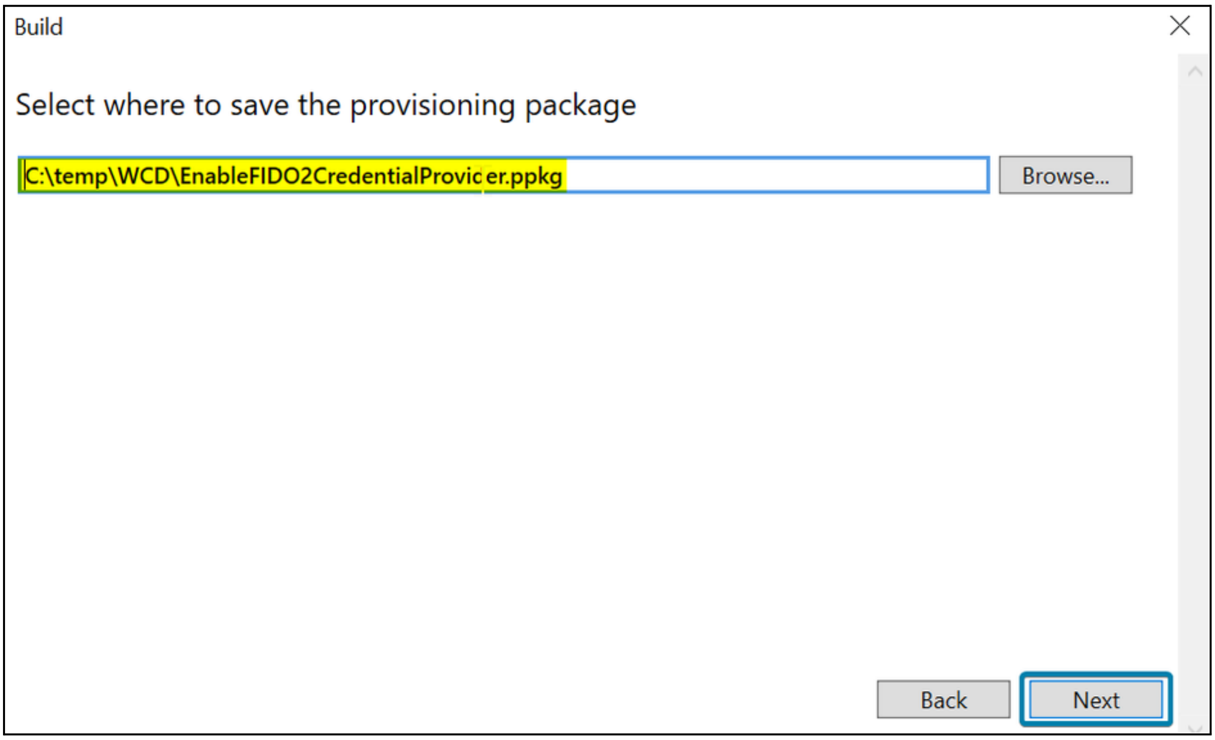
Select security details for the provisioning package

□ Encrypt package

□ Sign package

Selected certificate:

11. Take note of or change the path in the **Build** windows under **Select where to save the provisioning package** and select **Next**.

