# YubiKeys for Entra ID passwordless admin deployment guide

#### 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 <u>yubi.co/contact</u>

#### **Original Document Release Date**

September 22, 2020

#### Version History

Version	Date	Changes
2.4	May 20, 2025	<ul> <li>Updated with Entra branding</li> <li>Introduced passkey terminology</li> <li>Added references for Windows 11</li> <li>Updated guidance to include enforcing attestation and key restrictions</li> <li>Added enabling and configuring passkey (FIDO2) authentication policy using PowerShell</li> <li>Added instructions to generate a TAP using PowerShell</li> <li>Added expected results table for successful TAP generation</li> <li>Updated permission requirements</li> <li>Added expected results table for successful Entra Kerberos configuration</li> <li>Updated instructions for Intune</li> <li>Added operating system support for remote desktop</li> <li>Updated licensing link</li> </ul>
2.3	May 8, 2023	<ul> <li>Added TAP and associated caveats.</li> <li>Reference links to Conditional Access and deployment flows. Status update on mobile support.</li> </ul>
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

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

## 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 <u>FIDO2 security key sign-in isn't</u> 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: <u>Supported-scenarios</u> Learn more about different Entra ID user types <u>here</u>

## **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 <u>Appendix A</u>. *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)
  - <u>Security Key Series (includes Enterprise Edition)</u>

## Software

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

## 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

## 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.

Microsoft	
to continue to Microsoft Entra Email, phone, or Skype	
No account? Create one! Can't access your account?	
	Next
Sign in with GitHub	
Sign-in options	

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)

Microsoft Entra admin center		d docs (G+/)		🚺 Copilot 🗳 🕸 🕐 🕅	and the second second
A Home	Home >				
	🔥 Authentication meth	nods   Policies			×
What's new	Demo - Microsoft Entra ID Security				
Diagnose & solve problems		+ Add external method (Preview) 🕐	Refresh 🛛 🛜 Got feedback?		
	Manage	Authentication method policies			
★ Favorites	Policies	Use authentication methods policies to cont	figure the authentication methods your u	isers may register and use. If a user is in	
Identity	Password protection	scope for a method, they may use it to auth scenarios). Learn more	enticate and for password reset (some m	ethods aren't supported for some	
() Quantique	😼 Registration campaign	Method	Tarriet	Enabled	
- Overview	Authentication strengths	N C Bulle In	niger	LINDICU	
A Users	V 🏶 Settings	V Built-in	411	16-	
<sup>ሳ</sup> ጸ <sup>8</sup> Groups	✓ Monitoring	Passkey (FIDO2)	All users	Tes	
E Devices	🗸 👬 Activity	Microsoft Authenticator	All users	1es	
	User registration details	Temporani Access Pass	All usars	Vac	
A protection	Registration and reset events	Hardware OATH tokens (Preview)	All BCTS	No	
Protection	Bulk operation results	Third-party software OATH tokens	All users	Yes	
Identity Governance	~	Voice call		No	
ତ୍ମି External Identities	$\sim$	Email OTP	All users	Yes	
··· Show more		Certificate-based authentication		No	
	-	QR code (Preview)		No	
2. Protection	^				
Authentication methods					
Password reset					
E Custom security attributes					
channen and					
Stownore	*				
🚨 Learn & support	^				
	~				

- 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

Home > Authentication methods   Policies > Passkey (FIDO2) settings > U	sers > Authentication methods   Policies >		
Passkey (FIDO2) settings			$\times$
Passkeys are a phishing-resistant standards-based passwordless authentication m	ethod available from a variety of vendors. Learn more		
Passkeys 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	Туре	Registration	
YubiKau Tert Group	Group	Ontional	$\mathbf{\mathbf{x}}$
Tubikey lest droup	Gloup	Optional	
Save Discard			

- 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)

Home > What's new > Authentica	ation methods   Policies >	
Passkey (FIDO2) set	tings …	×
	-	
Passkeys are a phishing-resistant, stan Passkeys are not usable in the Self-Se	ndards-based passwordless authentication method available from a variety of vendors. Learn more. rvice Password Reset flow.	
Enable and Target	]	
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	
Microsoft Authenticator 🕕		
Add AAGUID		
No AAGuids have been added.		
Save Discard		
Discard		

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 <u>ykman CLI</u> by running the command: *ykman fido info*. The full list of YubiKey AAGUIDs is referenced in the <u>YubiKey hardware FIDO2</u> <u>AAGUIDs support article</u>. You can also verify the AAGUID on your YubiKey using the <u>Retrieve a YubiKey AAGUID</u> support article.
  - ii. Click Ok.
- e. Click **Save** to enable the policy.

