YubiKeys for Entra ID passwordless admin deployment guide

© Yubico 2025

Copyright

© 2025 Yubico Inc. All rights reserved.

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
2.4	May 20, 2025	• Updated with Entra branding • Introduced passkey terminology • Added references for Windows 11 • Updated guidance to include enforcing attestation and key restrictions • Added enabling and configuring passkey (FIDO2) authentication policy using PowerShell • Added instructions to generate a TAP using PowerShell • Added expected results table for successful TAP generation • Updated Entra Kerberos Cloud Trust guidance • Updated permission requirements • Added expected results table for successful Entra Kerberos configuration • Updated instructions for Intune • Added operating system support for remote desktop • Updated known limitations • Updated licensing link
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

yubico

Copyright 2
Trademarks 2
Disclaimer 2
Contact Information 2
Original Document Release Date 2
Version History 2
Introduction 5
Objectives 5
Before you begin 5
Minimum Requirements 6
Licensing 6
Hardware 6
Software 6
Role Assignments and Permissions: 7
Enabling passkey (FIDO2) security key sign-in for web-based applications 8
Option 1: Enabling and configuring the Passkeys (FIDO2) authentication policy via the Entra Admin Center 8
Option 2: Enabling and configuring the Passkeys (FIDO2) authentication policy via Powershell 12
Enabling and configuring the Temporary Access Pass authentication policy 13
Create a Temporary Access Pass (TAP) 15
Option 1: Using the Entra Portal 15
Option 2: Using PowerShell 16
Enabling passkey (FIDO2) security key sign-in into on-premises resources using Entra joined and Entra hybrid joined devices 18
Install the AzureADHybridAuthenticationManagement Module 18
Create the Kerberos Server Object: 19
Viewing and verifying the Entra ID Kerberos Server 19
Rotate the Microsoft Entra Kerberos server key 20
Remove the Kerberos Server: 20
Enabling passkey (FIDO2) security key sign-in into Windows 10 and 11 machines 21
Option 1. Using a Provisioning package method 21
Create a provisioning package 21
Apply a provisioning package 27
Option 2: Intune method 29
Option 2a: All users and devices 29
Option 2b: Targeted Intune deployment 30
Option 3: Group policy method 33
Supported vs Unsupported Scenarios 34
Known Issues 34
Appendix A - Microsoft Azure Licensing 35

© Yubico 2025

Introduction

This document provides guidance for deploying phishing-resistant passwordless authentication with passkeys (FIDO2) using YubiKeys in a Microsoft Entra ID environment. It also includes instructions for configuring single sign-on (SSO) to on-premises resources by enabling Microsoft Entra ID to issue Kerberos Ticket Granting Tickets (TGTs) for Active Directory domains using Entra Kerberos with Cloud Kerberos Trust, when signing in from Entra joined and Entra hybrid joined devices.

Microsoft and the FIDO2/Webauthn ecosystem as a whole have undergone a rebranding of "FIDO2 security keys" to "passkeys." While there are nuanced differentiators to these two terms, in the context of these guides they refer to the same concept, to help with the transition of the rebranding we will try to use the new "Passkey" terminology but also refer to the older "FIDO2 security key" terminology.

Objectives

- Enable passkeys (FIDO2) security key sign-in to Web-based applications
- Enable passkeys (FIDO2) security key sign-in into Windows 10 and 11 devices
- Enable passkeys (FIDO2) security key sign-in into on-premise resources using Single sign-on (SSO)

Before you begin

- **Enablement vs Enforcement**
    - **Enablement** is the introduction of passwordless authentication methods such as passkeys (FIDO2) on YubiKeys to provide users with a seamless and secure sign-in experience. This represents the initial phase in deploying phishing-resistant, passwordless authentication and is the primary focus of this guide.
    - **Enforcement** goes a step further by actively preventing the use of weaker authentication methods, such as passwords and phishable MFA, and requiring strong authentication with passkeys (FIDO2) to strengthen overall security posture. For enforcement guidance please refer to the **Enforce YubiKeys for Entra ID Sign-in guide.**
- Yubico recommends identifying a select number of users or a group to test these configurations instead of applying to all users.
    - For testing purposes, we recommend:
        - Using standard user accounts with lower privileges.
          Note: In Entra ID Hybrid deployments, Microsoft blocks high privileged accounts (e.g., Domain Admins) from signing in with a Security Key by default. To learn more, please refer to FIDO2 security key sign-in isn't working for my Domain Admin or other high privilege accounts. Why?
        - Using internal member accounts.
          Note: Entra ID guest accounts have several limitations in registration and usage of passkeys (FIDO2). To learn more, please refer to: Supported-scenarios
          Learn more about different Entra ID user types here

© Yubico 2025

Minimum Requirements

Licensing

- Registration and passwordless sign-in with security keys in Microsoft Entra does not require a license. However, Microsoft recommends at least a Microsoft Entra ID P1 license to take full advantage of passwordless capabilities.

  For example, a P1 license allows you to:

  - Enforce sign-in with YubiKeys through Conditional Access
  - Track adoption using the Authentication Methods Activity Report

  Microsoft Entra Licensing requirements are referenced in Appendix A. *Note: licensing requirements are subject to change.*

Hardware

- You will need at least one (preferably two) supported YubiKeys from the following series:
  - YubiKey 5 Series
  - YubiKey 5 FIPS Series
  - YubiKey Bio Series (includes FIDO and Multi-protocol Editions)
  - Security Key Series (includes Enterprise Edition)

Software

- **Web Sign-in Requirements**
  A compatible browser and platform that supports Passkeys (FIDO2)
- **Windows Sign-in Requirements**
  Devices must be running a supported version of Windows 10 or 11 and joined to Entra ID (or hybrid joined).
  - **Browser SSO** in Windows 10 or newer is supported on Microsoft Edge (natively), Chrome (via the Windows 10 Accounts or Mozilla Firefox v91+ (Firefox Windows SSO setting).
- **Single Sign-On to On-Premises Resources**
  Requires Microsoft Entra Kerberos trust prerequisites, including minimum operating system requirements for domain controllers , Entra Connect, and a healthy hybrid identity configuration.

© Yubico 2025

Role Assignments and Permissions:

- **Enable FIDO2 Security Key Sign-in (Tenant Level)**
  - To enable FIDO2 security key sign-in across the tenant, one of the following Microsoft Entra roles is required:
    - **Global Administrator** role
    - **Authentication Policy Administrator** role

  These roles are necessary for:
  - Configuring the **Authentication Methods** policies:
    - Passkey (FIDO2)
    - Temporary Access Pass (TAP)
- **Enable security keys for Windows sign-in:**
  - **Intune**
    - To create and assign profiles for enabling security key sign-in via Microsoft Intune, assign one of the following Intune (Endpoint Manager) roles:
      - **Intune Administrator**
      - **Policy and Profile Manager**
      - **Endpoint Security Manager**

  These roles include permissions to create and assign configuration profiles:
  - **Group Policy**
    - When deploying policies at the domain level:
      - A member of the **Domain Admins** group in the domain
    - When deploying policies at the OU level
      - Delegated **Create** and **Link GPOs permission**
- **SSO into On-Premises Resources:**

  To configure **Entra Kerberos Cloud Trust:**
  - An **Active Directory user** must be:
    - A member of the **Domain Admins** group in the domain, and
    - A member of the **Enterprise Admins** group in the forest.
  - A **Microsoft Entra user** must be assigned the:
    - **Hybrid Identity Administrator** role

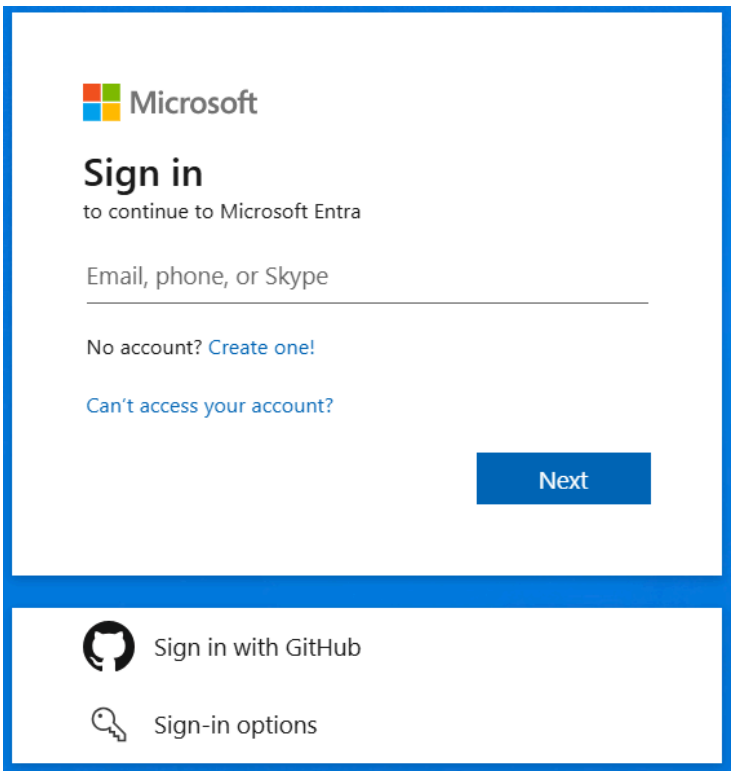
yubico

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

This section describes how to enable Entra ID users to leverage passkeys (FIDO2) on YubiKeys for passwordless authentication into web-based applications.

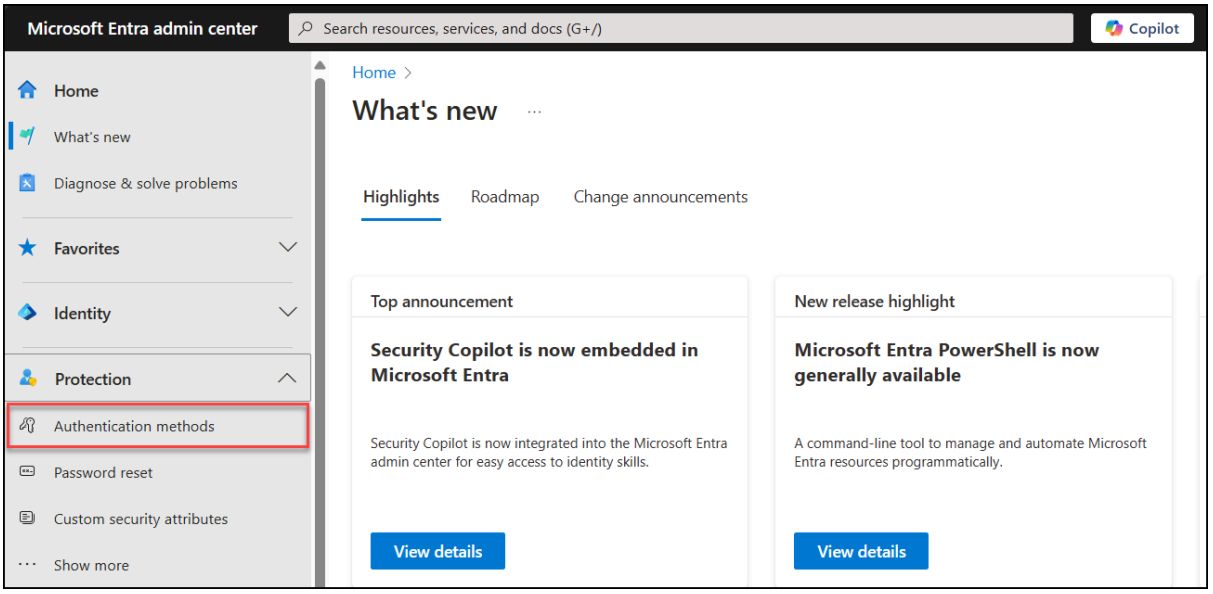
Option 1: Enabling and configuring the Passkeys (FIDO2) authentication policy via the Entra Admin Center

1. Navigate to the **Entra Admin Center:** https://entra.microsoft.com
2. Sign-in with an account that holds at least the **Authentication Policy Administrator** role.