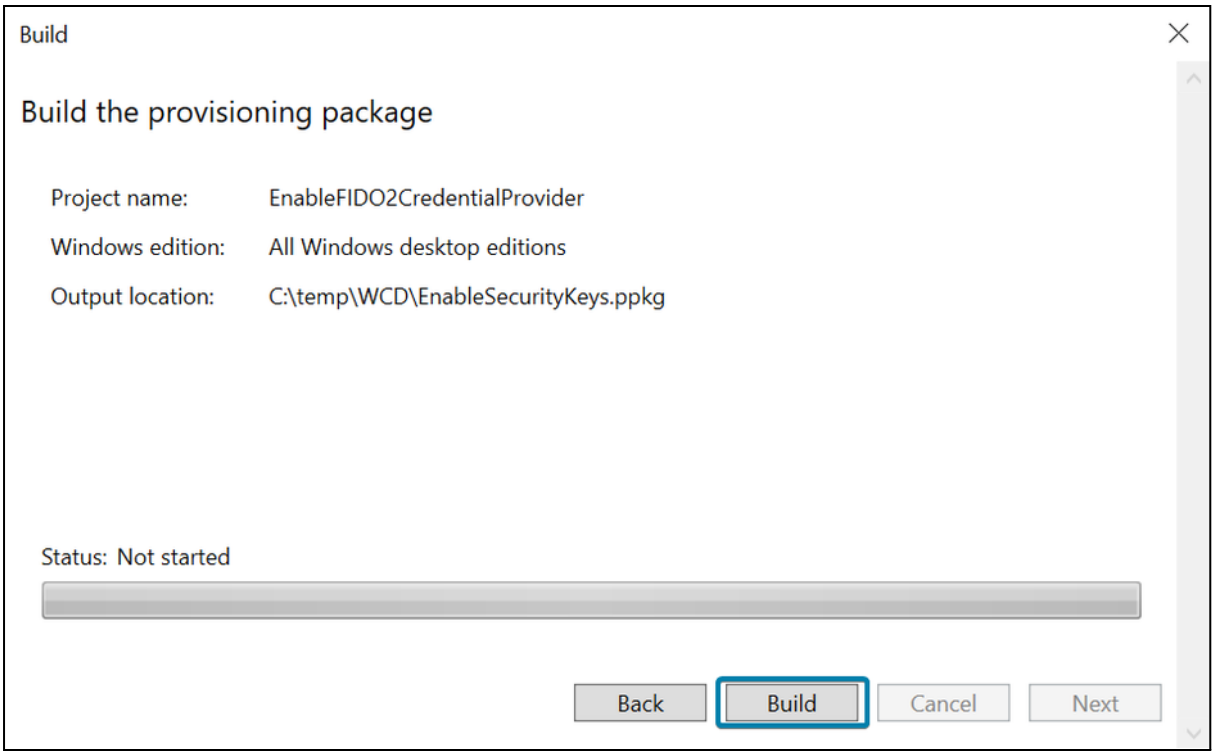


Build

Select where to save the provisioning package

C:\temp\WCD\EnableFIDO2CredentialProvider.ppkg

12. Select **Build** on the **Build the provisioning package** page.



Build

Build the provisioning package

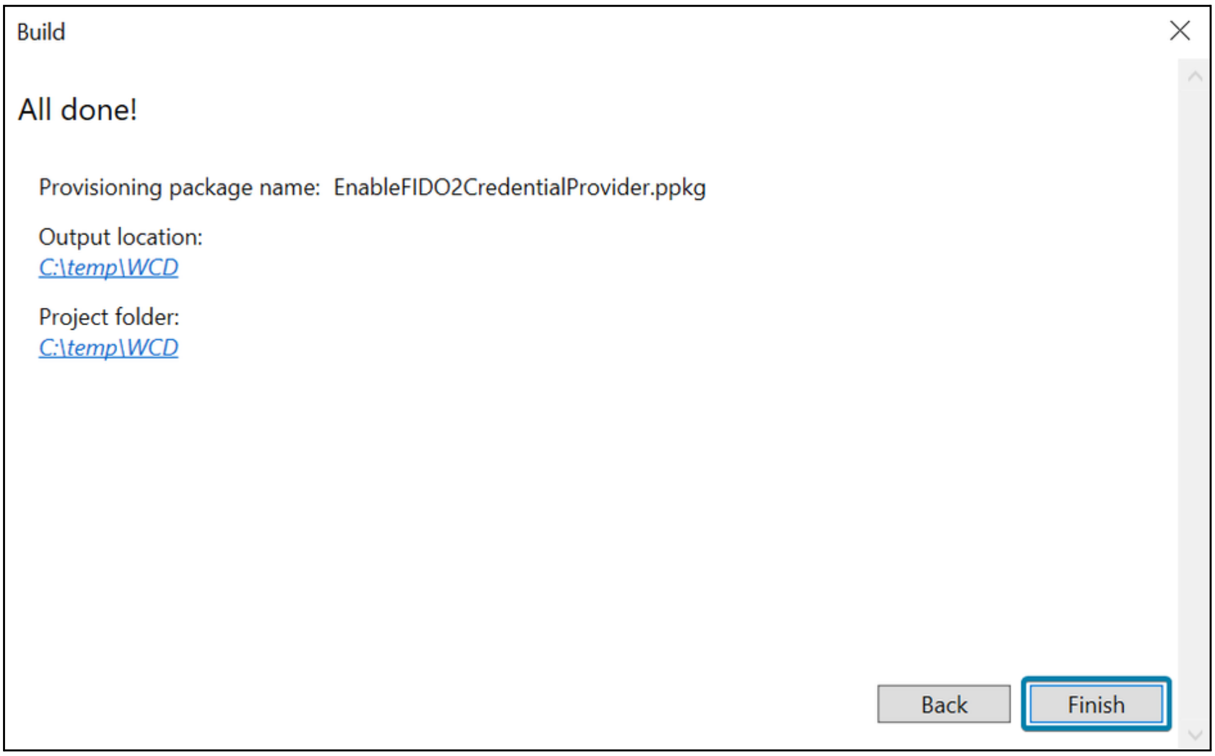
Project name: EnableFIDO2CredentialProvider

Windows edition: All Windows desktop editions

Output location: C:\temp\WCD\EnableSecurityKeys.ppkg

Status: Not started

13. Select **Finish**.



Build

All done!

Provisioning package name: EnableFIDO2CredentialProvider.ppkg

Output location:
C:\temp\WCD

Project folder:
C:\temp\WCD

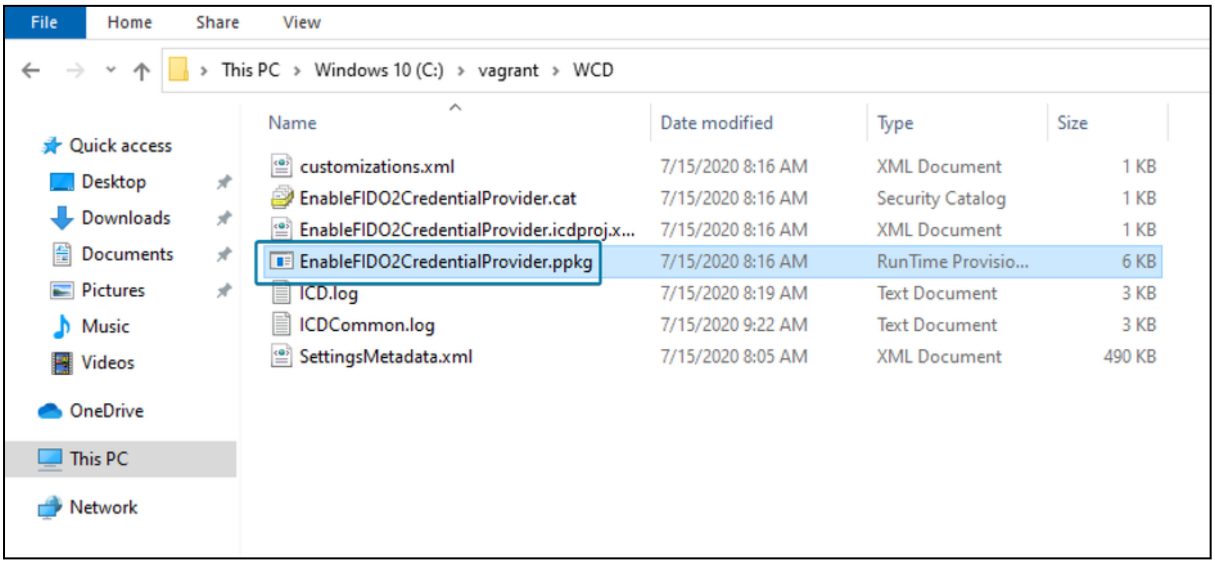
14. Save the two files created (.ppkg and .cat) to a location where you can apply them to machines later.

Apply a provisioning package

Notes

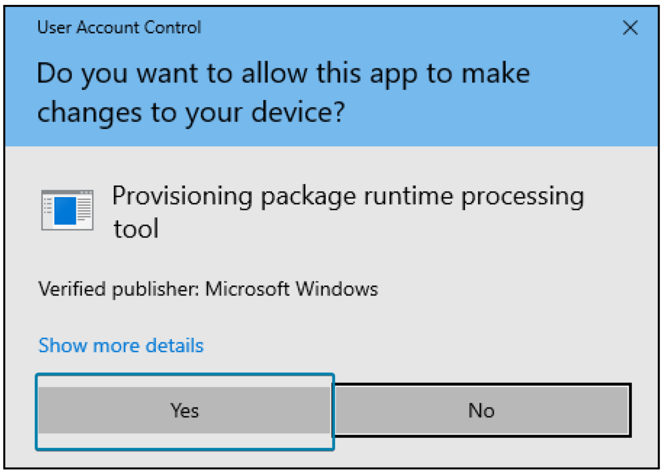
1. *Applying a provisioning package to a desktop device requires administrator privileges on the device.*
2. *Microsoft provides multiple methods to apply a provisioning package. The following steps show only one of the available methods. See the following Microsoft page for alternate methods for applying a provisioning package.* *https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package*

1. Make sure the provisioning package is accessible from the machine that you will apply the provisioning package to.
2. Locate the provisioning package and double-click the file with the **.ppkg** extension.