Home > Authentication methods   Policies > Passkey (FIDO2) settings > Users > Authentication methods   Policies >	Add AAGUID ×
Passkey (FIDO2) settings	
Passkey (FIDO2) settings          Passkeys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. Learn more.         Passkeys are not usable in the Self-Service Password Reset flow.         Enable and Target       Configure         GENERAL         Allow self-service set up       Vs         Enforce attestation       Vs         KEY RESTRICTION POLICY         Enforce key restrictions         Microsoft Authenticator         Add AGGID         d7781e5d-e353-46aa-afe2-3ca49f13332a	Which AAGUID would you like to add?
Save Discard	Ok Cancel

## 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:

```
$AAGUIDs = @("d7781e5d-e353-46aa-afe2-3ca49f13332a")
Connect-MgGraph -Scopes "Policy.ReadWrite.AuthenticationMethod"
$params = @{
   state
                                    = @ (
   includeTargets
       @ {
           targetType = "group"
   excludeTargets
                                    = @ (
   isSelfServiceRegistrationAllowed = $true
    isAttestationEnforced
                                    = @{
    keyRestrictions
       isEnforced = $true
       enforcementType = "Allow"
       aaGuids = $AAGUIDs
figuration -AuthenticationMethodConfigurationId "Fido2"
-BodyParameter $params
```

## **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.

Home > Authentication methods   Polici	es > Passkey (FIDO2) settings > Users >			
Authentication met	hods   Policies			×
₽ Search «	+ Add external method (Preview) 💍 Refres	ih 🛛 🖗 Got feedback?		
Manage				
Policies	Authentication method policies	the authentication methods your users	may register and use. If a user is in	
Password protection	scope for a method, they may use it to authentica	ite and for password reset (some metho	ds aren't supported for some	
📙 Registration campaign	scenarios), Learn more			
Q Authentication strengths	Method	Target	Enabled	
Settings	∨ Built-In			
Monitoring	Passkey (FIDO2)	1 group	Yes	
A A ARIAN	Microsoft Authenticator	All users	Yes	
Activity	SMS		No	
User registration details	Temporary Access Pass		No	
Registration and reset events	Hardware OATH tokens (Preview)		No	
Bulk operation results	Third-party software OATH tokens	All users	Yes	
	Voice call		No	
	Email OTP	All users	Yes	
	Certificate-based authentication		No	
	QR code (Preview)		No	

- 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

Home > Authentication methods   Policies > Passkey (FIDO2) setting	gs > Users > Authentication methods   Policies >		
Temporary Access Pass settings			×
······································			
Temporary Access Pass, or TAP, is a time-limited or limited-use passcode th TAP is issuable only by administrators, and is seen by the system as strong a	at can be used by users for bootstrapping new accounts, acco authentication. It is not usable for Self Service Password Reset.	unt recovery, or when other auth methods are unavailable. Learn m	ore.
Enable and Target Enable			
Include         Exclude           Target         All users         Select groups			
Add groups			
Name	Туре	Registration	
YubiKey Test Group	Group	Optional	$\sim$ X

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.

Home > Authentication methods   Po	olicies > Passkey (FIDO2) settings > Users > Authentication methods   Policies >	Temporary Access Pass settings $\times$
Temporary Access Pas	ss settings	, , , , , , , , , , , , , , , , , , , ,
Temporary Access Pass, or TAP, is a time- TAP is issuable only by administrators, ar	- limited or limited-use passcode that can be used by users for bootstrapping new accounts, account recovery, or when Id is seen by the system as strong authentication. It is not usable for Self Service Password Reset.	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
Enable and Target		Minimum lifetime O Minutes 💿 Hours O Days
GENERAL		0 1 hour
Minimum lifetime:	1 hour	Maximum lifetime
Maximum lifetime:	a hours	🔿 Minutes 💿 Hours 🔿 Days
One-time:	No	8 hours
Length:	8 characters	Default lifetime Minutes  Hours Days
		Length (characters) * 8
		Require one-time use
Save Discard		Update Cancel