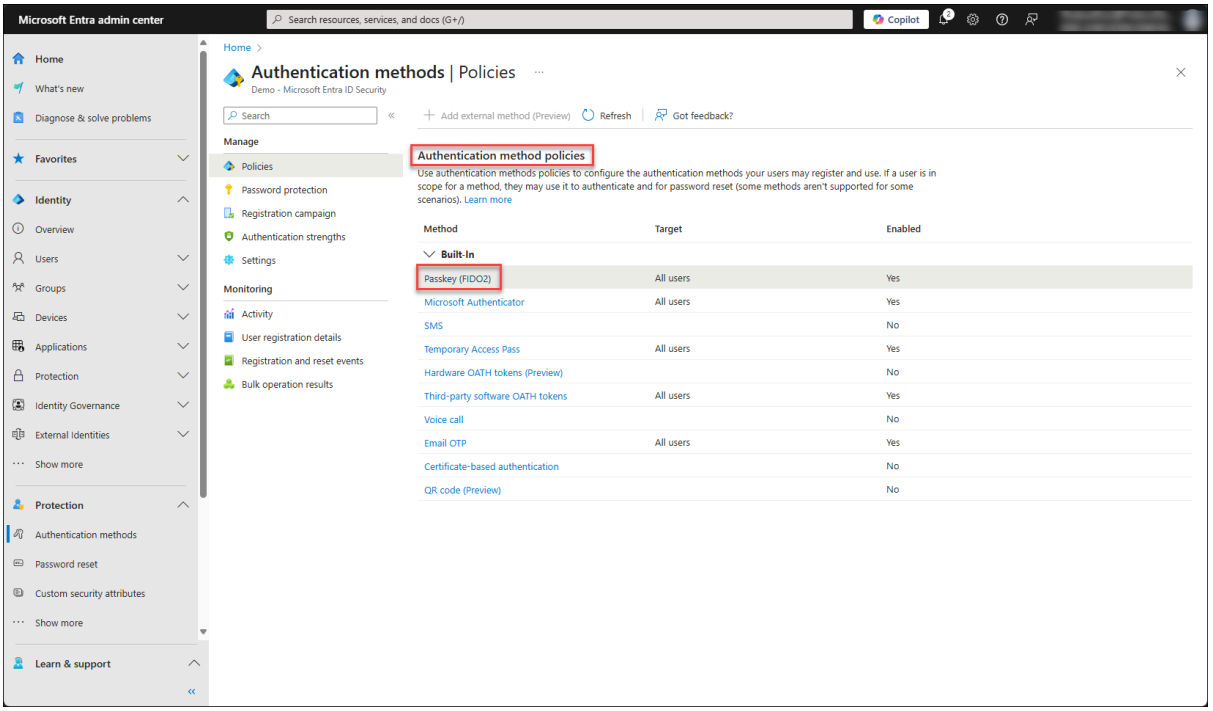


© Yubico 2025

3. In the menu pane on the left, expand the **Protection** blade and select **Authentication methods**

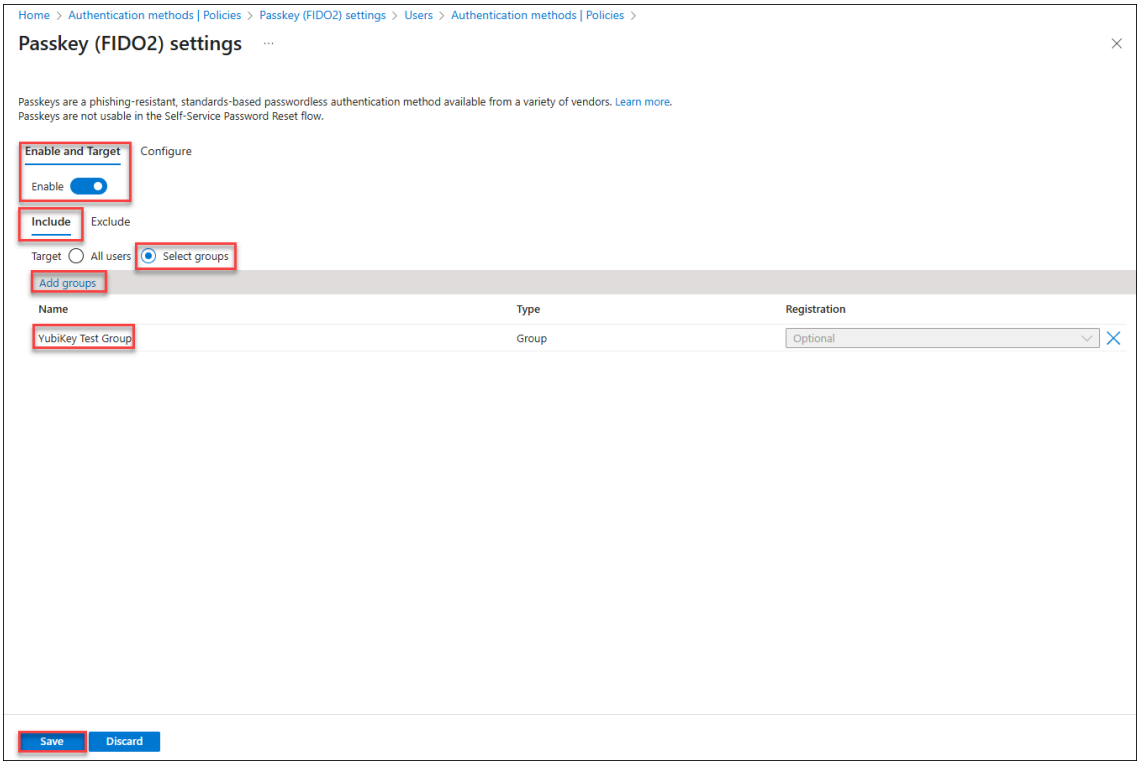


4. Under the **Authentication methods policy** options select **Passkeys (FIDO2)**

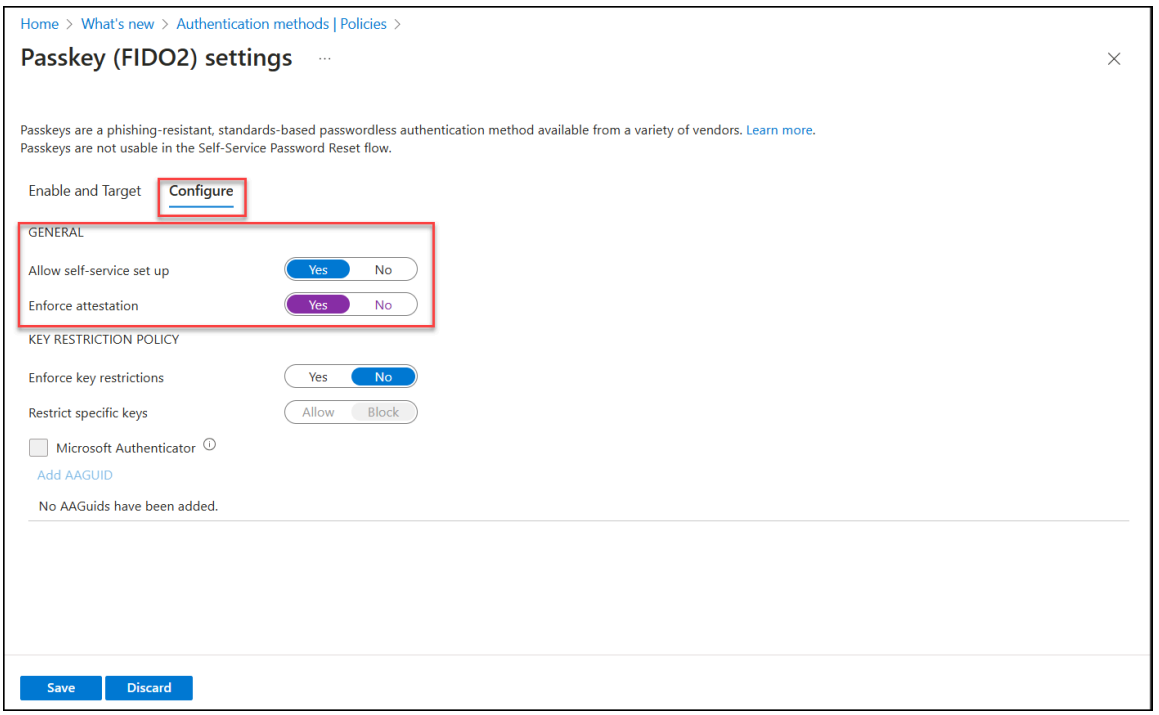


© Yubico 2025

5. Under **Enable and Target**, toggle the **Enable** option. By default the **Target** is set to **All Users.** For testing purposes Yubico recommends scoping the deployment to a group populated with test users. Under **Include**:
    a. Click on **Select groups** > **Add groups**
    b. Locate and **Select** your test group
    c. Click **I Acknowledge**
    d. Click **Save**



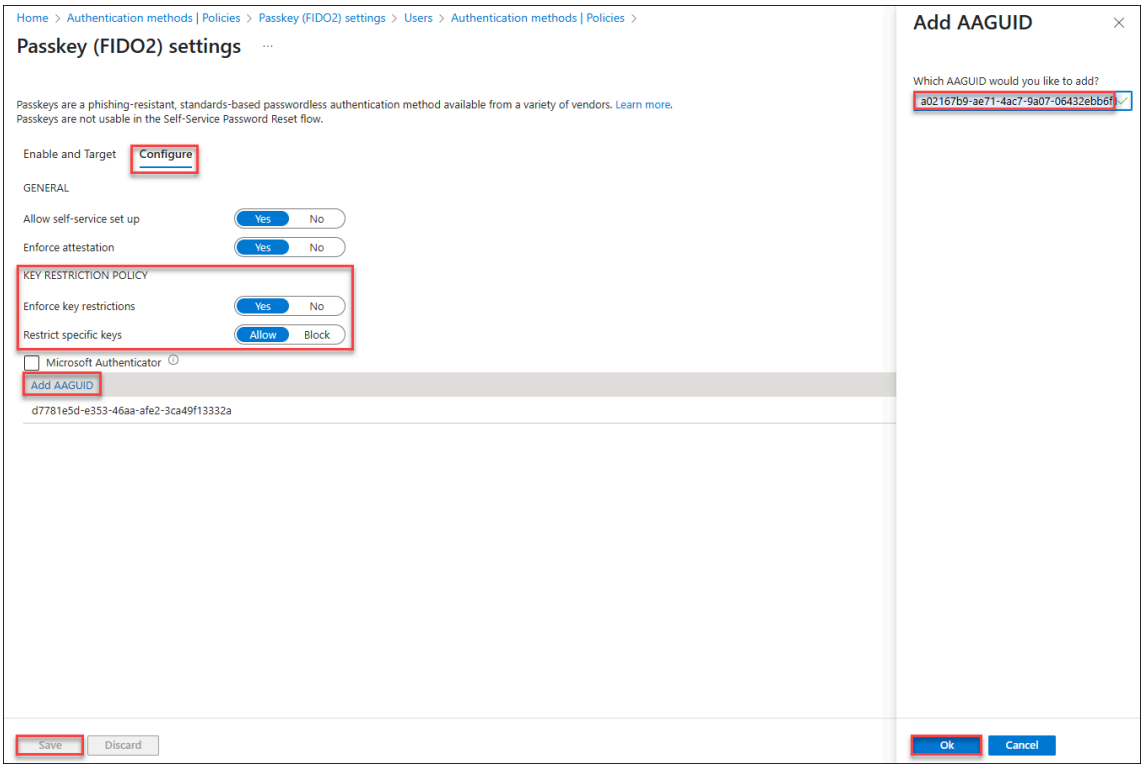
6. Select the **Configure** option and enable the following settings:
    a. **Allow self-service setup** is set to **Yes** by default
    b. Set **Enforce attestation** to **Yes (recommended)**



© Yubico 2025

We recommend you enable the **Key Restriction Policy** settings to restrict key registration to specific make and model of security keys you intend to use. This is a tenant-wide list so should include a list of all passkey (FIDO2) authenticators that are used in the tenant, this list will influence which authenticators can be **registered** in the tenant. Please review the additional guides to enforce which authenticators are used during **authentication**. For this Passkey (FIDO2) policy Yubico recommends:

c. Set the **Enforce key restrictions** setting to **Yes**.
d. Set the **Restrict specific keys** setting to **Allow**.
    i. Click **Add AAGUID** and enter the FIDO2 AAGUID for the YubiKey model type. You can identify the AAGUID of the YubiKey using the ykman CLI by running the command: ***ykman fido info***. The full list of YubiKey AAGUIDs is referenced in the YubiKey hardware FIDO2 AAGUIDs support article. You can also verify the AAGUID on your YubiKey using the Retrieve a YubiKey AAGUID support article.
    ii. Click **Ok.**
e. Click **Save** to enable the policy.