Name	Date modified	Type	Size
customizations.xml	7/15/2020 8:16 AM	XML Document	1 KB
EnableFIDO2CredentialProvider.cat	7/15/2020 8:16 AM	Security Catalog	1 KB
EnableFIDO2CredentialProvider.icdproj.x...	7/15/2020 8:16 AM	XML Document	1 KB
EnableFIDO2CredentialProvider.ppkg	7/15/2020 8:16 AM	RunTime Provisio...	6 KB
ICD.log	7/15/2020 8:19 AM	Text Document	3 KB
ICDCommon.log	7/15/2020 9:22 AM	Text Document	3 KB
SettingsMetadata.xml	7/15/2020 8:05 AM	XML Document	490 KB

3. Select **Yes** to allow the app to make changes.



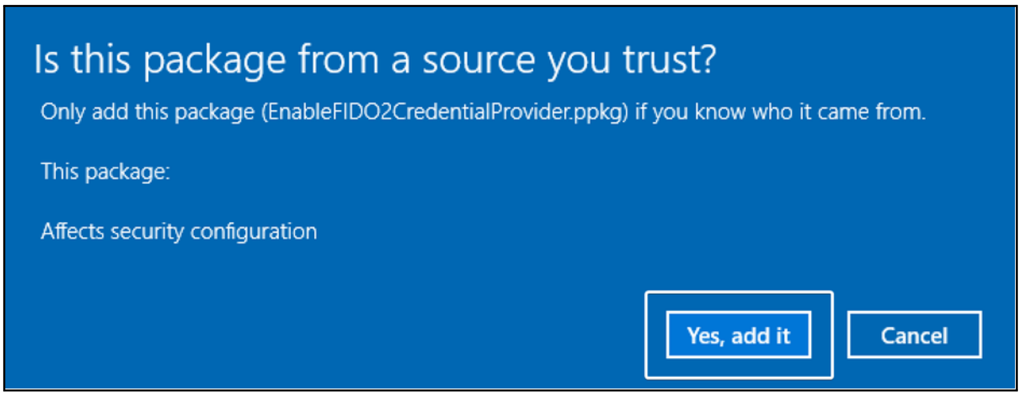
User Account Control

Do you want to allow this app to make changes to your device?

Provisioning package runtime processing tool

Verified publisher: Microsoft Windows

4. If you trust the package, select **Yes, add it**.



Is this package from a source you trust?

Only add this package (EnableFIDO2CredentialProvider.ppkg) if you know who it came from.

This package:

Affects security configuration

5. The changes are immediately applied without any other visual cues to the user.
6. Sign out.

7. The lock screen on the Windows 10 device should now be enabled with a security key option. See “User Experience: Lock screen enabled” section for expected results.

Option 2: Intune method

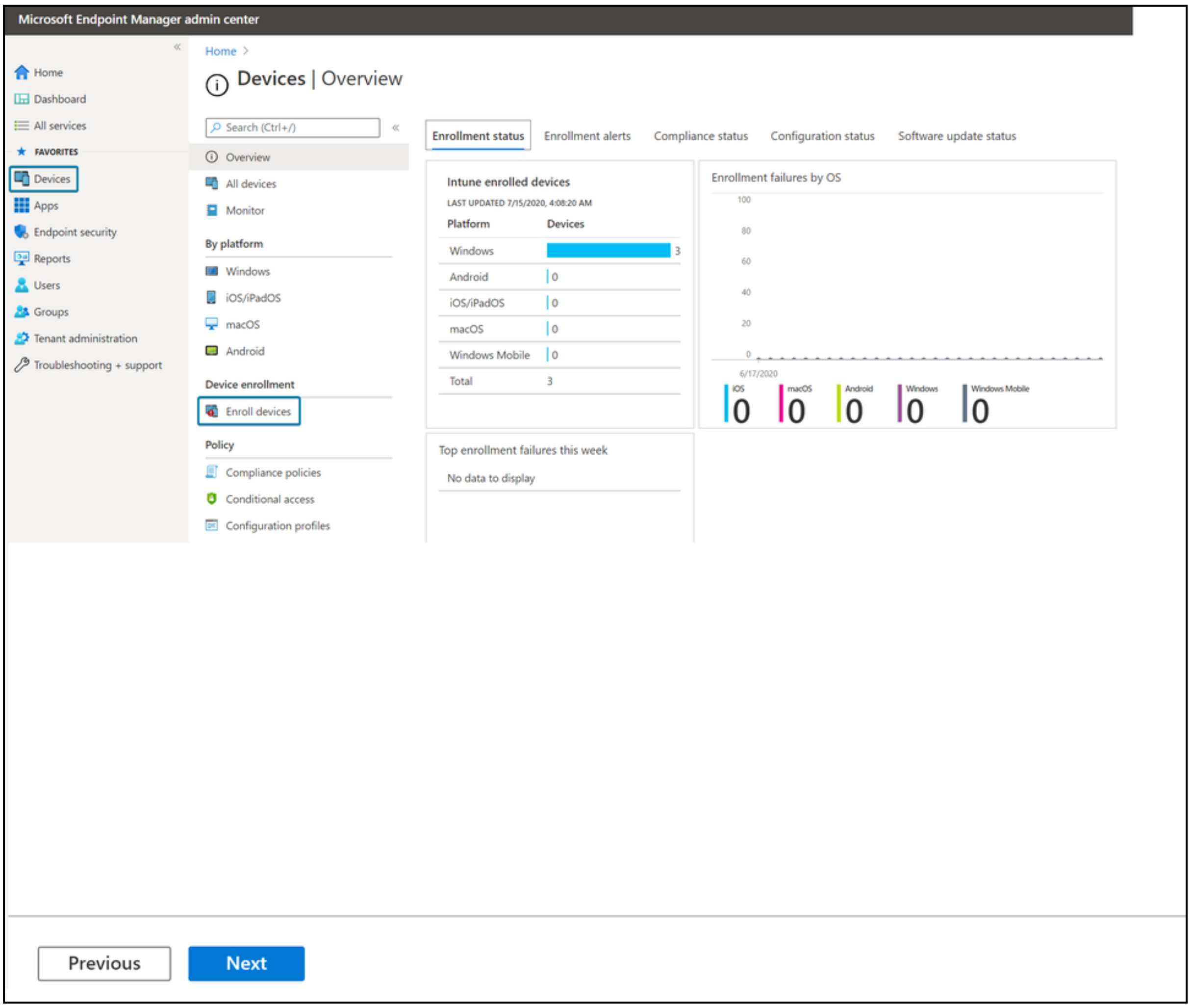
Intune provides multiple options for enabling the lock screen to use security keys on Windows 10 devices. Two different methods are described below. One method will describe how to enable the setting for all users' devices, and the other method will describe how to apply the setting for targeted groups.