## 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

Erin Engineer   Authentication methods          User          Ø Search          Authentication method          Sign-in logs          Diagnose and solve problems       Default sign-in method (Preview) ()       No default ?         Custom security attributes       Usable authentication methods         Administrative units           Applications           Licenses           Provices           Authentication methods.           System preferred multifactor authentication method          Authentication methods.           Authentication methods.           System preferred multifactor authentication method <th>Choose method Temporary Access Pass Create a Temporary Access Pass for Erin Engineer. While the pass is valid, the user can use it to sign in and register strong credentials. Learn more Delayed start time</th>	Choose method Temporary Access Pass Create a Temporary Access Pass for Erin Engineer. While the pass is valid, the user can use it to sign in and register strong credentials. Learn more Delayed start time
User	Choose method Temporary Access Pass Create a Temporary Access Pass of Erin Engineer. While the pass is valid, the user can use it to sign in and register strong credentials. Learn more Delayed start time
Authentication methods are the ways users sign into Microsoft Entra ID and perform the users 'default sign-in method' is the first one shown to the user when they a second factor - the user always can choose another registered, enabled authentication is a sign-in logs     Diagnose and solve problems     Default sign-in method (Preview) ① No default      Default sign-in method (Preview) ① No default      Default sign-in method     Administrative units     Authentication methods     Administrative units     Authentication method     No usable authentication methods     Authentication method     No-usable authentication methods     Authentication method     Devices     No non-usable methods.     System preferred multifactor authentication method	n § ref create a Temporary Access Pass for Erin Engineer. While the pass is valid, the user can use it to ior sign in and register strong credentials. Learn more Delayed start time
Licenses     Authentication method      Devices     No non-usable methods.      Azure role assignments     System preferred multifactor authentication method	Activation duration () One-time use Ves No
Devices     No non-usable methods.      Azure role assignments     System preferred multifactor authentication method	
Azure role assignments     System preferred multifactor authentication method	
R New support request Feature status System preferred MFA method	
Enabled	

- 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

Home > Users > Erin		Temporary Access Pass details	
<b>Erin</b>   Authentication	n methods		
✓ Search «	+ Add authentication method 🔰 🖉 R	Provide Pass Provide this Temporary Access Pass to the user so they can set their strong credentials.	
🚨 Overview	Authentication methods are the ways users s	WK-7=-N+	
<ul> <li>Audit logs</li> <li>Sign-in logs</li> </ul>	service password reset (SSPR). The user's 'de user when they are required to authenticate another registered, enabled authentication m	Secure registration To register their credentials, have the user go to My Security Info.	
🗙 Diagnose and solve problems	Default sign-in method (Preview) 🕕	https://aka.ms/mysecurityinfo	
Custom security attributes	Usable authentication methods	Additional information	
Sector Assigned roles	Authentication method	Valid from 4/5/2025, 10:13:16 PM	
Administrative units	Temporary Access Pass	Valid until 4/5/2025, 11:13:16 PM	
Groups Applications	Non-usable authentication methods	Created 4/5/2025, 10:13:16 PM	
Licenses	Authentication method	Remove lost devices from the user's account. This is especially important for devices	
Devices	No non-usable methods.	used for user authentication.	
<ul> <li>Azure role assignments</li> <li>Authentication methods</li> </ul>	System preferred multifactor authentic		
R New support request	Feature status System		
	Enabled No syste		
			•
		Ok	

#### **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:



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 <u>Microsoft documentation</u>.