© Yubico 2025

Option 2: Enabling and configuring the Passkeys (FIDO2) authentication policy via Microsoft Graph Powershell SDK

1. Launch **PowerShell** as an **administrator** and run the following commands modifying input values as needed:

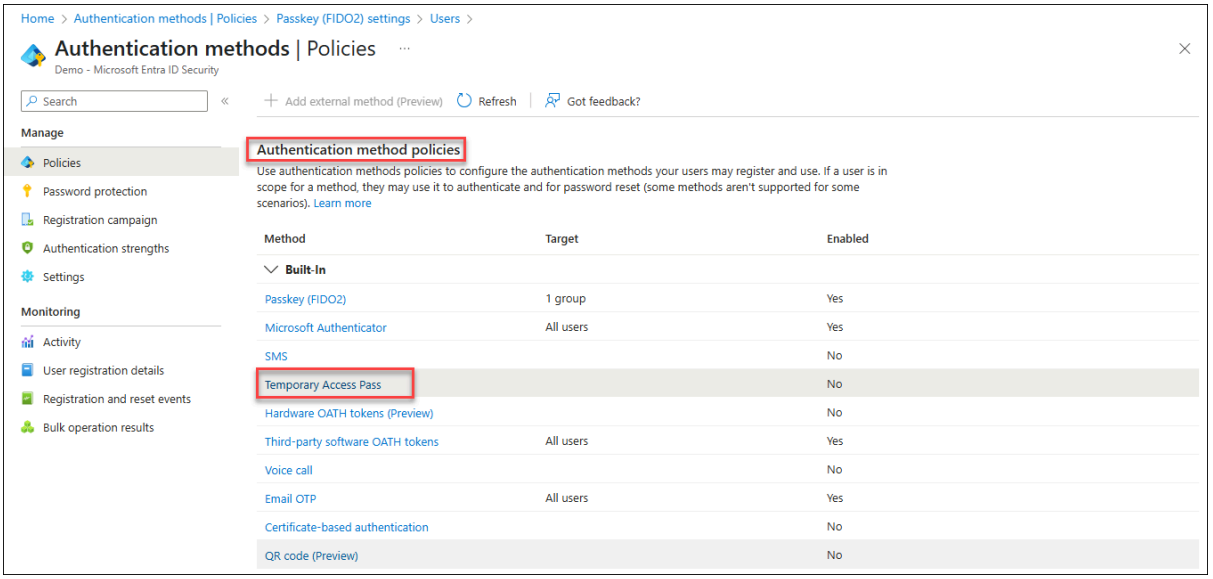
```
#Update Entra ID Passkey Auth Method Policy with the AAGUIDs
that are relevant to your Entra ID Tenant
#List of AAGUIDS
$AAGUIDs = @("d7781e5d-e353-46aa-afe2-3ca49f13332a")
#Connect to Microsoft Graph
Connect-MgGraph -Scopes "Policy.ReadWrite.AuthenticationMethod"
#Passkey Authentication Method Policy Configurations
$params = @{
    "@odata.type"                    =
"#microsoft.graph.fido2AuthenticationMethodConfiguration"
    id                               = "Fido2"
    state                            = "enabled"
    includeTargets                   = @(
        @{
            id          = "all_users"
            targetType = "group"
        }
    )
    excludeTargets                   = @(
    )
    isSelfServiceRegistrationAllowed = $true
    isAttestationEnforced            = $true
    keyRestrictions                  = @{
        isEnforced      = $true
        enforcementType = "Allow"
        aaGuids         = $AAGUIDs
    }
}
Update-MgPolicyAuthenticationMethodPolicyAuthenticationMethodCon
figuration -AuthenticationMethodConfigurationId "Fido2"
-BodyParameter $params
```

yubico

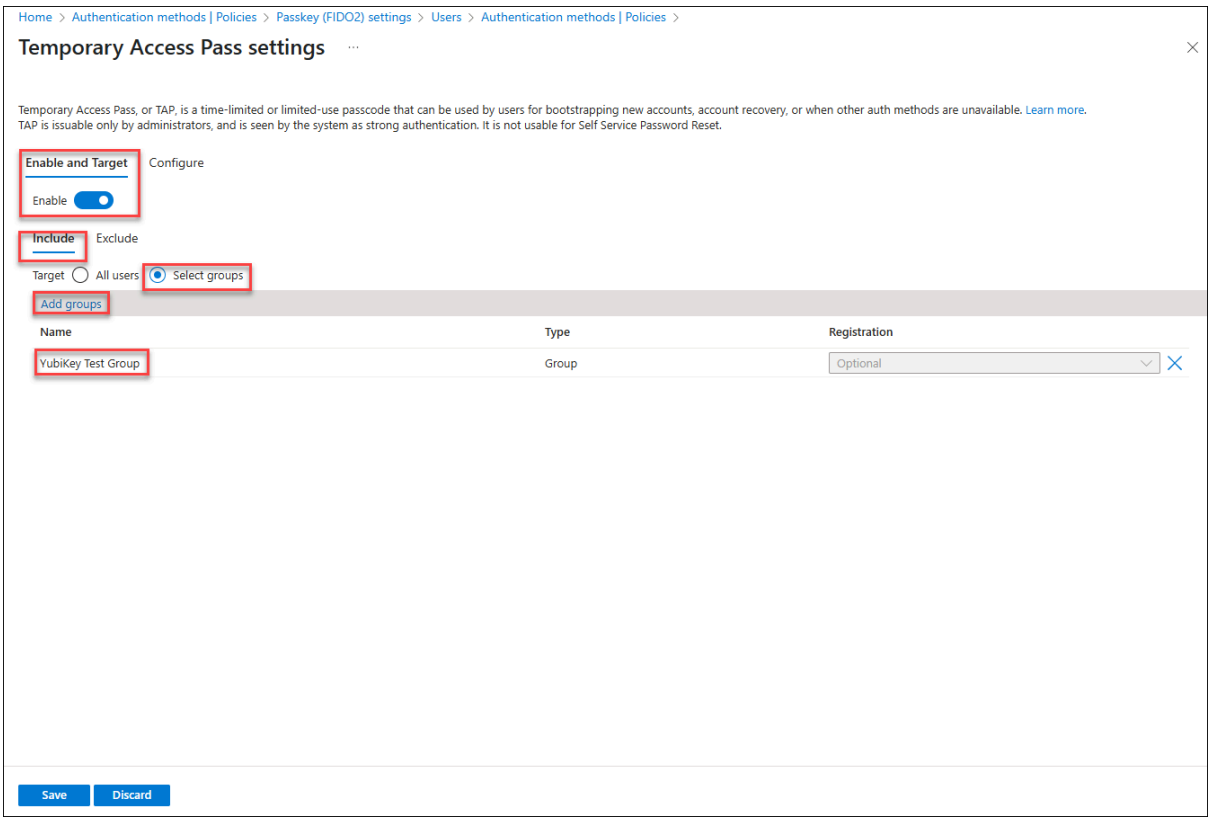
Enabling and configuring the Temporary Access Pass authentication policy

This section outlines how to enable the Temporary Access Pass (TAP) policy, allowing IT administrators to issue TAPs to users registering passkeys (FIDO2) on YubiKeys using the self-service method. TAPs also enable passwordless onboarding for new users.

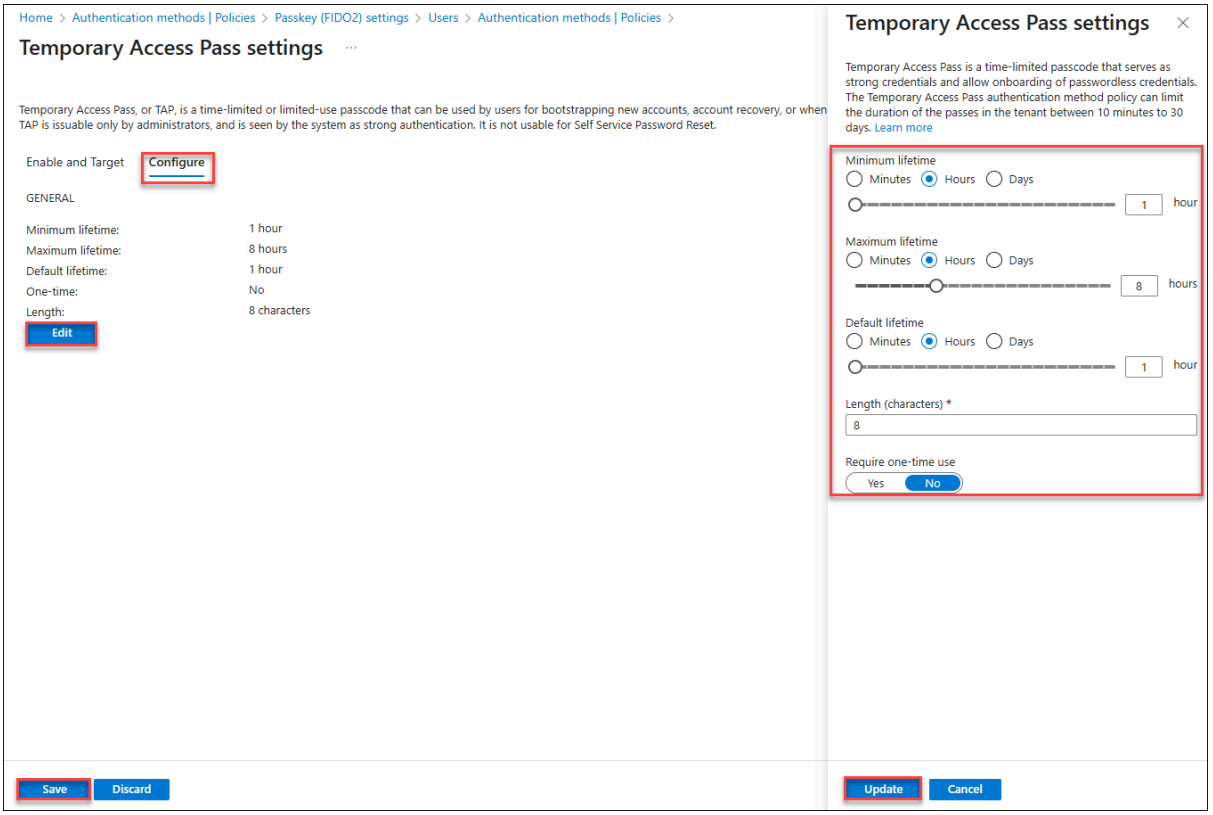
1. Under the **Authentication Methods policy** page, select the **Temporary Access Pass** policy. **Note:** Your tenant may have this policy enabled by default.



2. Under the **Enable and Target option**, ensure the setting is **Enabled.** By default the **Target** is set to **All Users.** For testing purposes Yubico recommends scoping the deployment to your test group. Under **Include**:
    a. Click **Select groups**
    b. Locate and **select** your test group



3. Select the **Configure** option and click **Edit** to modify the default settings as needed
    a. Click **Update** and click **Save** to apply the changes to the policy.



© Yubico 2025

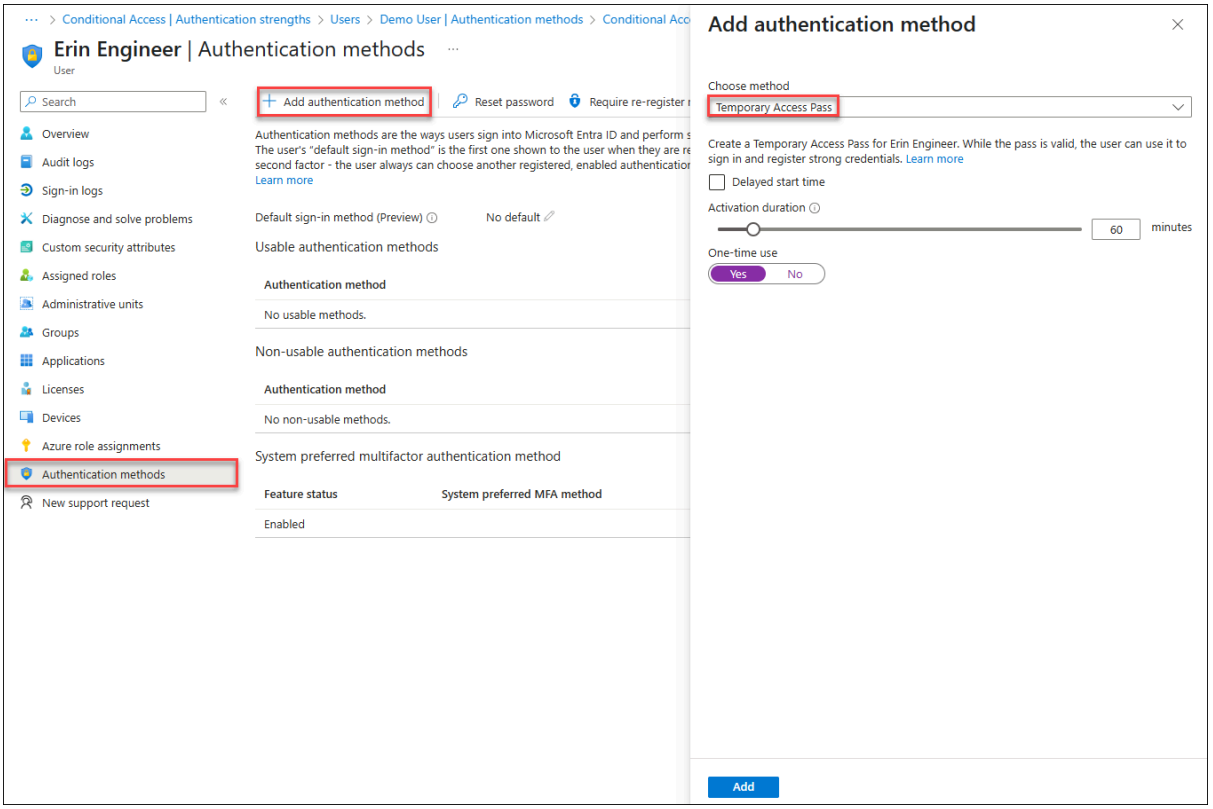
Create a Temporary Access Pass (TAP)

After you enable a policy, you can create a TAP for a user in Entra ID. These roles can perform the following actions related to a TAP:

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

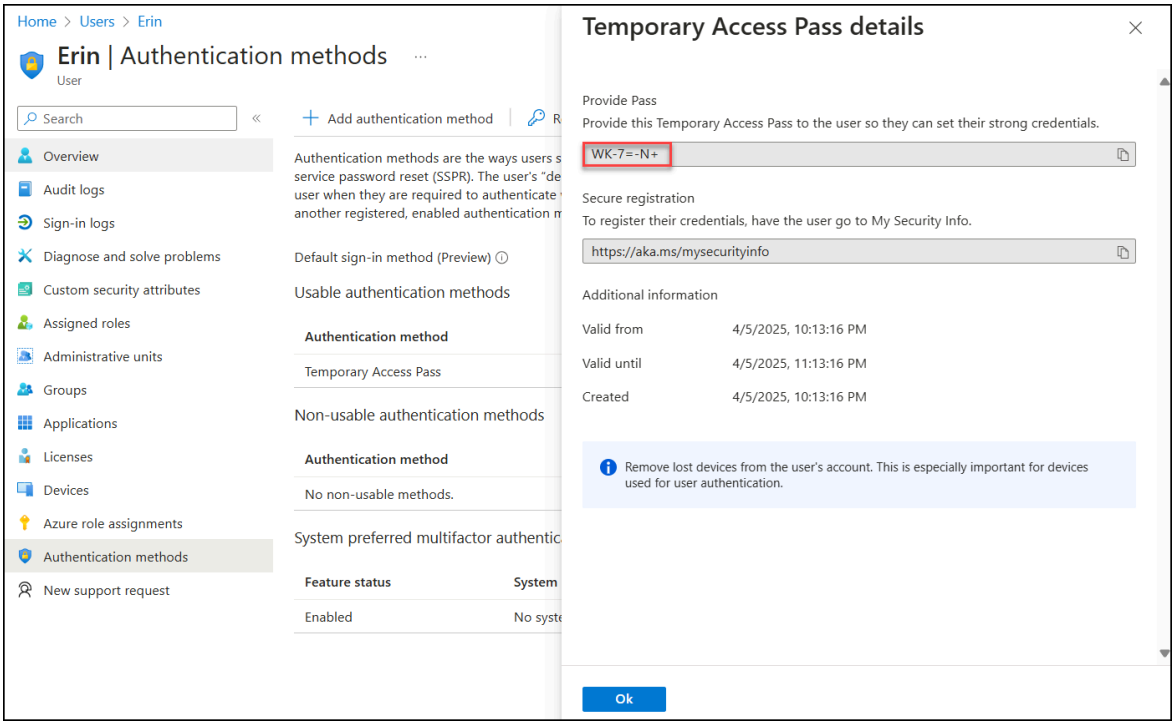
Option 1: Using the Entra Portal

1. Sign in to the **Entra Admin Center** with an account that holds at least the **Authentication administrator** role
2. In the left menu pane, expand the **Identity** blade and select **Users**
3. Select a user, then select **Authentication methods** in the menu on the left:
    a. Click on **Add authentication method**
    b. Select **Temporary Access Pass** from the drop-down menu
    c. Select your desired settings and then click **Add** to create a new Temporary Access Pass



© Yubico 2025

4. **Important**: Make a note of the actual TAP value, because you provide this value to the user. You can't view this value after you select **Ok**.
    a. Ensure the TAP is handled and delivered securely to the end-user



Option 2: Using PowerShell

The following sample commands show how to generate a TAP using PowerShell.

2. Launch **PowerShell** as an **administrator** and run the following commands modifying input values as needed:

```
 # Connect to Microsoft Graph
Connect-MgGraph -Scopes "UserAuthenticationMethod.ReadWrite.All"

# Create a Temporary Access Pass
$properties = @{43
    isUsableOnce = $true
    startDateTime = '2025-04-06T19:15:00Z'
}

$propertiesJSON = $properties | ConvertTo-Json

New-MgUserAuthenticationTemporaryAccessPassMethod -UserId
"user@contoso.onmicrosoft.com" -BodyParameter $propertiesJSON
```

© Yubico 2025

You should receive results similar to the following:

Property	Value
User ID	user@contoso.onmicrosoft.com
TAP Created At	4/6/2025 7:09:43 PM UTC
TAP Start Time	4/6/2025 7:15:00 PM UTC
Is Usable	False
Is Usable Once	True
Lifetime	60 minutes
Usability Reason	NotYetValid
Temporary Access Pass	+xz$9vpa

What This Means:

- The TAP will become valid at 3:15 PM EDT (7:15 PM UTC).
- It's configured for one-time use, with a 60-minute validity window starting at that time.
- Until then, IsUsable = False with the reason: NotYetValid.
- Note: Configuring the IsUsableOnce property to True enhances security but may impact usability. If the security key registration process fails or is interrupted, the user will not be able to retry without a new Temporary Access Pass.

Users can now register and use YubiKeys for passwordless authentication. For end user instructions, please refer to the **User Enablement Guide**.

Note:

- An expired or deleted TAP can't be used for interactive or non-interactive authentication.
- Users need to reauthenticate with different authentication methods after the TAP is expired or deleted.
- The token lifetime (session token, refresh token, access token, and so on) obtained by using a TAP sign-in is limited to the TAP lifetime. When a TAP expires, it leads to the expiration of the associated token.
- When using a one-time TAP to register a passwordless method such as a FIDO2 security key the user must complete the registration within 10 minutes of sign-in with the one-time TAP. This limitation doesn't apply to a TAP that can be used more than once.

For more information on Temporary Access Pass configuration and limitations, refer to the official Microsoft documentation.

yubico

Enabling passkey (FIDO2) security key sign-in into on-premises resources using Entra joined and Entra hybrid joined devices

This section outlines the administrative steps required to enable passwordless single sign-on (SSO) to on-premises resources from Windows 10 and 11 devices that are either Microsoft Entra ID joined or Entra hybrid joined. This setup requires Microsoft Entra Connect to be installed and properly configured to integrate your on-premises Active Directory with your Entra ID tenant.

Before proceeding, ensure that FIDO2 authentication has been enabled in Entra ID as described in the previous section.

Note: The instructions below cover the core enablement steps. For complete, step-by-step guidance, refer to the official Microsoft documentation.

Install the AzureADHybridAuthenticationManagement Module

1. Login to a Windows server running Entra Connect with a user who is a member of the **Domain Admins** group for the Active Directory domain and a member of the **Enterprise Admins** group for the Active Directory forest.
2. Run **Powershell** as an **administrator.**
3. Install the **AzureADHybridAuthenticationManagement** module:
    a. Note: You can install the **AzureADHybridAuthenticationManagement** module on any computer from which you can access your on-premises Active Directory Domain Controller, without dependency on the Microsoft Entra Connect solution.
    b. The **AzureADHybridAuthenticationManagement** module is distributed through the PowerShell Gallery. The PowerShell Gallery is the central repository for PowerShell content.

```
# First, ensure TLS 1.2 for PowerShell gallery access.
[Net.ServicePointManager]::SecurityProtocol =
[Net.ServicePointManager]::SecurityProtocol -bor
[Net.SecurityProtocolType]::Tls12

# Install the AzureADHybridAuthenticationManagement PowerShell module.
Install-Module -Name AzureADHybridAuthenticationManagement
-AllowClobber
```

© Yubico 2025

Create the Kerberos Server Object:

1. Run the following PowerShell commands to enable Entra Kerberos and create a server object both in your on-premises Active Directory domain and in your Entra tenant:

> *Note: If your organization protects password-based sign-in and enforces modern authentication methods such as multifactor authentication, FIDO2, or smart card technology, you must use the -UserPrincipalName parameter with the User Principal Name (UPN) of a Hybrid Identity Administrator.*
>
> - *Replace contoso.corp.com in the following example with your on-premises Active Directory domain name.*
> - *Replace administrator@contoso.onmicrosoft.com in the following example with the UPN of a Hybrid Identity Administrator.*

```
# Specify the on-premises Active Directory domain. A new Microsoft
Entra ID
# Kerberos Server object will be created in this Active Directory
domain.
$domain = $env:USERDNSDOMAIN

# Enter a UPN of a Hybrid Identity Administrator
$userPrincipalName = "administrator@contoso.onmicrosoft.com"

# Enter a Domain Administrator username and password.
$domainCred = Get-Credential

# Create the new Microsoft Entra ID Kerberos Server object in Active
Directory
# and then publish it to Entra ID.
# Open an interactive sign-in prompt with given username to access
Microsoft Entra ID.
Set-AzureADKerberosServer -Domain $domain -UserPrincipalName
$userPrincipalName -DomainCredential $domainCred
```

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)
```

© Yubico 2025

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

Rotate the Microsoft Entra Kerberos server key

The Microsoft Entra Kerberos server encryption krbtgt keys should be rotated on a regular basis. Microsoft recommends that you follow the same schedule you use to rotate all other Active Directory DC krbtgt keys.

1. Launch **Powershell** as an **Administrator.**
2. Execute the following PowerShell command to rotate the krbtgt keys.