Option 2a: All users and devices

To enable the use of security keys using Intune for all of your organization's Windows devices, complete the following steps:

1. Sign into the Intune portal at https://intune.microsoft.com

2. Browse to **Devices** > **Enroll devices.**



Intune enrolled devices

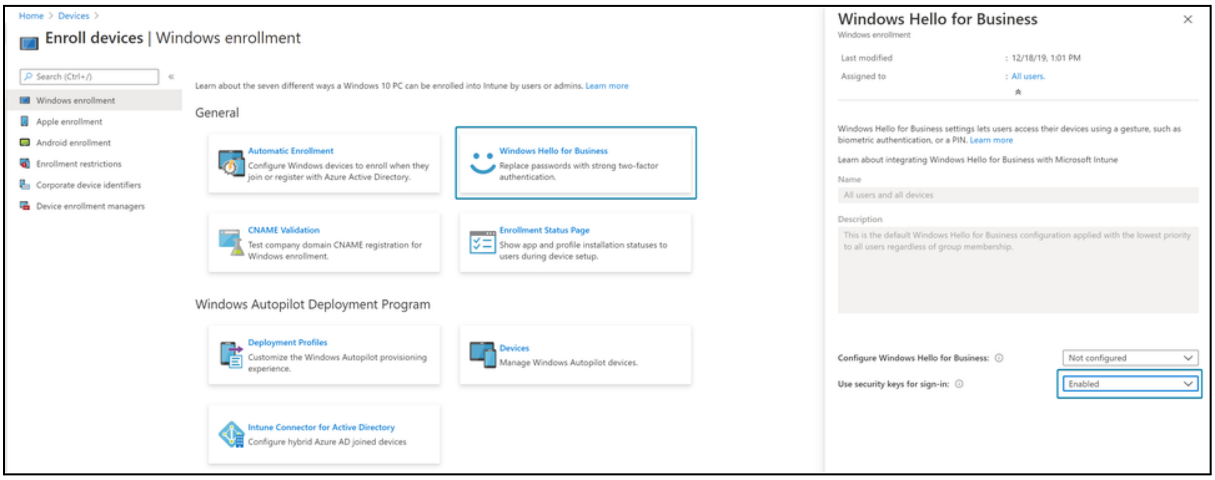
LAST UPDATED 7/15/2020, 4:08:20 AM

Platform	Devices
Windows	3
Android	0
iOS/iPadOS	0
macOS	0
Windows Mobile	0
Total	3

Top enrollment failures this week

No data to display

3. Browse to **Windows Hello for Business** and change the setting for **Use security keys for sign-in** to **Enabled**.



Learn about the seven different ways a Windows 10 PC can be enrolled into Intune by users or admins. Learn more

Automatic Enrollment: Configure Windows devices to enroll when they join or register with Azure Active Directory.

Windows Hello for Business: Replace passwords with strong two-factor authentication.

CNAME Validation: Test company domain CNAME registration for Windows enrollment.

Enrollment Status Page: Show app and profile installation statuses to users during device setup.

Deployment Profiles: Customize the Windows Autopilot provisioning experience.

Devices: Manage Windows Autopilot devices.

Intune Connector for Active Directory: Configure hybrid Azure AD joined devices

Windows Hello for Business
Windows enrollment

Last modified : 12/18/19, 1:01 PM
Assigned to : All users.

Windows Hello for Business settings lets users access their devices using a gesture, such as biometric authentication, or a PIN. Learn more

Learn about integrating Windows Hello for Business with Microsoft Intune

Name: All users and all devices

Description: This is the default Windows Hello for Business configuration applied with the lowest priority to all users regardless of group membership.