## 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 <u>Microsoft documentation</u>.

## 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 PowerShel
Install-Module -Name AzureADHybridAuthenticationManagement
```

-AllowClobber

## 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. \$et-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) 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

## 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 <u>Microsoft Store</u>. 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\WICD Browse	
Description: This provisioning package will enable the FIDO2 sign-in option for Windows 10 and 11	7
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.

New project	×
Choose which settings to view and configure	^
O All Windows editions	
All Windows desktop editions	
<ul> <li>All Windows mobile editions</li> </ul>	
O Windows 10 IoT Core	
O Windows 10 Holographic	
O Windows 10 Holographic (HoloLens 2)	
<ul> <li>Common to Windows 10 Team edition</li> </ul>	
Selecting this option will display settings that are specific to the desktop editions as well as settings that are common to all Windows editions.	
Back Next	

#### 6. Select Finish.

New project		×
Import a provisioning package (optional)	Browse	]
Back	Finish	, ,

- 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

🖙 Windows Configuration Designer				- 🗆 X
File 🖌 About 🖌 🚺 Export 🖌				
Start page EnableFIDO2CredentialProvi	der 🗙			
Start page EnableFIDO2CredentialProvi Available customizations View: All settings Search ProvisioningCommands SharedPC SMISettings Start StorageD3InModernStandby TabletMode TakeATest TenantDefinedTelemetry Time UnifiedWriteFilter UniversalAppUninstall UniversalAppUninstall UniversalAppUninstall UniversalAppUninstall UniversalAppUninstall UniversalAppUninstall Starters Biometrics PoliciesForAllTenants PoliciesForTenant SecurityKeys Starters Starters Starters PoliciesForTenant SecurityKeys Starters	der X WindowsHelloForBusi UseSecurityKeyForSignin	ness/SecurityKey:	s/UseSecurityKeyF	Selected customizations  A Runtime settings  WindowsHelloForBusiness  SecurityKeys UseSecurityKeyForSignin
Version: 2025 225 0.0+3f6f0e308809e6f7adcafa	186e028fac489f4e01_Cus	tomizations () Invalid	Project: Provisioning p	ackage Edition: All Windows desktop:
			riojecu riovisioning p	

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

Windows Configuration Designer			
File 🖌 About 🖌	🔀 Export 🖌		
Start page	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:	Version (in Major.Minor format)
679249bd-8e02-4a8b-aaa9-6be093595b8c	1.0
Owner:	Rank (between 0 - 99):
OEM ~	0
	Next

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:		
	Browse	
Back	Next	, ,

\_

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

Build	$\times$
Select where to save the provisioning package	^
C:\Temp\WICD\EnableFIDO2CredentialProvider.ppkg Browse	
Back	
	• ~)

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

$\sim$

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.

#### 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 <u>Microsoft guidance</u> 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.

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					
Show more details					
Yes No					

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				
Yes, add it Cancel				

- 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.

## **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.

Microsoft Intune admin center				Q	영 ⑦ & DemoAdmin@dem0ten 🐢
« home	Home > Devices   Windows > Windows	nt	Windows Hello for Bu Windows enrollment	usiness ×	
Dashboard     All services     Devices     Apps	Search X «     Windows devices	Learn about the different ways a Windows 10/	11 PC can be enrolled into Intune by user	<ul> <li>Essentials</li> <li>Last modified</li> <li>Assigned to</li> </ul>	: 07/17/24, 1:56 PM : <u>All users</u> .
Endpoint security      Reports      Users	Monitor  Device onboarding  Windows 365  Compared to the second	Enrollment options	Configure Windows dev	Windows Hello for Business settings lets biometric authentication, or a PIN. Learr Learn about integrating Windows Hello Name	s users access their devices using a gesture, such as n more for Business with Microsoft Intune
Groups Tenant administration	Manage devices     Configuration	CNAME Validation	Test company domain C	All users and all devices Description	
🗙 Troubleshooting + support	Compliance     Scripts and compdiations	Co-management Settings	Configure co-managem	This is the default Windows Hello for E to all users regardless of group memb	Business configuration applied with the lowest priority ership.
	Group Policy analytics     Group Reliance profiles	Device platform restriction	Configure which platfor		
	I≡ esim central promes (preview) ✓ Manage updates	Enrollment notifications	Send email or push noti	ареканская кнагаккета на еник. 🕓	
	<ul> <li>Windows updates</li> <li>Organize devices</li> <li>Device devices</li> </ul>	U Windows Hello for Business	Replace passwords with	PIN expiration (days): ① Remember PIN history: ①	No V