```
Set-AzureADKerberosServer -Domain $domain -CloudCredential
$cloudCred -DomainCredential $domainCred -RotateServerKey
```

Remove the Kerberos Server:

If you want to revert the scenario and remove the Microsoft Entra Kerberos server from both the on-premises Active Directory and Microsoft Entra ID, run the following command:

1. Launch **Powershell** as an **Administrator**.
2. Execute the following PowerShell command to remove the Entra ID Kerberos server object.

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

© Yubico 2025

Enabling passkey (FIDO2) security key sign-in into Windows 10 and 11 machines

This section outlines how to enable passwordless (FIDO2) security key sign-in into Windows 10 and 11 machines in either a cloud-only or hybrid identity environment. You must first enable FIDO2 in Entra ID 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 and 11 lock screen.

- Create and apply a provisioning package to a Windows 10 or 11 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 your organization's current processes to manage devices.

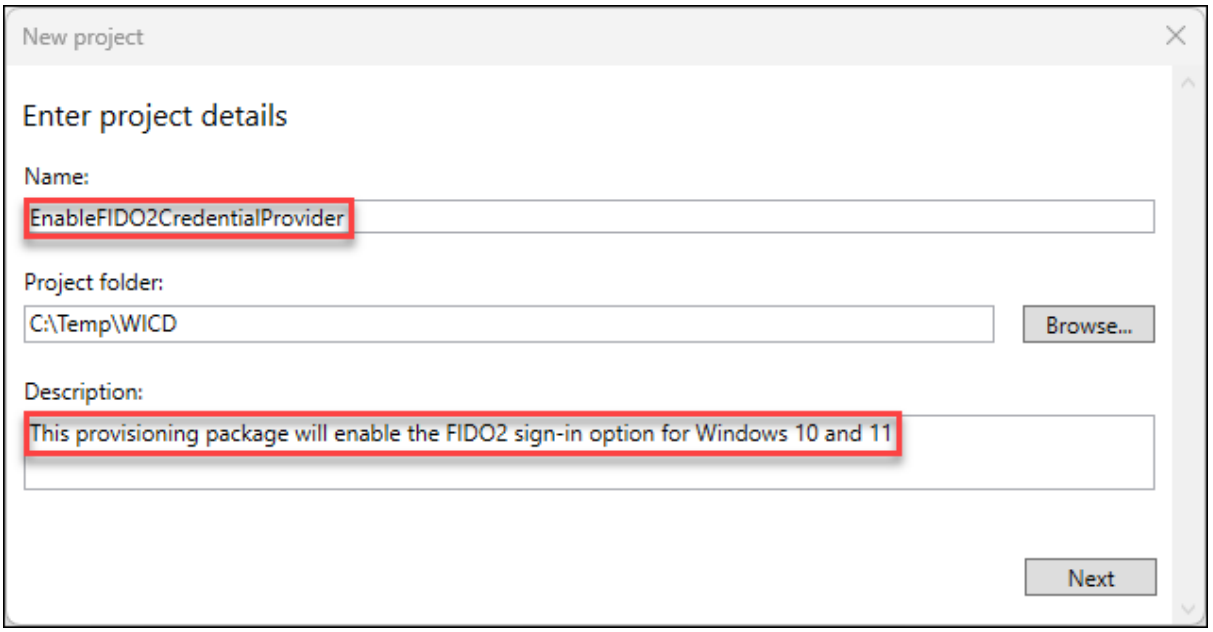
Option 1. Using a Provisioning package method

A provisioning package can be installed on the Windows 10 or 11 device to enable the FIDO2 security key sign-in option.

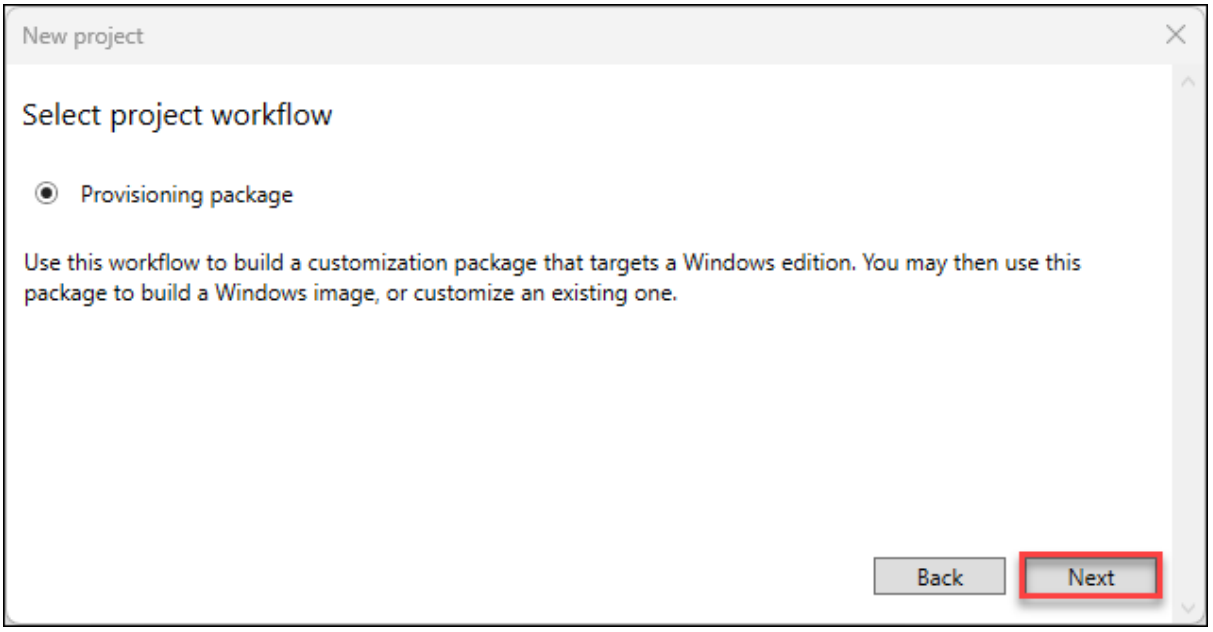
Create a provisioning package

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**.

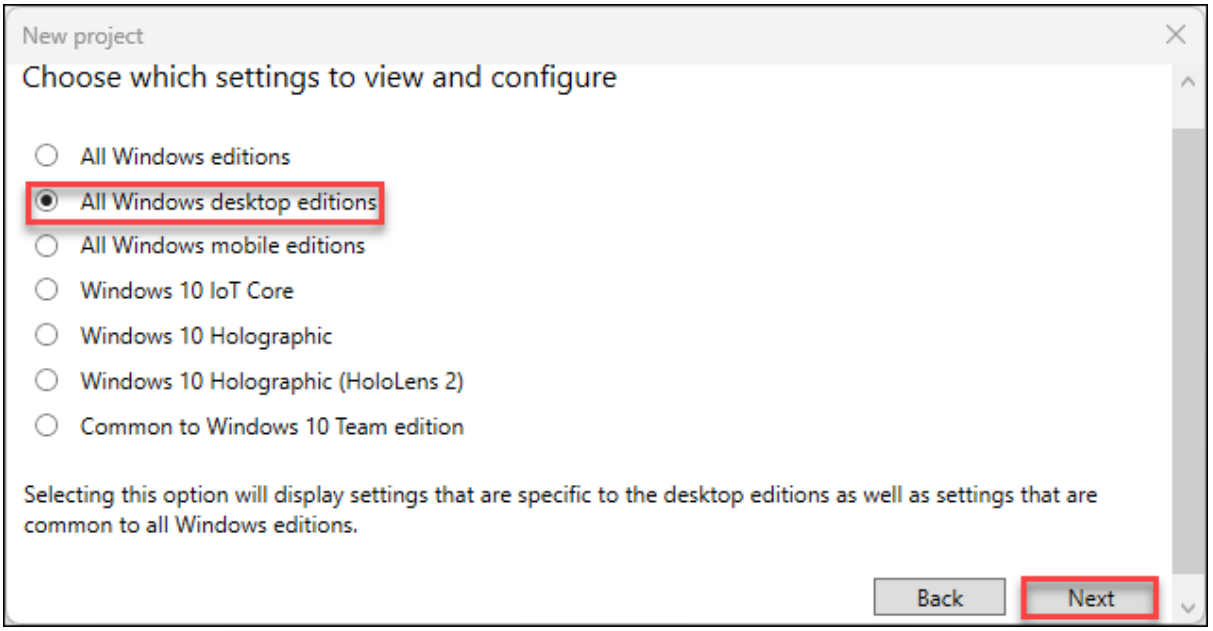


4. Leave **Provisioning package** selected as the Selected project workflow and select **Next**.



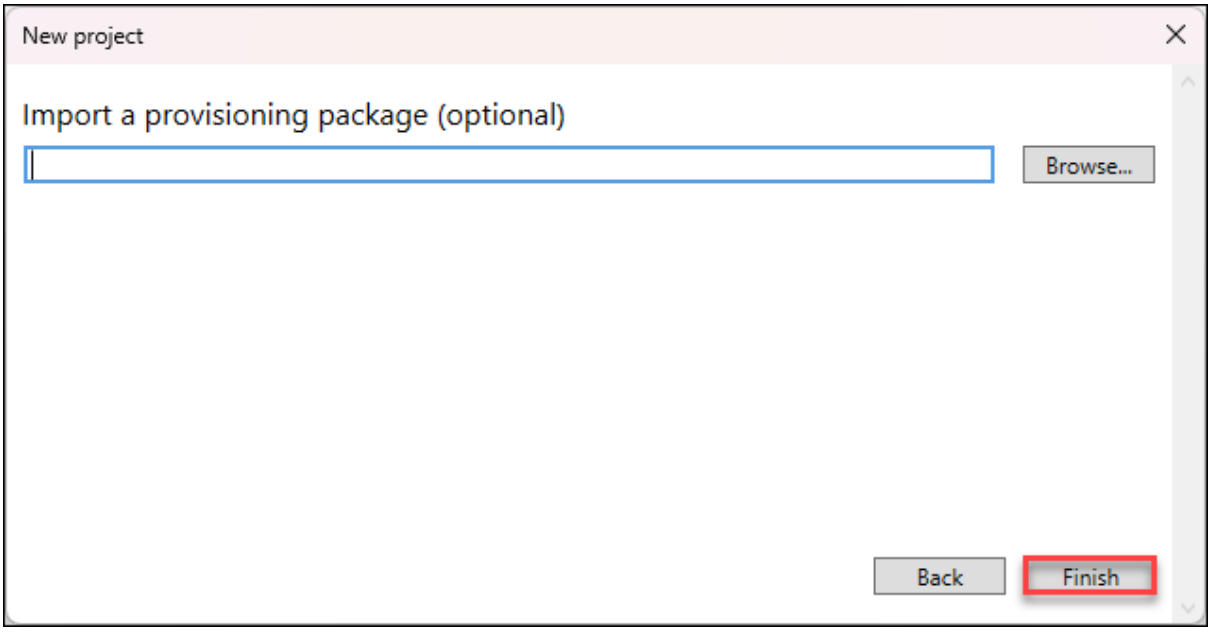
5. Select **All Windows desktop editions** under Choose which settings to view and configure, then select **Next**.

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



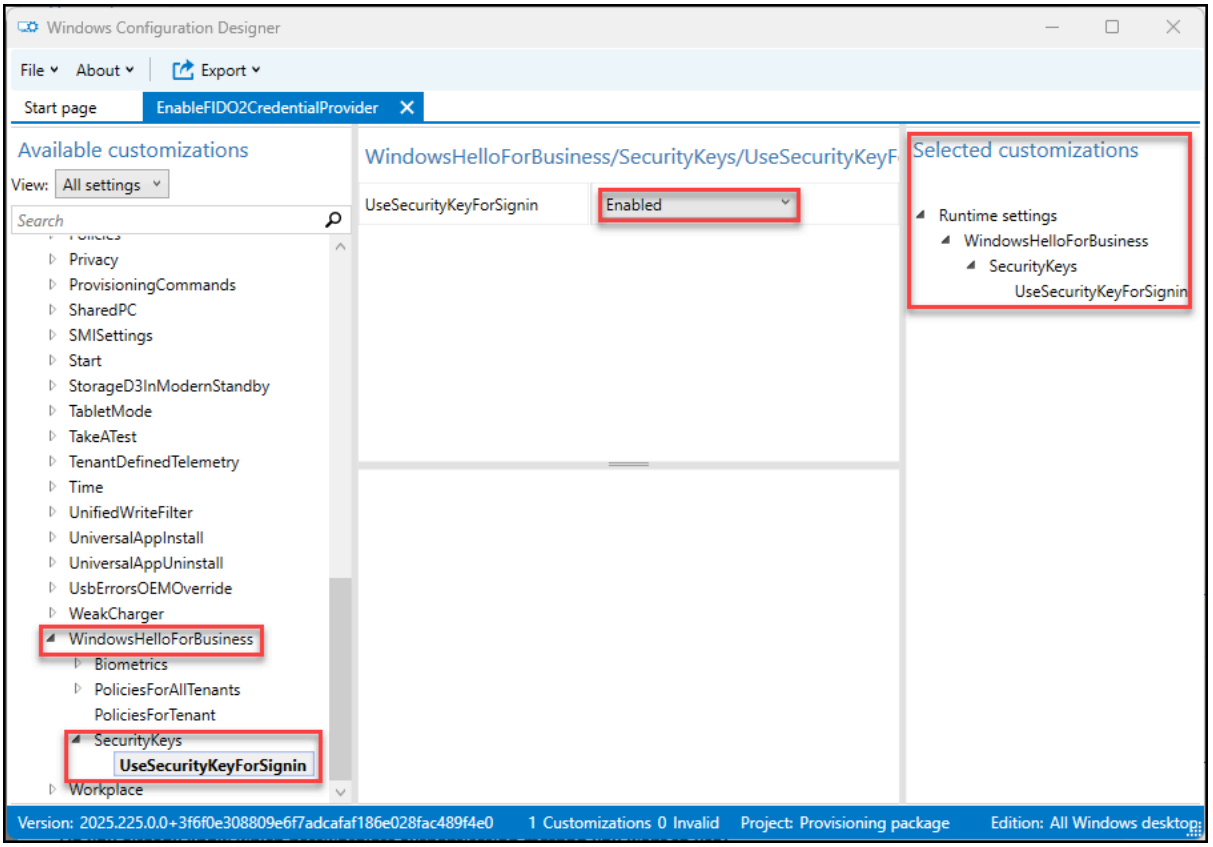
© Yubico 2025

6. Select **Finish**.



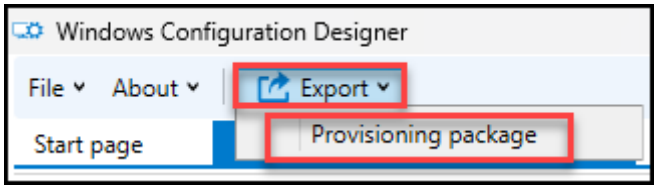
7. In your newly created project, in the left panel, browse to: **Runtime settings** > **WindowsHelloForBusiness** > **SecurityKeys** > **UseSecurityKeyForSignIn**.

    a. In the middle panel, change the **UseSecurityKeyForSignIn** to **Enabled**. The Selected customization options should display in the right pane

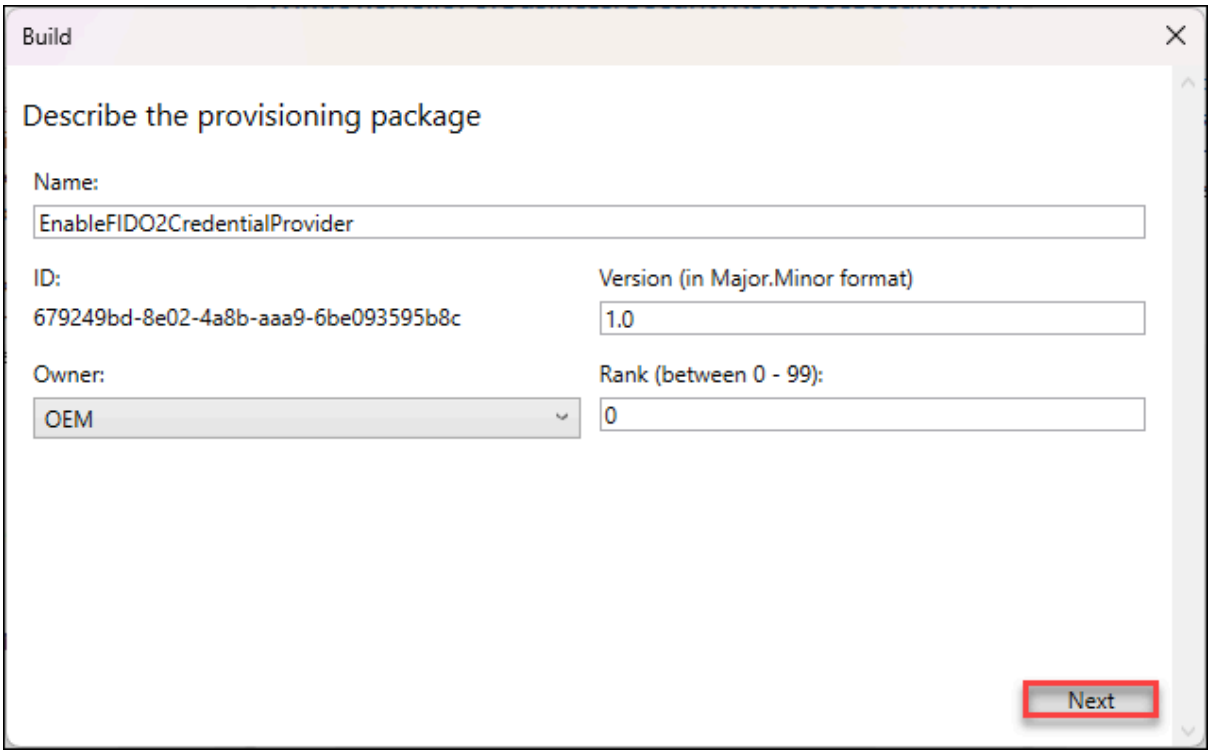


© Yubico 2025

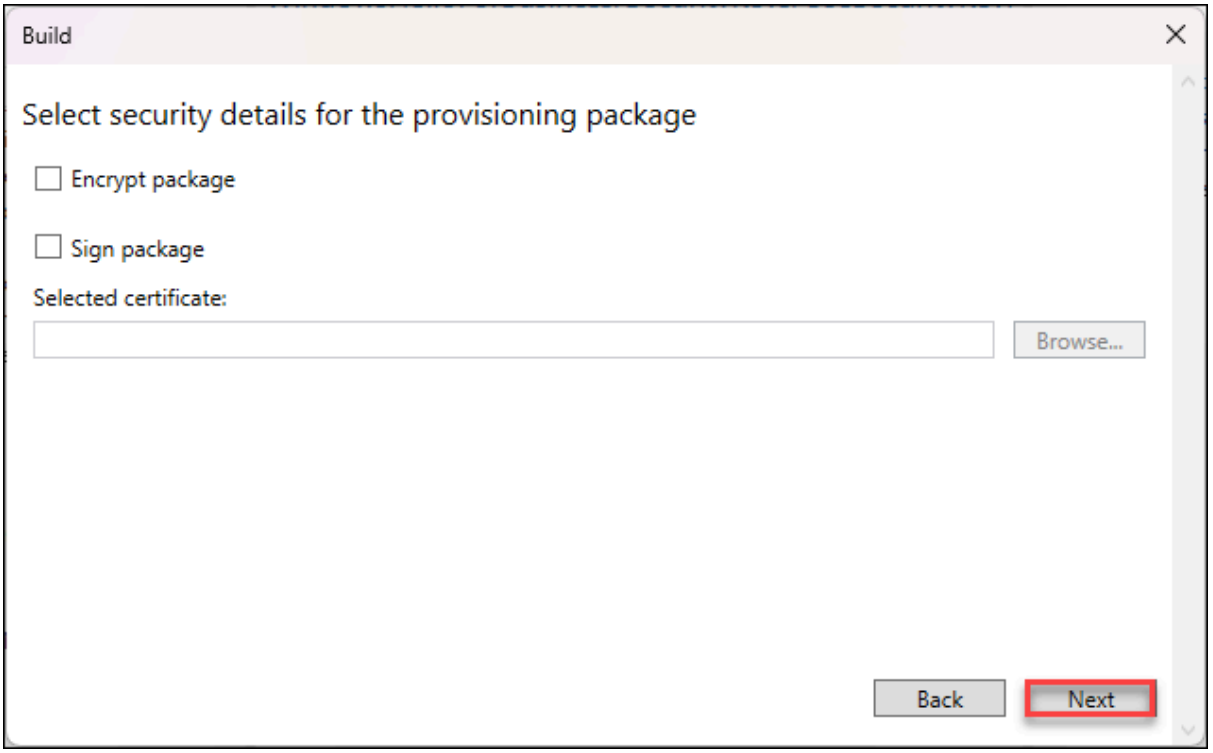
8. In the top left menus of the Configuration Designer, select **Export** > **Provisioning package**.



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

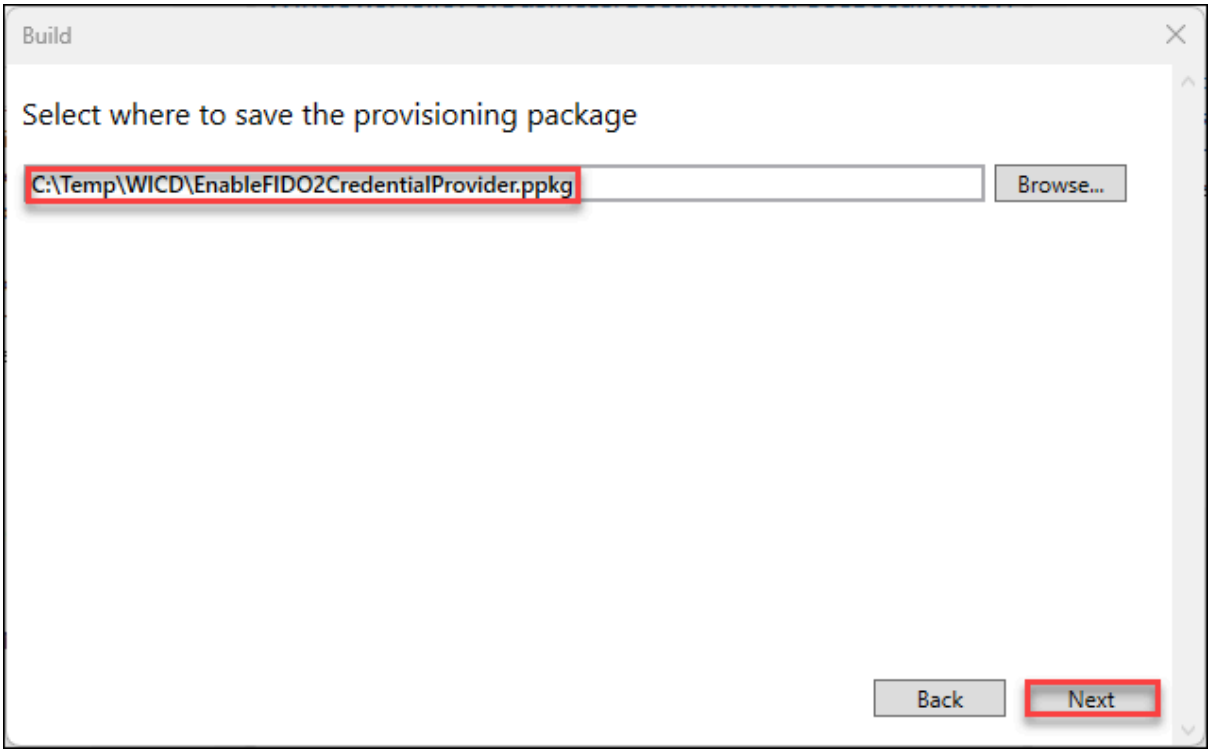


10. Leave the defaults in the **Build** window under **Select security details for the provisioning package** and select **Next**.

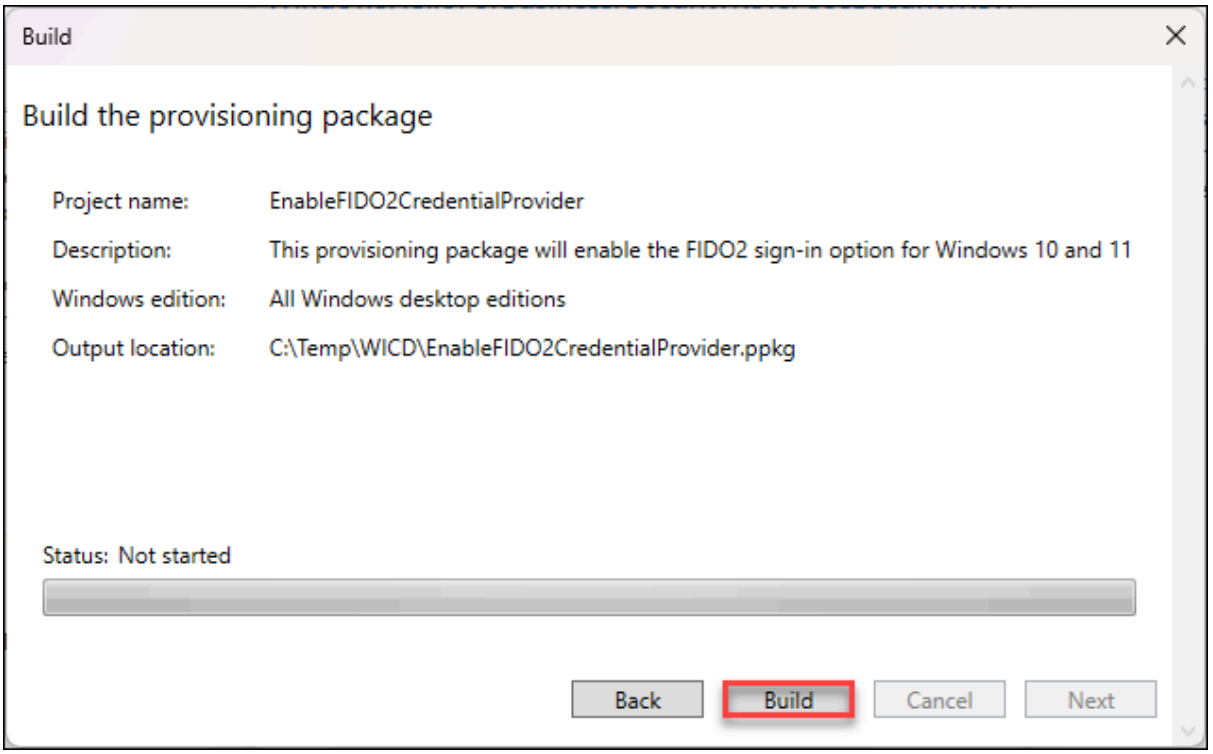


© Yubico 2025

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

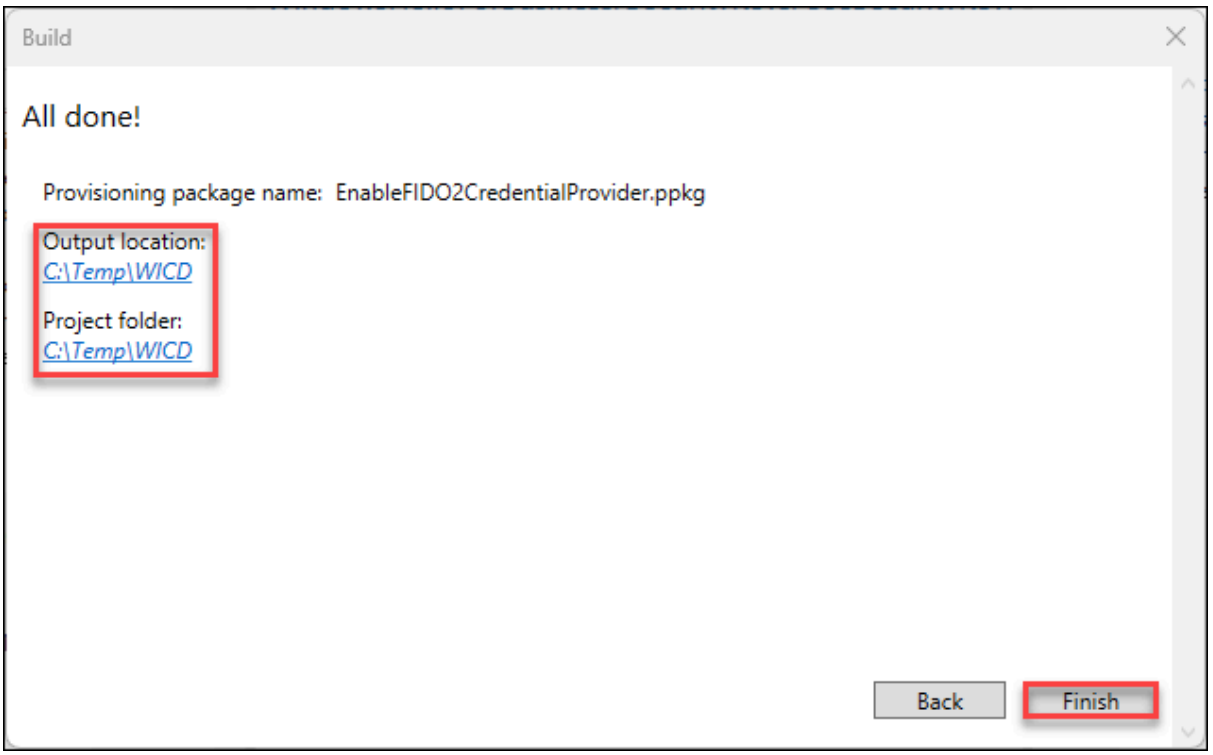


12. Select **Build** on the **Build the provisioning package** page.



© Yubico 2025

13. Note the **Output** and **Project folder** locations and select **Finish**.