Configure Windows Hello for Business: Not configured

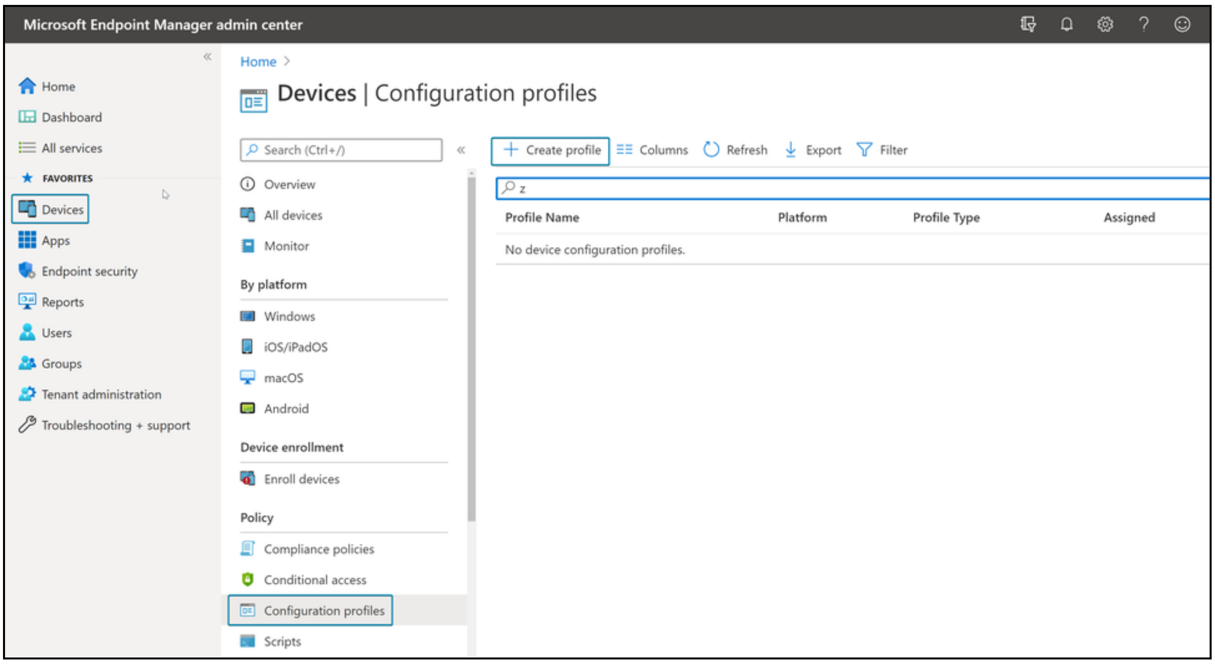
Use security keys for sign-in: Enabled

4. Select **Save**.

Option 2b: Targeted Intune deployment

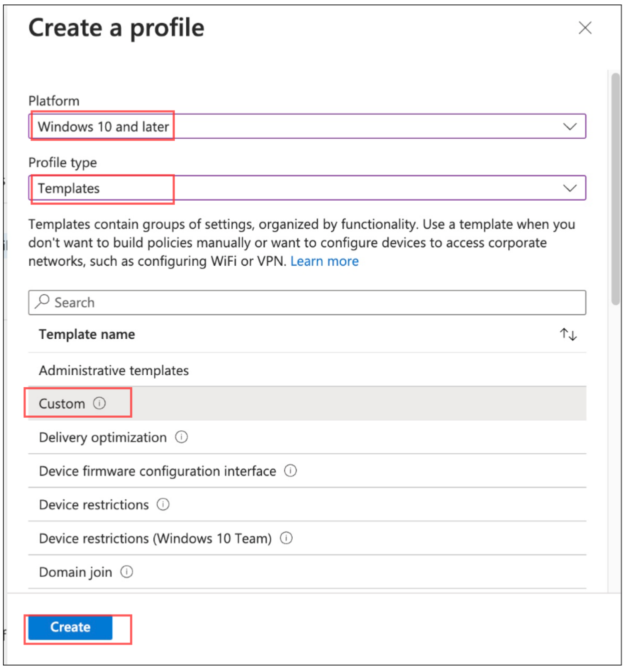
To enable the use of security keys for select user groups and select devices, complete the following steps:

1. Sign in to Intune portal at https://intune.microsoft.com/.
2. Browse to **Devices** > **Configuration profiles** > **Create profile**.



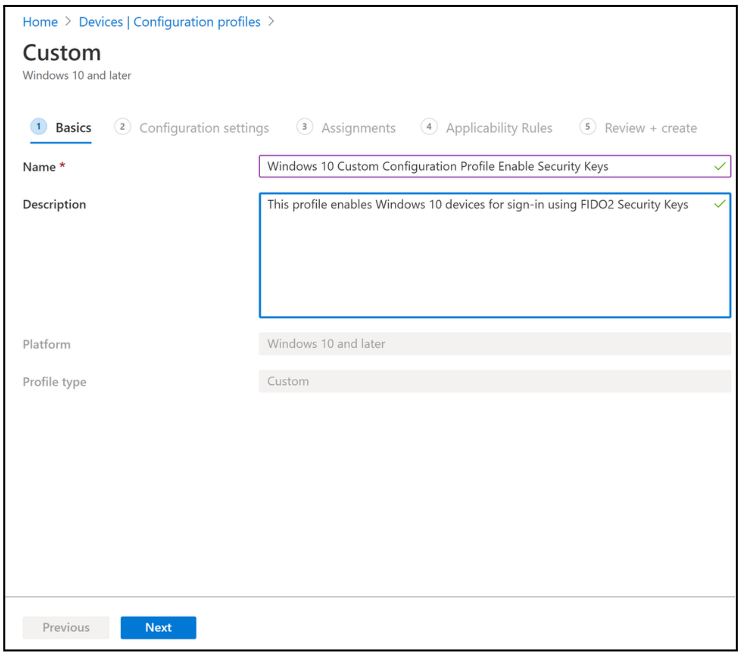
Profile Name	Platform	Profile Type	Assigned
No device configuration profiles.			

3. Set the Platform and Profile options and select **Create**.
   - **Platform**: Windows 10 and later
   - **Profile type**: Templates
   - **Template Name**: Custom



Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

4. Provide the name and description and select **Next**.



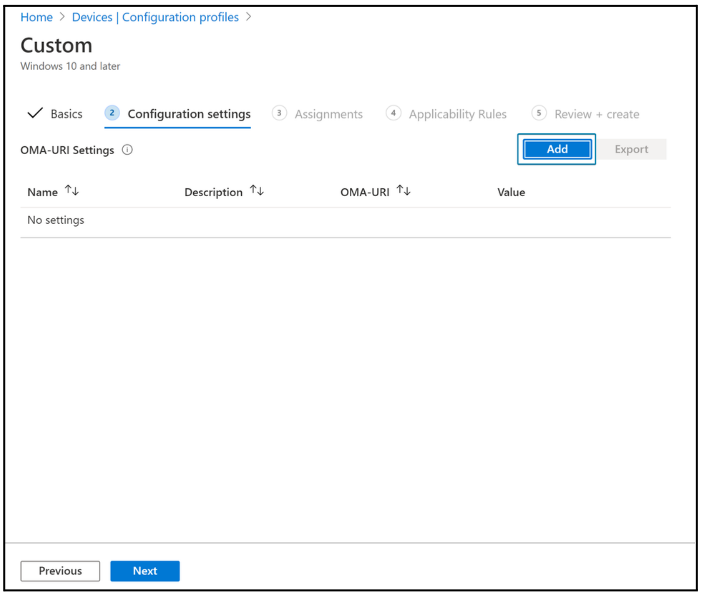
Name * Windows 10 Custom Configuration Profile Enable Security Keys

Description This profile enables Windows 10 devices for sign-in using FIDO2 Security Keys