	E Device deam-up rules	Windows Autopilot device preparation		Allow biometric authentication: ① Use enhanced anti-spoofing, when	Yes No
		Use Windows Autopilot device preparation to  Device preparation policies	streamline configuration, reporting, and 1 Configure devices for in	available: 💿 Allow phone sign-in: 💿	Ves No
		Windows Autopilot		Enable enhanced sign in security: ① Use security keys for sign-in: ①	Not Configured V
		Use Windows Autopilot to customize the Wind	dows onboarding out of box experience a		
	Add or remove favorites by pressing CtrL+Shift+F	Devices	Manage Windows Auto;	Save Discard	

#### 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: <u>https://intune.microsoft.com/</u>.
- 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

Microsoft Intune admin center			
×	Home > Devices		
숚 Home	📺 Devices   Configura	ation	
📶 Dashboard			
E All services		Policies Import ADMX	Monitor
Devices	() Overview		
Apps	All devices	+ Create 🗸 🖒 Refresh	🛓 Export ᠄ Columns 🗸
퉋 Endpoint security	🦻 Device query	+ New Policy	
Reports	Monitor	The Import Policy	i) 😨 Add filters
🙎 Users	✓ By platform	In import Policy	
A Groups	Windows	Policy name	Platform
Tenant administration	iOS/iPadOS		
🗙 Troubleshooting + support	🖵 macOS		
	Android		
	🦲 Linux		
	$\checkmark$ Device onboarding		
	🗊 Windows 365		
	👩 Enrollment		
	✓ Manage devices		
	Configuration		
	Compliance		

- 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

Create a profile ×
Platform
Windows 10 and later V
Profile type
Templates V
don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more
Template name
Administrative templates (retired) ①
BIOS configurations and other settings
Custom ①
Create

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

Home > Devices   Configuration >	
Custom Windows 10 and later	
Basics     Configuration setti	ngs ③ Assignments ④ Applicability Rules ⑤ Review + create
Name *	Enable on FIDO2 Security Keys for Windows Sign-In
Description	This configuration policy will enable FIDO2 security keys for Windows sign-in
Platform	Windows 10 and later
Profile type	Custom
Previous Next	

- 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

Home > Devices   Configuration > Custom	Add Row OMA-URI Settings	×
Windows 10 and later	Name *	Turn on FIDO2 Security Keys for Windows Si 🗸
Basics Configuration settings 3 Assignments 4 Applicability Rules 5 Review + create	Description	Enable FIDO2 Security Keys
OMA-URI Settings () Add Export	OMA-URI *	./Device/Vendor/MSFT/PassportForWork/Sec </th
Name <sup>↑</sup> ↓ Description <sup>↑</sup> ↓ OMA-URI <sup>↑</sup> ↓ Value	Data type *	Integer V
No settings	Value *	1
Previous Next	Save Cancel	

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

Home > Devices   Configuration >							
Custom Windows 10 and later							
Basics Configuration settings Assignments Applicability Rules      Applicability Rules      Applicability Rules     Applicability Rules     Applicability Rules     Applicability Rules							
Groups	Group Members 🛈	Filter	Filter mode	Edit filter	Remove		
YubiKey Users	0 devices, 5 users	None	None	Edit filter	Remove		
Excluded groups							
When excluding groups, you cannot mix user and device	When excluding groups, you cannot mix user and device groups across include and exclude. <u>Click here to learn more about excluding groups</u> .						
+ Add groups							
Groups	Group Members 🛈	Remove					
No groups selected							
Previous							

- 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 <u>Microsoft guidance</u>.

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.

## 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:

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							
	Tum on security key sign-in Enabled							
_								

- 3. Associate the GPO to the appropriate OU's containing the targeted Windows 10 and 11 devices.
- 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.

## **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 <u>unsupported</u> 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 <u>supported</u> 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
  - $\circ$   $\;$  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 <u>supported operating</u> <u>systems</u>
      - 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.

## **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	FREE⁵	M365	PREMIUM P1	PREMIUM P2	Other Required Licenses
Entra ID	~	~	~	~	
Azure Multi-Factor Authentication	~	~	~	v	
Microsoft Licenses for Pass	wordles	s Sing	le Sign On	•	
Combined Security Registration	~	~	~	~	
Passkey (FIDO2 Security Key	~	~	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	
Microsoft Licenses for Entra	Joined	Windo	ows 10/11 Pass	wordless Sign	On
Windows 10 1909+	~	~	<ul> <li>✓</li> </ul>	<ul> <li>✓</li> </ul>	Windows 10/11 License
(Optional) Microsoft Intune		~	~	~	Microsoft Intune License
(Optional) Provisioning Packages	~	~	V	~	
Microsoft Licenses for Entra	Hybrid	Joined	d Windows 10/ <sup>,</sup>	11 Passwordles	ss Sign On
Windows 10 2004+	~	~	~	~	Windows 10/11 License
Windows Server 2016 and/or 2019	~	~	~	~	Windows Server License
Entra Connect	~	~	~	<ul> <li>✓</li> </ul>	
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