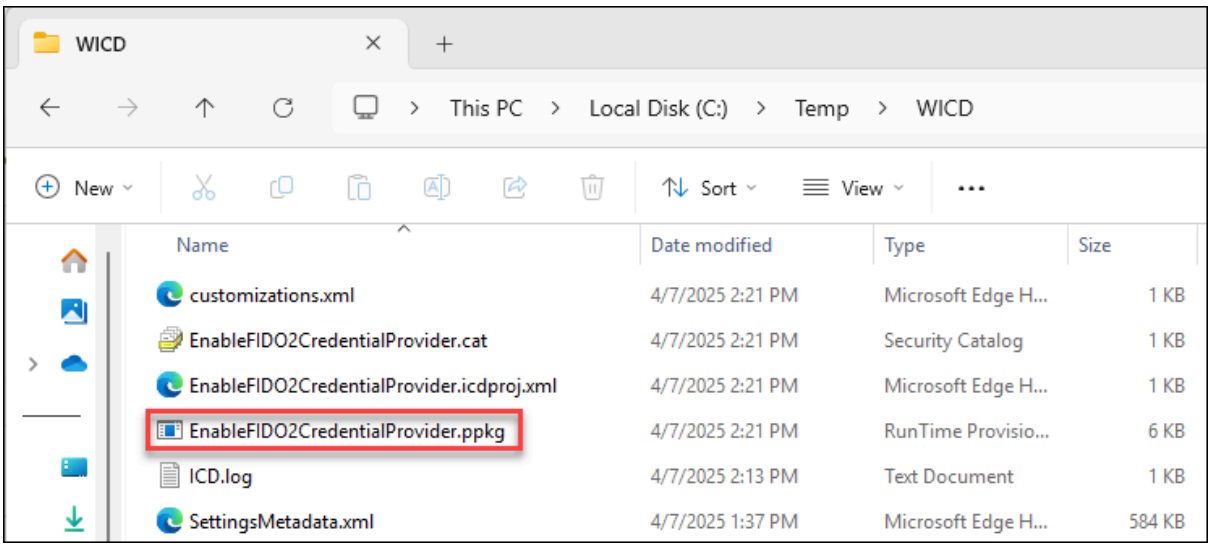
14. Save the two files created (.ppkg and .cat) to a location where you can apply them to machines later.

© Yubico 2025

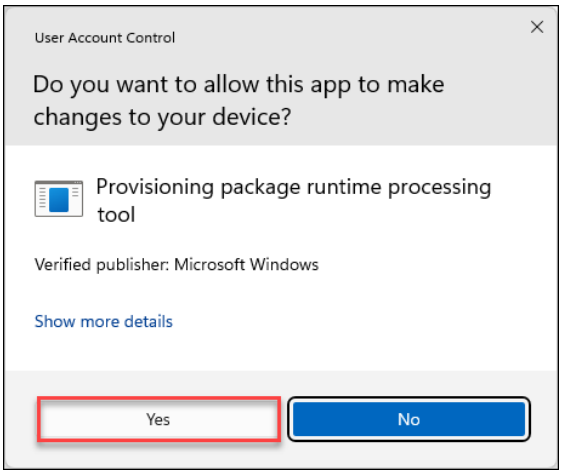
Apply a provisioning package

Applying a provisioning package to a desktop device requires administrator privileges on the device. Microsoft provides multiple methods to apply a provisioning package. The following steps show only one of the available methods. Refer to the official Microsoft guidance for alternate methods for applying a provisioning 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.

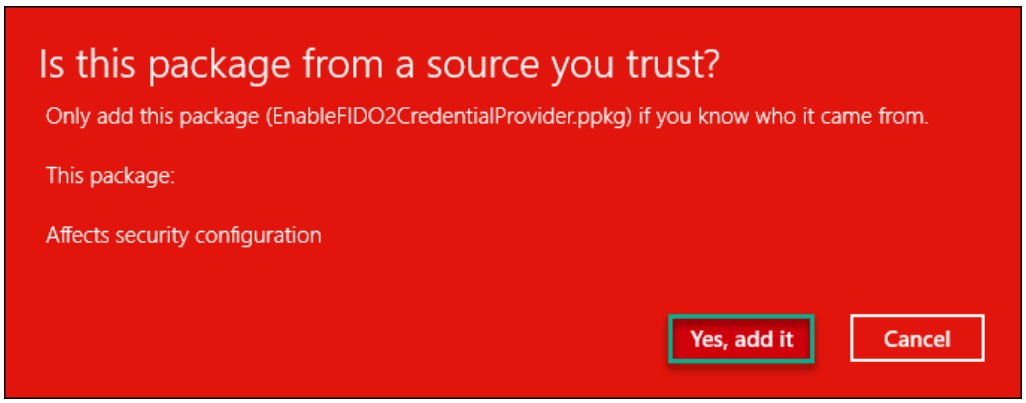


3. Select **Yes** to allow the app to make changes.



© Yubico 2025

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



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 and 11 device should now be enabled with a security key option. Refer to the **"User Enablement Guide"** section for expected results.

yubico

Option 2: Intune method

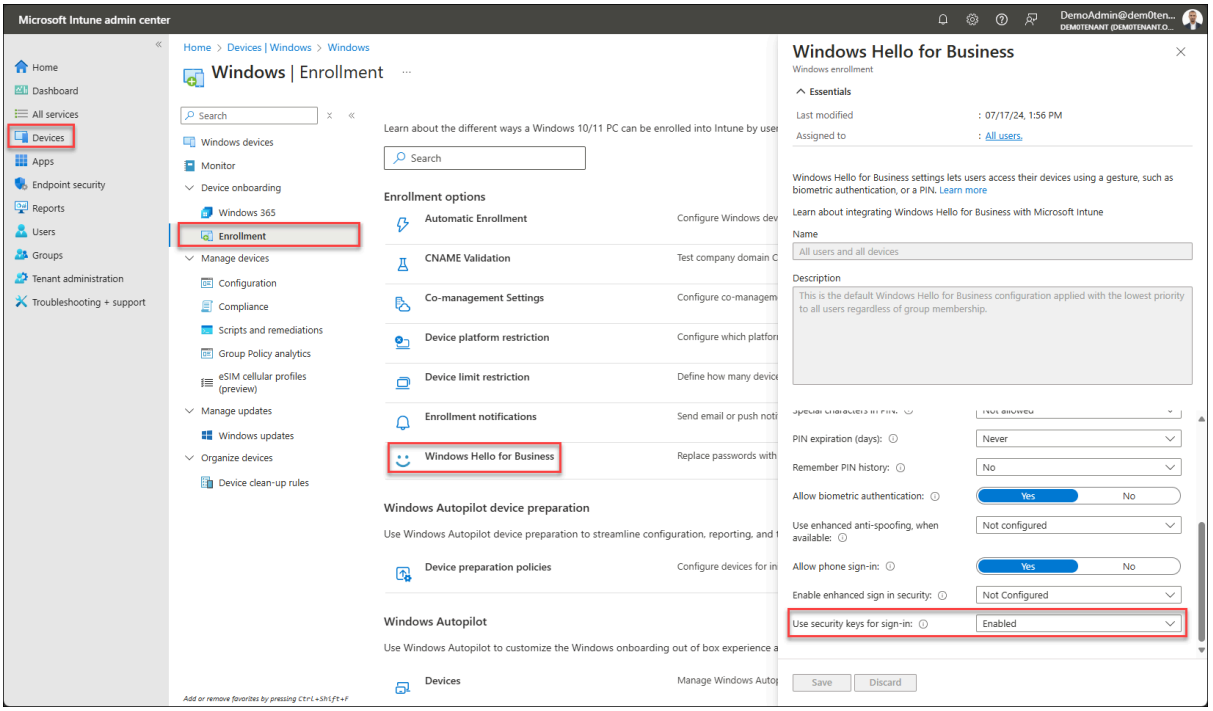
Intune provides multiple options for enabling the lock screen to use security keys on Windows 10 and 11 devices. Two different methods are described below. One method will describe how to enable the setting for all users' devices, and the other method will describe how to apply the setting for targeted 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 Admin Center**: https://intune.microsoft.com
2. Browse to **Devices** and expand **Device Onboarding**:
    a. Select **Enrollment**
    b. Select **Windows Hello for Business** under the Enrollment options
    c. In the Windows Hello for Business options pane:
        i. Select **Enabled** in the **Use security keys for sign-in** drop-down menu
        ii. Click **Save**

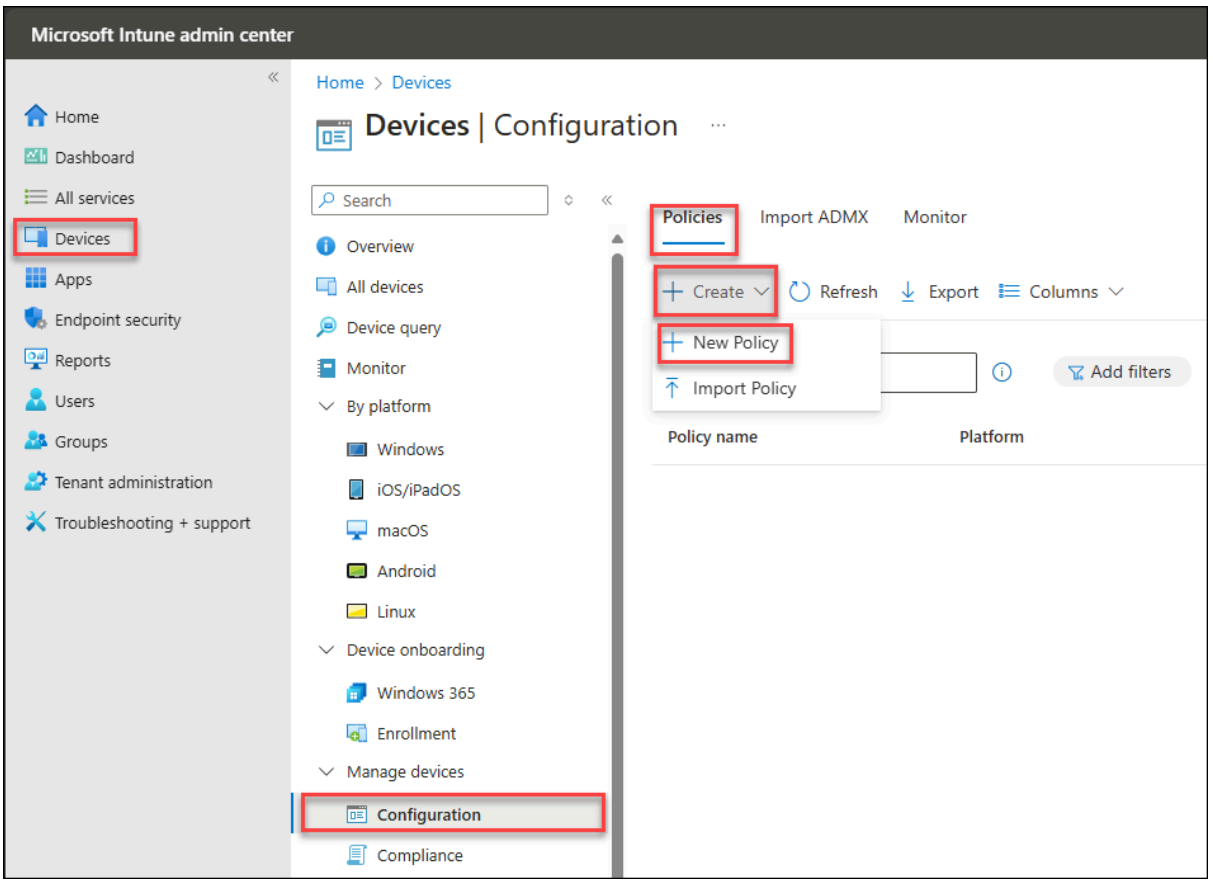
Note: Configuration of security keys for sign-in isn't dependent on configuring Windows Hello for Business.



Option 2b: Targeted Intune deployment

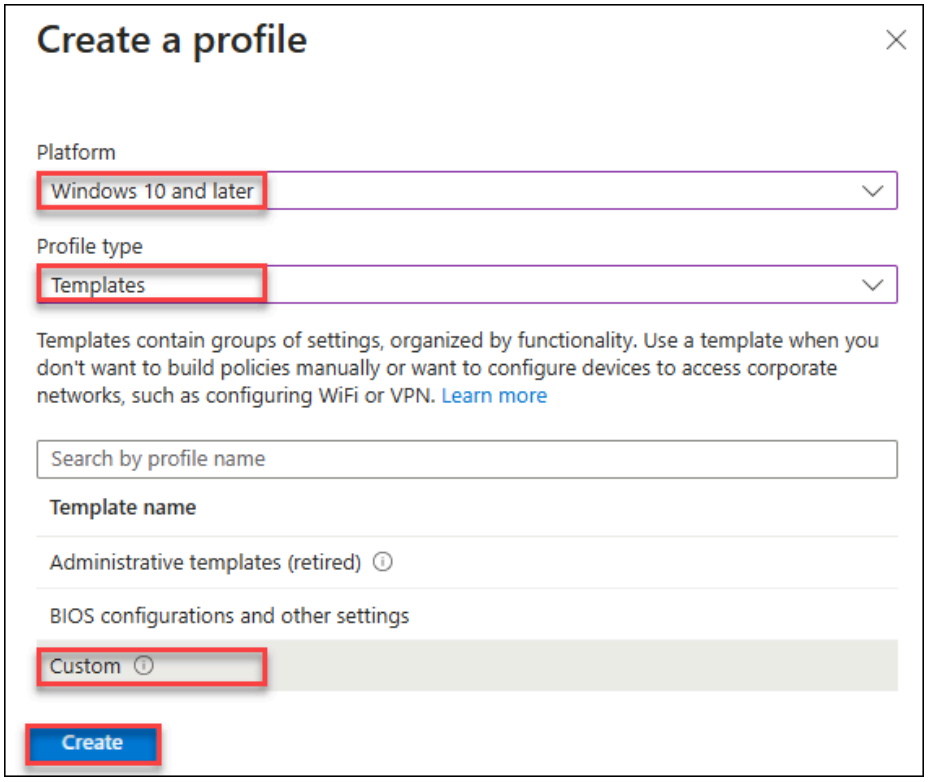
To enable the use of security keys for select user groups and select devices, complete the following steps:

1. Sign in to the **Intune Admin Center:** https://intune.microsoft.com/.
2. In the menu pane on the left, select **Devices**
3. Expand **Manage Devices**, select **Configuration**
4. Under **Policies**, select **Create** from the drop-down menu and select **New Policy**

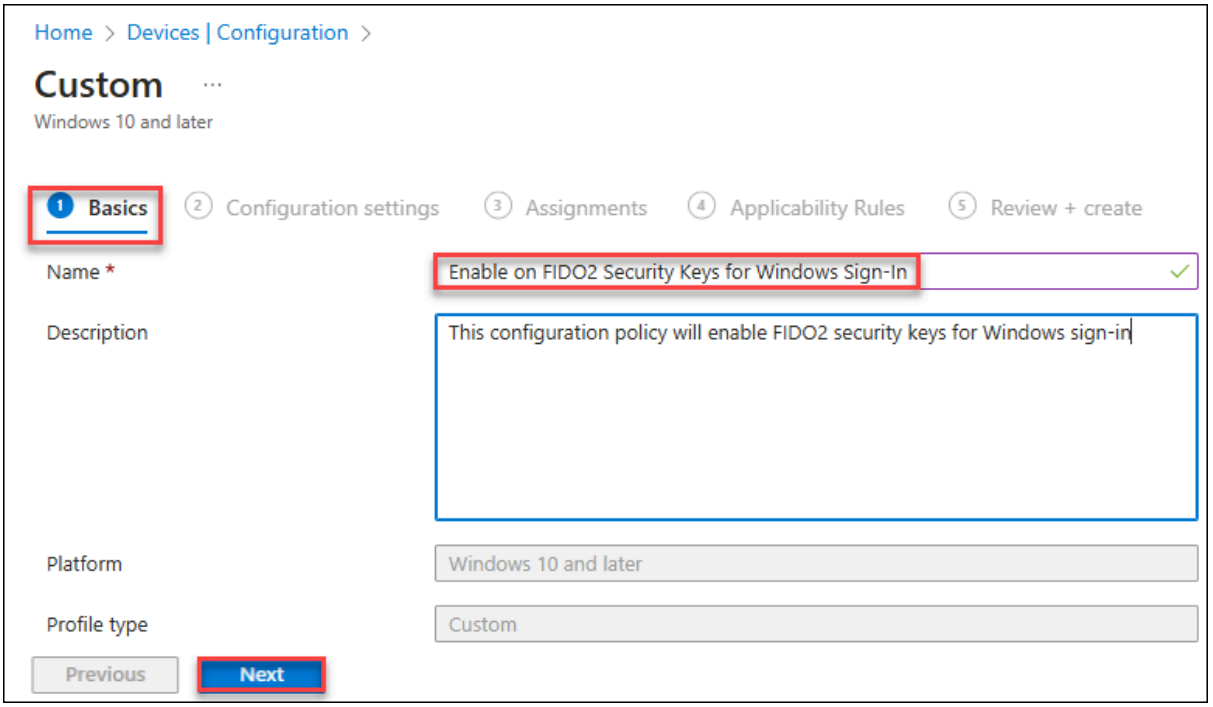


© Yubico 2025

5. In the **Create a profile** section, configure the following settings:
    a. In the **Platform** drop-down menu select **Windows 10 and later**
    b. In the **Profile** type drop-down menu select **Templates**
    c. Under **Template** name, select **Custom**
    d. Click **Create**

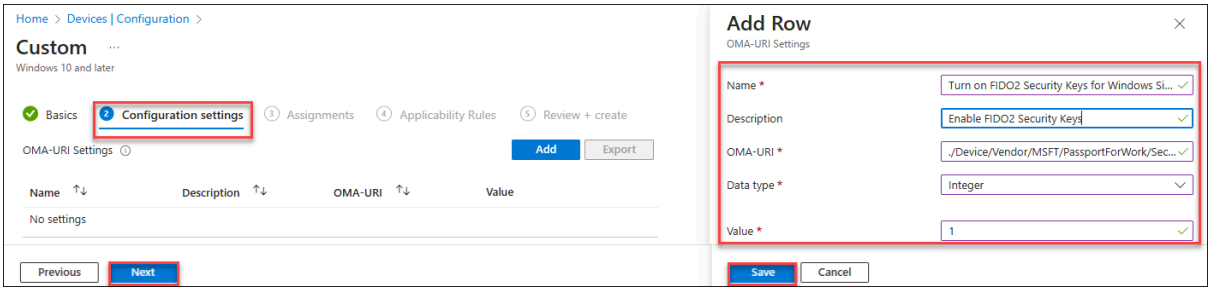


6. In the **Basics** section add a **Name** and optional description and click **Next**

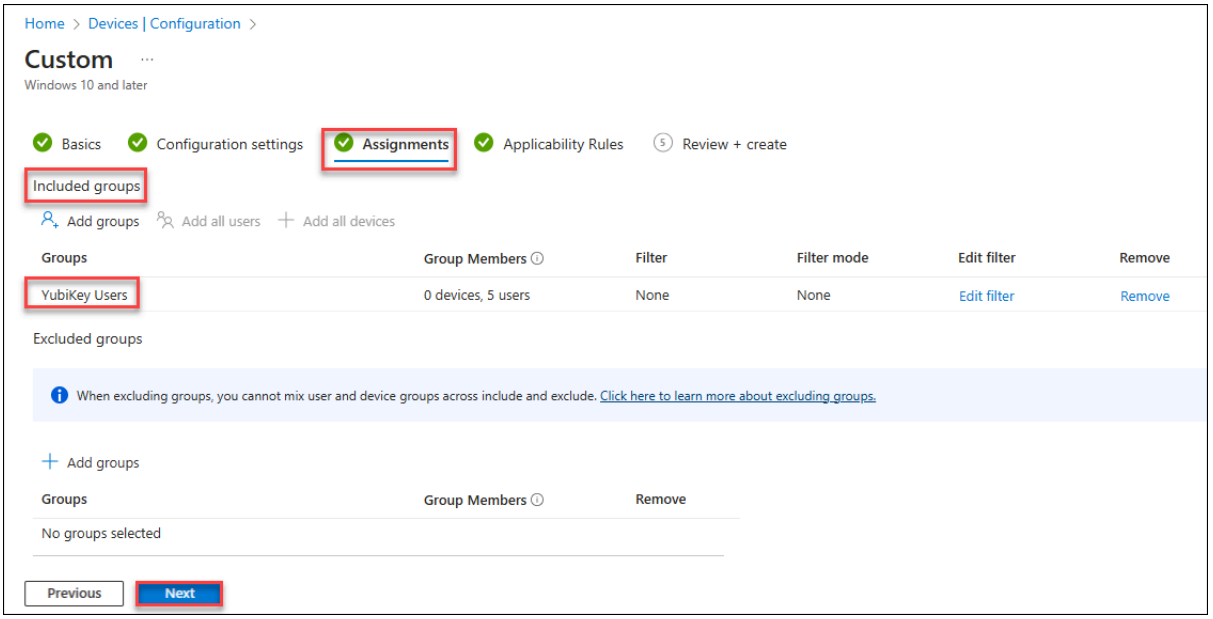