Platform Windows 10 and later

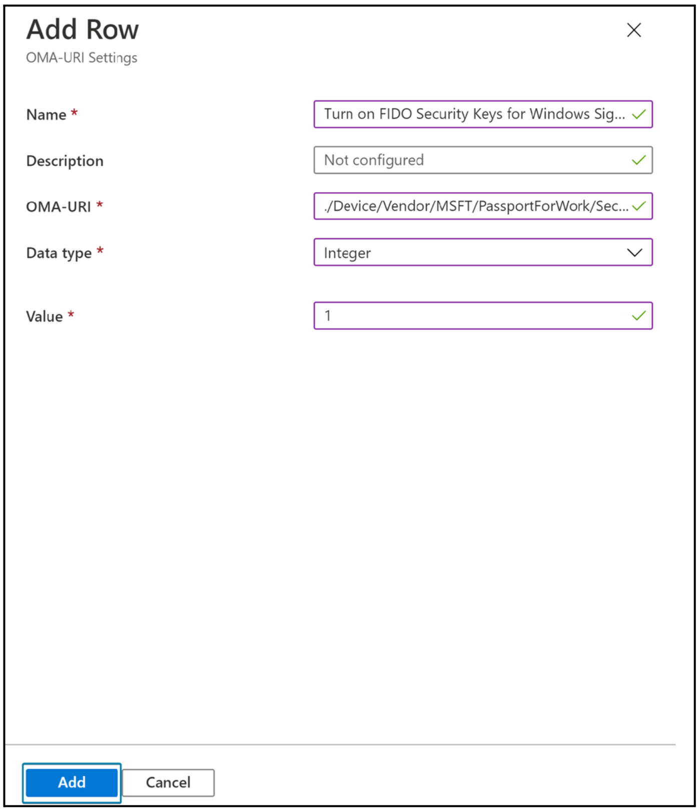
Profile type Custom

5. Under Configuration settings, select **Add**.



Name	Description	OMA-URI	Value
No settings			

6. Set the OMA-URI Settings to the following and then select **Add**.
   - **Name**: Turn on FIDO Security Keys for Windows Sign-In
   - **OMA-URI:** `./Device/Vendor/MSFT/PassportForWork/SecurityKey/UseSecurityKeyForSignin`
   - **Data Type:** Integer
   - **Value**: 1



Name * Turn on FIDO Security Keys for Windows Sig...

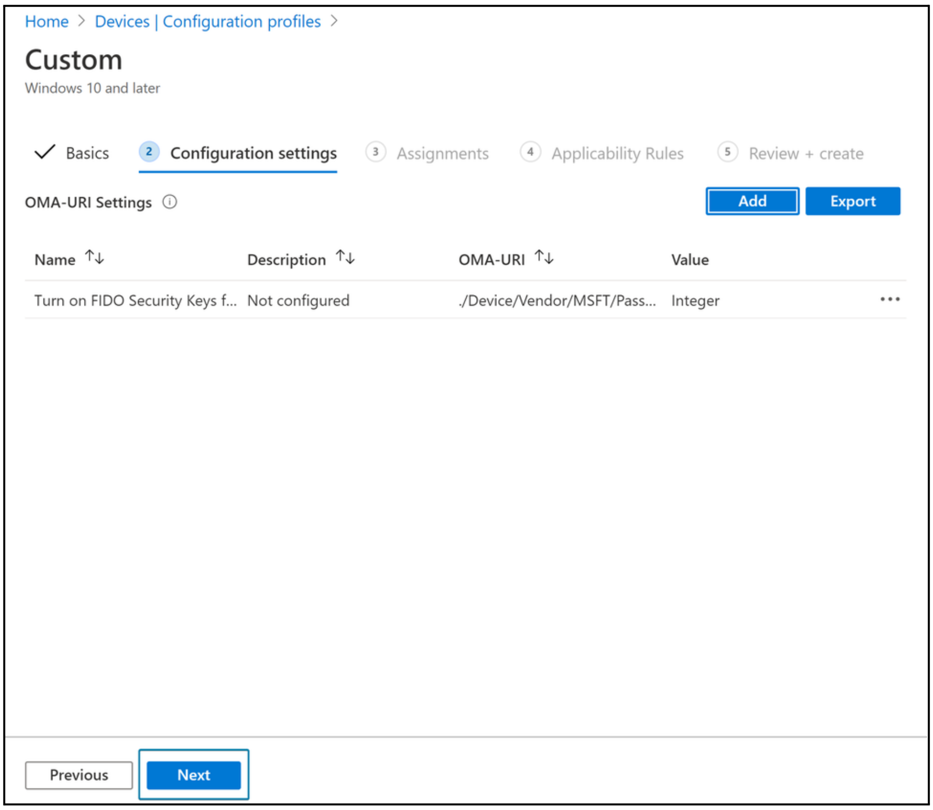
Description Not configured

OMA-URI * ./Device/Vendor/MSFT/PassportForWork/Sec...

Data type * Integer

Value * 1

7. Select **Next**.



Home > Devices | Configuration profiles >

Custom

Windows 10 and later

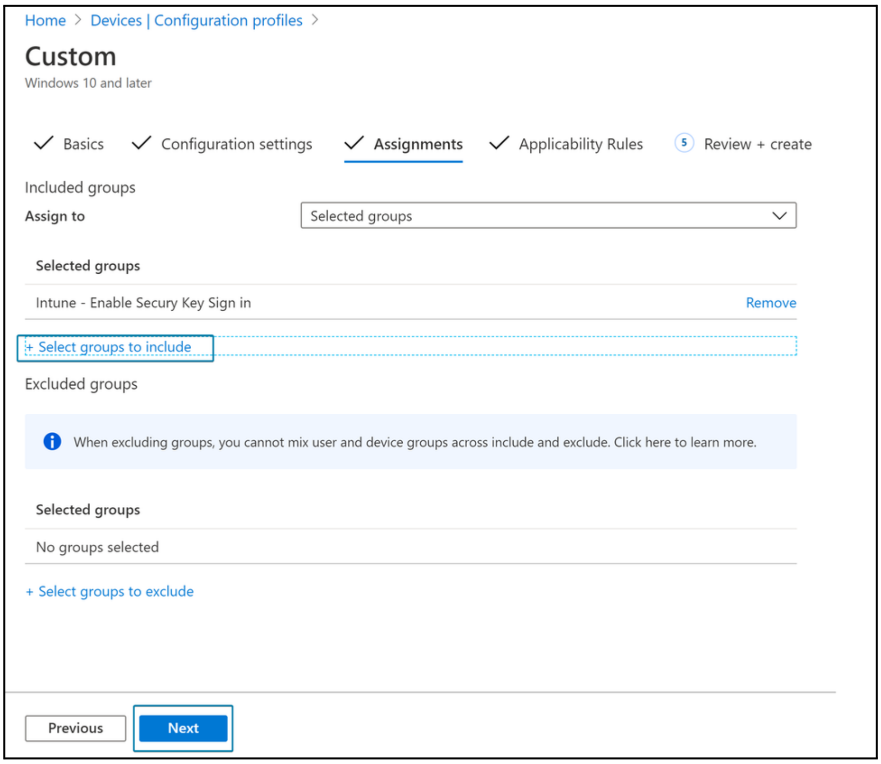
✓ Basics ② Configuration settings ③ Assignments ④ Applicability Rules ⑤ Review + create

OMA-URI Settings ⓘ

Name ↑↓	Description ↑↓	OMA-URI ↑↓	Value
Turn on FIDO Security Keys f...	Not configured	./Device/Vendor/MSFT/Pass...	Integer

8. This policy can be assigned to specific users, devices, or groups. For more information, see Assign user and device profiles in Microsoft Intune.

   Select the groups and devices that this policy will apply to and select **Next**.