© Yubico 2025

7. Under **Configuration settings**, select **Add** and configure the settings below:
    a. **Name: Turn on FIDO Security Keys for Windows Sign-In**
    b. **Description: Enables FIDO Security Keys to be used during Windows Sign In**
    c. **OMA-URI:./Device/Vendor/MSFT/PassportForWork/SecurityKey/UseSecurityKeyForSignin**
    d. **Data: Type: Integer**
    e. **Value:1**
    f. Click **Save**
    g. Click **Next**



8. In the Assignments settings, select the Groups, Users and Devices this policy will apply to and click **Next**



9. Select **Next** under **Applicability Rules**.
10. Select **Create** under **Review + Create**
11. The configuration policy should be enabled now for the users and devices that you selected.

Note: After assigning an Intune policy it may take some time for the policy to propagate and apply to targeted devices. Devices must check in with the Intune service to receive the updated policy, which typically occurs during the next sync interval. You can initiate a manual sync from the device or Intune portal to expedite this process. For more information, refer to official Microsoft guidance.

Once the policy has been successfully applied, the Windows 10/11 lock screen will display the option to sign-in with a security key. Refer to the **User Enablement Guide** section for expected results.

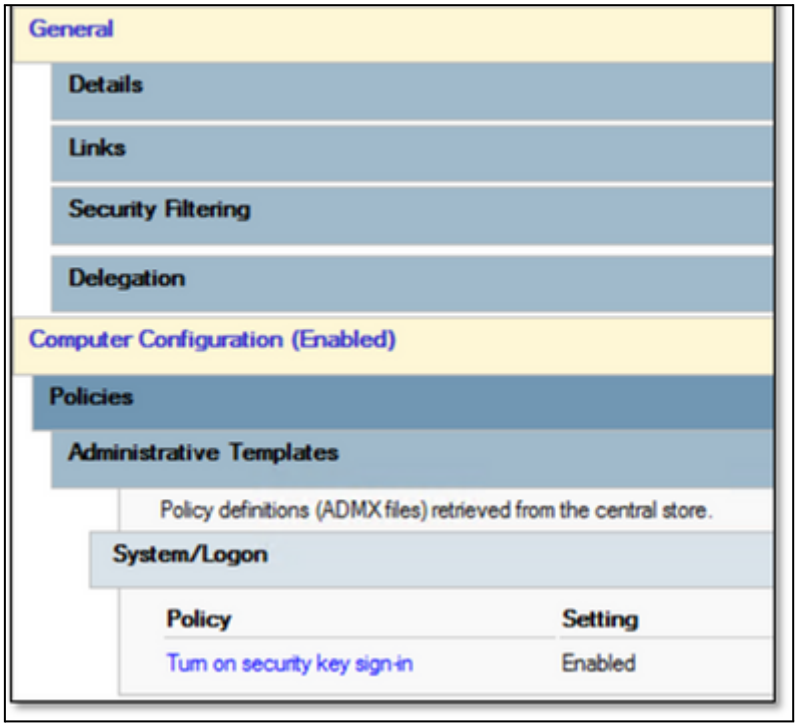
© Yubico 2025

Option 3: Group policy method

For Entra hybrid Entra ID joined devices, organizations can use Group Policies to enable FIDO2 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:
    a. **Computer Configuration** >**Administrative Templates** > **System** > **Logon** > **Turn on security key sign-in**:



3. Associate the GPO to the appropriate OU's containing the targeted Windows 10 and 11 devices.
4. Once the policy has been successfully applied, the Windows 10 and 11 lock screen will display the option to sign-in with a security key. Refer to the **User Enablement Guide** section for expected results.

© Yubico 2025

Supported vs Unsupported Scenarios

The following information is accurate as of March 2025. Microsoft plans to evolve support for passkey (FIDO2) authentication within their ecosystem.

- Passkey (FIDO2) authentication is unsupported in the following scenarios:
  - Signing-in to a server using a security key
  - RunAs using a security key
  - S/MIME using a security key
  - Windows Server Active Directory Domain Services (AD DS) domain-joined (on-premises only devices) deployment.
- Passkey (FIDO2) authentication is supported in the following scenarios:
  - Cloud resources such as Microsoft 365 and other SAML enabled applications
  - On-premises resources and Windows-integrated authentication to websites when the device is Entra joined or Entra Hybrid joined
  - Access over Remote Desktop Protocol (RDP) under the following conditions:
    - The remote device needs to be Entra joined or Entra hybrid joined
      - Session host and local PC are using supported operating systems
      - Please refer to the **Remote Desktop Guide** for detailed guidance
- For third party VDI support, please refer to the official vendor documentation
- After 14 days of being completely offline, a Microsoft Entra joined device will likely prevent sign-in with Microsoft Entra credentials because the cached Primary Refresh Token (PRT) will have expired. An internet connection will be required to re-authenticate and obtain a new PRT.

Known Issues

- For Windows device sign-in:
  - If multiple Passkey (FIDO2) credentials are loaded on a FIDO2 Security Key, only one FIDO2 credential will be selected for authentication during Windows device login. The last registered FIDO2 credential will be automatically selected.
  - If your password has expired, signing in with FIDO2 is blocked. The expectation is that users reset their passwords before they can log in by using FIDO2.
- For Windows device sign-in on hybrid devices:
  - The default security policy doesn't grant Microsoft Entra permission to sign high privilege accounts on to on-premises resources.
  - If you're clean-installing a Microsoft Entra hybrid joined machine, after the domain join and restart process, you must sign in with a password and wait for the policy to sync before you can use the FIDO2 security key to sign in.
    - This delay in syncing is a known limitation of domain-joined devices and isn't FIDO2-specific.
  - If you receive requests for credential prompts when accessing on-premises resources over SSO, ensure that enough DCs are patched to and available to respond in time to service resource requests.
  - A FIDO2 Windows login requires at least one writable DC to exchange for a TGT exchange.
- For browser-based sign-in, the pick list is limited to displaying up to 20 passkeys on Windows devices.

© Yubico 2025

Appendix A - Microsoft Azure Licensing

The table below highlights the Microsoft Entra Licensing requirements to deploy Entra Passwordless sign-in with passkeys (FIDO) on 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
Entra ID	✔	✔	✔	✔	
Azure Multi-Factor Authentication	✔	✔	✔	✔	
Microsoft Licenses for Passwordless Single Sign On					
Combined Security Registration	✔	✔	✔	✔	
Passkey (FIDO2 Security Key	✔	✔	✔	✔	
Microsoft Licenses for Entra Joined Windows 10/11 Passwordless Sign On					
Windows 10 1909+	✔	✔	✔	✔	Windows 10/11 License
(Optional) Microsoft Intune		✔	✔	✔	Microsoft Intune License
(Optional) Provisioning Packages	✔	✔	✔	✔	
Microsoft Licenses for Entra Hybrid Joined Windows 10/11 Passwordless Sign On					
Windows 10 2004+	✔	✔	✔	✔	Windows 10/11 License
Windows Server 2016 and/or 2019	✔	✔	✔	✔	Windows Server License
Entra 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. Entra ID pricing:
https://www.microsoft.com/en-ca/security/business/microsoft-entra-pricing
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

© Yubico 2025