Home > Devices | Configuration profiles >

Custom

Windows 10 and later

✓ Basics ✓ Configuration settings ✓ Assignments ✓ Applicability Rules 5 Review + create

Included groups

Assign to: Selected groups

Selected groups

Intune - Enable Secury Key Sign in — Remove

+ Select groups to include

Excluded groups

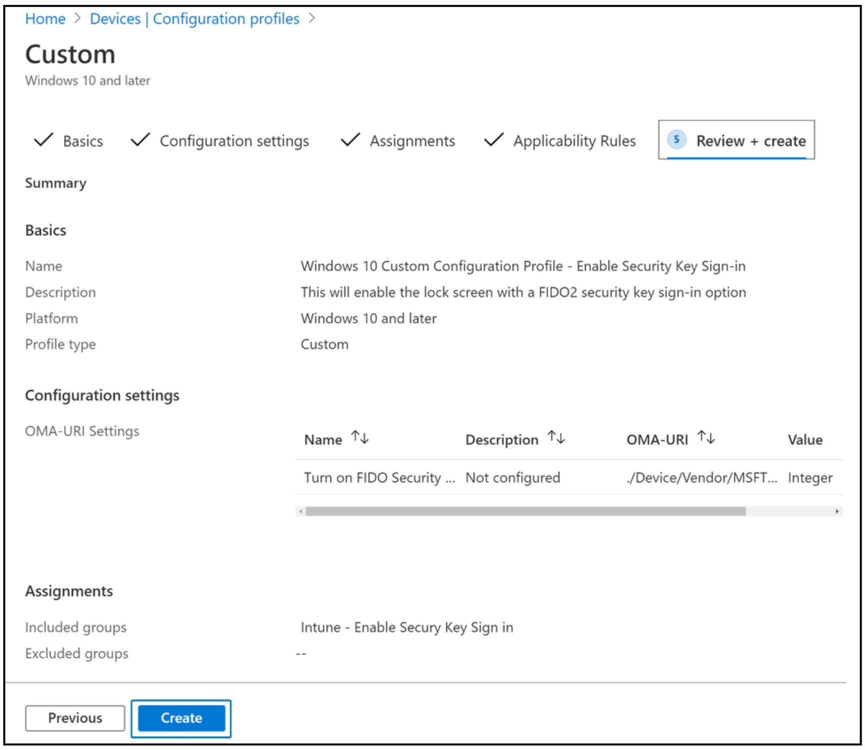
When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.

Selected groups

No groups selected

+ Select groups to exclude

9. Select **Next** under Applicability Rules.
10. Select **Create**.



Home > Devices | Configuration profiles >

Custom

Windows 10 and later

✓ Basics ✓ Configuration settings ✓ Assignments ✓ Applicability Rules 5 Review + create

Summary

Basics

Name: Windows 10 Custom Configuration Profile - Enable Security Key Sign-in

Description: This will enable the lock screen with a FIDO2 security key sign-in option

Platform: Windows 10 and later

Profile type: Custom

Configuration settings

OMA-URI Settings

Name	Description	OMA-URI	Value
Turn on FIDO Security ...	Not configured	./Device/Vendor/MSFT...	Integer

Assignments

Included groups: Intune - Enable Secury Key Sign in

Excluded groups: --

11. The configuration profile should be enabled now for the users and devices that you selected.

12. The profile may not apply immediately to the devices. See the Intune device profile troubleshoot link below for estimated synchronization times.
13. The lock screen on the Windows 10 device will then be enabled with a security key option. See “User Experience: Lock screen enabled” section for expected results.

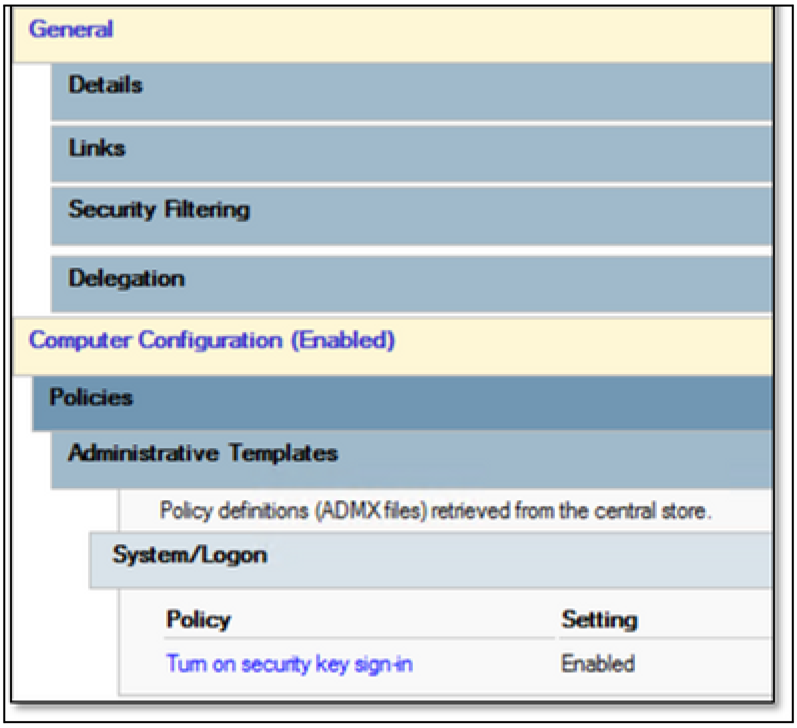
Option 3: Group policy method

For **hybrid Azure AD joined devices** only, organizations can use Group Policies to enable FIDO security key sign-in. This setting can be found under **Computer Configuration** > **Administrative Templates** > **System** > **Logon** > **Turn on security key sign-in**:

- Setting this policy to **Enabled** allows users to sign in with security keys.
- Setting this policy to **Disabled** or **Not Configured** stops users from signing in with security keys.

1. Create a Group Policy Object.
2. Configure the setting:

   Computer Configuration > **Administrative Templates** > **System** > **Logon** > **Turn on security key sign-in**:



General

Details

Links

Security Filtering

Delegation

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

System/Logon

Policy	Setting
Turn on security key sign-in	Enabled

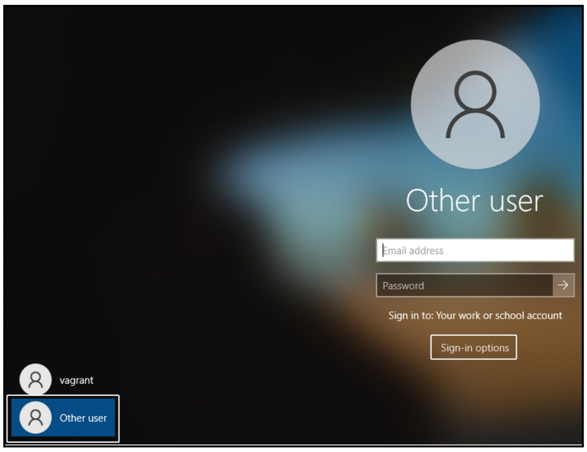
3. Associate the GPO to the appropriate Windows 10 devices.

User Experience: Lock screen enabled

After going through any of the 3 methods above, an end user should see the lock screen enabled with an additional security key sign-in option.

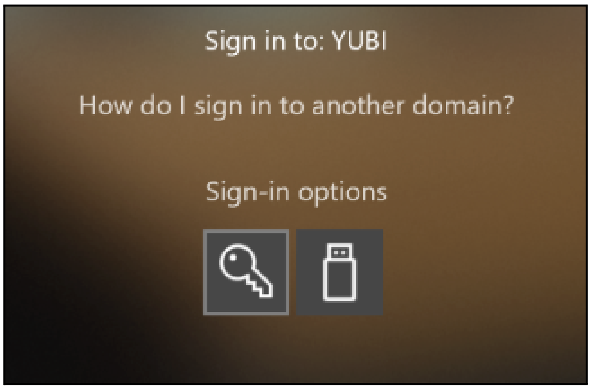
<u>Note</u>: The process below assumes that the user has already registered one or more YubiKeys as FIDO2 security keys with their Azure AD account.

1. The first time signing in with the user, the user may need to select **Other user**.



Sign in to: Your work or school account

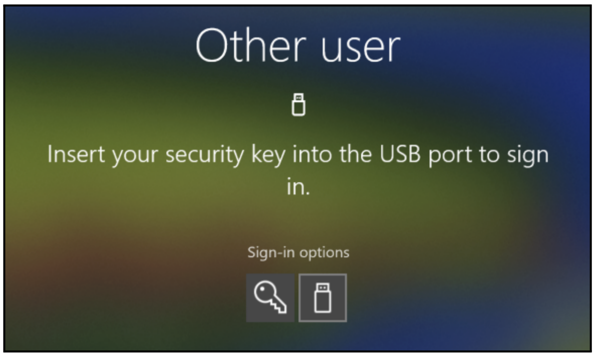
2. Then, at the bottom, click on **"Sign-in options"**



Sign in to: YUBI

How do I sign in to another domain?

3. Click on the Security Key icon
4. The verbiage "**Insert your security key…**" should appear.



Insert your security key into the USB port to sign in.

5. This confirms successful enablement of FIDO2 Sign-in on Windows 10 devices.

Known Limitations

The following information is accurate as of August 2021. Microsoft plans to evolve support for FIDO2 passwordless authentication within their ecosystem.

- FIDO2 authentication is not supported for logging into Windows Servers.
- For information on RDP support, refer to the “YubiKeys for Azure AD Passwordless User Enablement Guide”.
- Users who are in privileged groups in on-prem Active Directory will be blocked from Windows 10 sign in by default.
- If multiple FIDO2 credentials are loaded on a FIDO2 Security Key, only one FIDO2 credential will be selected for authentication into Windows 10 at this time. The last loaded FIDO2 credential will be automatically selected.

Additional Considerations

While this document outlines the basics steps to enable and test FIDO2 passwordless authentication within an AAD environment, we recommend evaluating some additional configurations within AAD:

- Key Restriction Policy
    - This feature allows administrators to limit allowed FIDO2 Security Key to specific identifiers (AAGUIDs). Yubico’s AAGUIDs can be found here: https://support.yubico.com/hc/en-us/articles/360016648959
- Enabling high privilege groups
- Kerberos server maintenance
- Passwordless authentication auditing
- Conditional Access - Azure AD Conditional Access policies allow you to build conditions that manage security controls that can block access, require multi-factor authentication, or restrict the user’s session when needed and stay out of the user’s way when not.
- Employee onboarding - When onboarding a new employee, organizations can leverage several of Microsoft’s solutions with the intention of minimizing friction - Autopilot to simplify the provisioning of new hardware, Intune to setup applications the employee will need and enforce device policy, and finally, Temporary Access Pass (TAP) to provide an initial login which will enable the user to subsequently self-register their YubiKey(s).

References

Yubico and partner references that support this document.

- FIDO2 Operating Systems and Browser Support Report for latest platform support for FIDO2. Passwordless requires user verification and resident key support.

- Microsoft - Deploying passwordless

- Microsoft - Apply a Provisioning Package.

Appendix A - Microsoft Azure Licensing

The table below highlights the Microsoft Azure Licensing requirements to deploy Azure Passwordless sign-in with YubiKeys. These licenses provide the minimum requirements to deploy YubiKeys within an environment. The requirements are subject to change by Microsoft and Yubico recommends confirming with Microsoft representatives to ensure accurate licensing has been enabled. Additional features, including Conditional Access Policies, may require additional licenses.

Microsoft Licenses for					
Service/Software Component	FREE[5]	M365	PREMIUM P1	PREMIUM P2	Other Required Licenses
Azure Active Directory	✔	✔	✔	✔	
Azure Multi-Factor Authentication	✔	✔	✔	✔	
Microsoft Licenses for Passwordless Single Sign On					
Combined Security Registration	✔	✔	✔	✔	
FIDO2 Security Key	✔	✔	✔	✔	
Microsoft Licenses for Azure-Joined Windows 10 Passwordless Sign On					
Windows 10 1909	✔	✔	✔	✔	Windows 10 License
(Optional) Microsoft Intune		✔	✔	✔	Microsoft Intune License
(Optional) Provisioning Packages	✔	✔	✔	✔	
Microsoft Licenses for Hybrid Azure Joined Windows 10 Passwordless Sign On					
Windows 10 2004	✔	✔	✔	✔	Windows 10 License
Windows Server 2016 and/or 2019	✔	✔	✔	✔	Windows Server License
Azure AD Connect	✔	✔	✔	✔	
Seamless SSO	✔		✔	✔	
(Optional) Microsoft Intune		✔	✔	✔	Microsoft Intune License
(Optional) Provisioning Packages	✔	✔	✔	✔	

1. This licensing assumes all free trials have expired and customers are testing in a licensed staged environment
2. Azure Active Directory pricing: https://azure.microsoft.com/en-us/pricing/details/active-directory/
3. Features and licenses for Azure Multi-Factor Authentication https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing
4. Azure Licensing tiers support a limited amount of objects. Please verify the appropriate limits for your organization
5. Microsoft’s Azure Active Diretory Security Defaults and Limitations https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults