YubiKeys for Entra ID passwordless enforce YubiKeys for Entra ID sign in

yubico

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

March 25, 2025

Version History

Version	Date	Changes
1.0	May 22, 2025	Initial Release

Copyright		
Trademarks	÷	
Disclaimer		
Contact Information		
Original Document Release Date		
Version History		
Introduction		
Before you begin	1	
Minimum requirements	5	
Create an authentication strength control	6	
Option 1: Using Entra Admin Portal	6	
Option 2: Create Authentication Strength Using Microsoft Graph Powershell Module	9	
Create a Conditional access policy	10	
Option 1: Using the Entra admin portal	10	
Option 2: Create Conditional Access Policy Using Microsoft Graph Powershell SDK	13	
Testing the policy	14	
Scenario 1: Step-up Authentication - User has already registered approved YubiKey a	ind	
begins sign-in with a password	15	
Scenario 2: User is MFA Incapable and begins sign-in with password	19	
Scenario 3: MFA Capable - Signing-in with MFA using an approved security key	20	
Scenario 4: User is MFA Capable and begins sign-in with MFA and tries register an		
unapproved security key	27	

Introduction

This document provides guidance on enforcing the use of passkeys (FIDO2) on YubiKeys for sign-in within Microsoft Entra ID environments. It outlines how to configure Conditional Access policies and Authentication Strengths to require phishing-resistant authentication when accessing the Microsoft Office 365 application.

Conditional Access

<u>Conditional Access</u> policies at their simplest are if-then statements; if a user wants to access a resource, then they must complete an action. For example: If a user wants to access an application or service like Office 365, then they must perform multifactor authentication to gain access.

Note: Even though passkeys (FIDO2) are considered passwordless and fulfill MFA requirements, Conditional Access policies are evaluated only after the authentication process is successfully completed. As a result, authentication strength doesn't restrict a user's initial authentication. Suppose you are using the built-in phishing-resistant MFA strength. A user can still type in their password, but they are required to sign in with a phishing-resistant method such as FIDO2 security key before they can continue.

In addition, conditional access does not affect authentication at the Windows sign-in and lock screens.

Authentication Strengths

<u>Authentication strengths</u> in Microsoft Entra ID allow organizations to define which authentication methods meet specific security requirements. In the context of phishing-resistant authentication, they are used to enforce the use of strong methods such as passkeys (FIDO2 security keys) to protect sensitive resources.

Built-in vs Custom Conditional Access authentication strengths

Built-in authentication strengths are combinations of authentication methods that are predefined by Microsoft. Built-in authentication strengths are always available and can't be modified.

Custom authentication strengths offer greater flexibility by allowing administrators to select specific authentication methods that meet their organization's unique security and compliance requirements. This enables precise control over which methods such as FIDO2 security keys only are permitted when accessing protected resources.

• FIDO2 security key advanced options

You can restrict the usage of FIDO2 security keys based on their Authenticator Attestation GUIDs (AAGUIDs). This capability allows administrators to require a FIDO2 security key from a specific manufacturer in order to access the resource.

This guide will focus on enforcing YubiKeys with the 5.7 firmware based on the AAGUID.

yubico

Objectives

- Enforce YubiKeys to be used during sign-in to Microsoft Office 365.
- Enable in-line registration of YubiKeys (Interrupt Mode)

Before you begin

- Make sure you have completed the steps on the <u>Yubico support page</u> in the **Admin Deployment Guide** and the **User Enablement Guide** before beginning the following steps.
- The focus of this guide is to enable authentication into defined resources as per the settings within a given policy.
- Don't lock yourself out.
 - Yubico recommends identifying a select number of users or a group to test these configurations before applying to all users.
 - Deploy in **Report-Only mode** first to allow you to analyze the impact of the policy.
 - Please refer to the following resource on <u>Break-glass Accounts</u> for best practices on leveraging break-glass accounts with YubiKeys.
- Learn more about two tools for evaluating Conditional Access Policy impacts:
 - Policy impact
 - Conditional Access gap analyzer workbook

Minimum requirements

- Entra ID P1 licensing is required for Conditional Access Policies. *Note: Licensing requirements are subject to change*
- Security Administrator or Conditional Access Administrator role to create and modify policies

Create an authentication strength control

This section will describe how administrators can start enforcing the use of phishing-resistant passkeys (FIDO2) on YubiKeys during sign-in to select Entra ID protected applications using Conditional Access Policies.

Authentication strength controls describe which authentication methods must be used when signing into an application where a Conditional Access Policy is applied. Depending on the requirements, admins may leverage Entra ID built-in coarse authentication strengths such-as Phishing-Resistant MFA or optionally admins can create their own more fine-grained custom authentication strength controls that require specific FIDO2 security keys to be used. This guide will demonstrate how to create custom authentication strength control that requires specific FIDO2 YubiKey AAGUIDs.

Every organization will have unique requirements for applying Conditional Access Policies so this section will only attempt to show a minimum basic policy that requires passkeys (FIDO2) on YubiKeys to be used for sign-in to the Office application. This section is simply intended to demonstrate how to add these additional requirements into their policy framework and is not intended to be the only policy applied to customer environments.

Yubico recommends first reviewing the <u>Microsoft guidance and concepts</u> about Conditional Access Policies and following Microsoft best practices.

Option 1: Using Entra Admin Portal

- 1. Navigate to the Entra Admin Center: <u>https://entra.microsoft.com</u>
- 2. Sign-in with an account that holds either the **Security Administrator** or **Conditional Access Administrator** role
- 3. In the menu pane on the left, expand the **Protection** blade and select **Conditional Access**



4. Navigate to Manage -> Authentication strength and select New authentication strength

Home > Conditional Access							
Conditional Access Authentication strengths							
Overview	+ New authentication strength O Refresh						
I Policies	Authentication strengths determine the co Learn more	mbination of au	thentication methods that can be used.				
Insights and reporting	Type: All Authentication methods:	All 🐨 Reset	filters				
X Diagnose and solve problems							
Manage	Authentication strength	Туре	Authentication methods	Conditional access policies			
↔ Named locations	Multifactor authentication	Built-in	Windows Hello For Business / Platform Credential	Not configured in any policy yet			
Custom controls (Preview)	Passwordless MFA	Built-in	Windows Hello For Business / Platform Credential	Not configured in any policy yet			
Terms of use	Dhishing and hard hard	Durille in	Mindawa Halla Faa Durinaan (Diatfarm Condential	Net confirmed in competition of			
VPN connectivity	Phisning-resistant MFA	Built-In	windows Helio For Business / Platform Credential	Not configured in any policy yet			
Authentication contexts							
Authentication strengths							
E Classic policies							
Monitoring							
Sign-in logs							
Audit logs							
Troubleshooting + Support							
New support request							

- 5. In the **New authentication strength** section enter the following details and make the following selections:
 - a. Name: Name of the authentication strength
 - b. **Description**: Descriptive name of the authentication strength
 - c. Select the checkbox beside the Passkeys (FIDO2) option
 - d. Select Advanced Options

New authentication strength	\times
Custom	
Configure Name *	Î
YubiKey 5 Series 5.7	
Description	
Only allow security keys that are of the YubiKey 5 Series make and model with the 5.7 firmware	
Search authentication combinations	Ī
Phishing-resistant MFA (3)	
Windows Hello For Business / Platform Credential	
Passkeys (FIDO2) Advanced options	
Certificate-based Authentication (Multifactor) Advanced options	

- Refer to the <u>Yubico support article</u> for the AAGUIDs that will be used in your Entra tenant. For this guide we will include all the AAGUIDs with 5.7 firmware. You can also confirm an AAGUID using the following <u>Retrieve a YubiKey AAGUID</u> by presenting your YubiKey.
 - a. Click on **Add AAGUID** and enter the AAGUID that corresponds to the AAGUID for your YubiKeys using the support article above.
 - b. Repeat the process until all your AAGUIDs have been enteredi. Note: There is a maximum of 15 AAGUIDs.
 - c. Click Save
 - d. Click Next
 - e. Click Create

Enter a list of authentication this authentica Learn more Provider Microsoft	Authenticator Attestation GUIDs (AAGUIDs) that can t strength. Passkeys with AAGUIDs not in this list will r tion strength. Authenticator (Preview)	be used to satisfy this not be usable to satisfy
OR		
Add AAGUID	+	
	19083c3d-8383-4b18-bc03-8f1c9ab2fd1b	۱.
	4599062e-6926-4fe7-9566-9e8fb1aedaa0	۱.
	20ac7a17-c814-4833-93fe-539f0d5e3389	İ
	a02167b9-ae71-4ac7-9a07-06432ebb6f1c	۱.
	24673149-6c86-42e7-98d9-433fb5b73296	۱.
	b90e7dc1-316e-4fee-a25a-56a666a670fe	1
	3b24bf49-1d45-4484-a917-13175df0867b	۱.
	a25342c0-3cdc-4414-8e46-f4807fca511c	Ĩ
	d7781e5d-e353-46aa-afe2-3ca49f13332a	İ
	1ac71f64-468d-4fe0-bef1-0e5f2f551f18	1
	6ab56fad-881f-4a43-acb2-0be065924522	۱.

7. The newly created Authentication Strength will be displayed as a type of Custom

Home > Conditional Access							
Conditional Access Authentication strengths							
~	+ New authentication strength 💍 Refresh						
 Overview 	Authentication strengths determine the combination of authentication methods that can be used.						
I Policies	Learn more 🛛						
Insights and reporting	Type: All Authentication methods:	All 🐨 Reset	filters				
X Diagnose and solve problems							
Manage	Authentication strength	Туре	Authentication methods	Conditional access policies			
Named locations	YubiKey 5 Series 5.7	Custom	Passkeys (FIDO2)	Not configured in any policy yet			
Custom controls (Preview)	Multifactor authentication	Built-in	Windows Hello For Business / Platform Credential	Not configured in any policy yet			
🦉 Terms of use							
VPN connectivity	Passwordless MFA	Built-in	Windows Hello For Business / Platform Credential	Not configured in any policy yet			
Authentication contexts	Phishing-resistant MFA	Built-in	Windows Hello For Business / Platform Credential	Not configured in any policy yet			
O Authentication strengths							
Elassic policies							

Option 2: Create Authentication Strength Using Microsoft Graph Powershell Module

1. Sign-in to the Entra ID tenant.

Connect-MgGraph -Scopes "Policy.ReadWrite.AuthenticationMethod"

2. Create Authentication strength. *See the <u>Yubico support page</u> for the current list of Yubico AAGUIDs

```
= "mfa"
allowedCombinations
combinationConfigurations
            "19083c3d-8383-4b18-bc03-8f1c9ab2fd1b",
```

3. Record the output id that is returned, this id will be referred to as "authenticationStrengthID" later in this guide.

Create a Conditional access policy

This section will demonstrate how the custom authentication strength can be applied to a Conditional access policy. The policy will target specific users for the Office 365 application and apply the Authentication Strength created above named 'YubiKey 5 Series 5.7' authentication strength.

Option 1: Using the Entra admin portal

- 1. In the Conditional Access Overview section:
 - a. Select Policies > New policy

Home > Passkey (FIDO2) settings > Conditional Access				
Image: Second tional Access Policies Image: Microsoft Entra ID ×				
 Overview 	+ New policy + New policy from template	Upload policy file 🛛 🤉 What if		
≇≣ Policies	What is Conditional Access?			
Insights and reporting	Conditional Access gives you the ability to enforce acce	ess requirements when specific conditions occur. Let's take a few		
X Diagnose and solve problems	examples Learn more 🖸			
Manage				
Named locations	Conditions	Controls		
Custom controls (Preview)	When any user is outside the company network	They're required to sign in with multifactor authentication		
✓ Terms of use	When users in the 'Managers' group sign-in	They are required be on an Intune compliant or domain-joined		
🔅 VPN connectivity	4			
Authentication contexts	Get Started			
Authentication strengths				
≣ Classic policies	 Create your first policy by clicking "+ Create new 2. Specify policy Conditions and Controls 	v policy"		

- 2. Provide the following:
 - a. Under **Name**: Provide a name for the policy
 - b. Under Assignments, click Specific users included
 - i. Under Include, click Users and groups and select the a test group

Home > Passkey (FIDO2) settings > Conditio	nal Access Policies > New > Conditional Access Overview >
New Conditional Access policy	
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more C	Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more 🗗
Name * CA 01 - Require YubiKeys for Office365	Include Exclude
Assignments	All users
Users (i)	Select users and groups
Specific users included	Guest or external users ①
Target resources ①	Directory roles ①
No target resources selected	Users and groups
Network NEW ①	
Not configured	Select
Conditions ①	1 group
0 conditions selected	YT YubiKey Test Group ····
Enable policy	
Report-only On Off	
Create	

- c. Under Target resources, select No target resources included
 - i. Under Include, click Select resources and click None
 - ii. In the Select menu pane, type Office 365 in the search box and select the Office 365 option
 - iii. Click Select

Home > Passkey (FIDO2) settings > Condition	nal Access Policies > New > Conditional Access Overview	Select ×
New		Resources
Conditional Access policy		
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.	Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more 🖒	Microsoft Admin Portals ①
Learn more 🖉	Select what this policy applies to	✓ U Office 365 ①
Name *	Resources (formerly cloud apps) V	AADReporting
CA 01 - Require YubiKeys for Office365 🗸 🗸		1b912ec3-a9dd-4c4d-a53e-76aa7a
Assignments	Include Exclude	AA Azure AD Identity Governa 810dcf14-1858-4bf2-8134-4c369fa
Users (i)	O None	
Specific users included	All internet resources with Global Secure Access	Ac Azure Credential Configur ea890292-c8c8-4433-b5ea-b09d06
Target resources ①	All resources (formerly 'All cloud apps')	Selected items
No target resources selected	Select resources	Office 365 ^① Remove
Select resources" must be configured	Edit filter	
Network NEW (i)	None	
Not configured	Select	
Conditions ①	None	
0 conditions selected		
Enable policy		
(Report-only) On Off		
Create		Select

- d. Under Access Controls, select 0 controls selected under the Grant option
 - i. In the **Grant** menu:
 - 1. Click in the **Require authentication strength** checkbox to enable it
 - 2. From the drop-down menu select the custom authentication strength option created in the previous step
 - 3. Click Select
 - 4. Click Create to create the policy

Home > Passkey (FIDO2) settings > Conditional Access Policies > New > Conditional Access Policies >	Grant	\times
New … Conditional Access policy	• Grant access	
Users ① Specific users included	Require multifactor ① authentication	
Target resources ① 1 resource included Network NEW ①	"Require authentication strength" cannot be used with "Require multifactor authentication". Learn more. C"	
Not configured Conditions ① 0 conditions selected	Require authentication strength ① YubiKey 5 Series 5.7 ✓	
Access controls Grant ① 0 controls selected Session ①	To require phishing-resistant authentication for external users, configure cross-tenant access settings to accept claims from Microsoft Entra tenants. Learn more. Of	
0 controls selected Enable policy	Require device to be marked ① as compliant Require Microsoft Entra ①	
Report-only On Off Create		

Note: By default, the policy will be created in Report-only mode. Yubico recommends you enable the policy in this mode during the testing phase.

e. The policy is now created and will enforce sign-in to the Office 365 application for the targeted group.

Home > Conditional Access						
E Conditional Access	Policies					
«	+ New policy	+ New policy from template	↑ Upload policy file	🔉 What if 💍 Refre	sh 💽 Preview features	🖗 Got feedback?
 Overview 	Microsoft Entra Co	nditional Access policies are used	to apply access contro	ls to keep vour organizati	on secure. Learn more 🛛	
I Policies		,				
Insights and reporting	All policies	Microsoft-managed po	licies			
X Diagnose and solve problems	1	0				
	Total	out of 1				
Manage	0 Soarch					
 Named locations 	- Search			Y Add filt	er	
Custom controls (Preview)	1 out of 1 policy f	ound				
🧭 Terms of use	Policy name			State	Creation date	Modified date
VPN connectivity	CA 01 - Require	YubiKeys for Office365		Report-only	4/16/2025, 9:37:35 PM	4/18/2025, 1:39:48 PM
Authentication contexts	· · · ·					
O Authentication strengths						
I Classic policies						

Option 2: Create Conditional Access Policy Using Microsoft Graph Powershell SDK

1. Sign-in to the Entra ID tenant



2. Create the Conditional Access Policy using the following template. Note that you will need to replace the groupID and authenticationStrengthID with the appropriate values.

```
applications = Q{
           includeApplications = @(
           includeGroups = @(
       clientAppTypes = @(
New-MgIdentityConditionalAccessPolicy -BodyParameter $body
```

Testing the policy

Once you have carefully evaluated the impact of the policy using logging data in the sign-in logs, you can enable the policy.

1. In the Conditional Access Policies page, select the policy

	··· > Authentication methods Policies > Conditional Access Policies > Users > Erin Sign-in logs > Conditional Access						
**	Econditional Access Policies ···· ×						
	~	+ New policy	+ New policy from templ	ate 👖 Upload policy file 🏅	🤉 What if 💍 Re	efresh ····	
1	Overview	Microsoft Entra C	anditional Access policies are	used to apply access controls t		ration socura Learn	
這	Policies	more 🗹	onutional Access policies are	used to apply access controls t	o keep your organiz	Zation secure. Learn	
•	Insights and reporting	All policies	All policies Microsoft-managed policies				
×	Diagnose and solve problems	1	0				
Ma	nage	Total	out of 1				
«· »	Named locations	✓ Search			Add	filter	
	Custom controls (Preview)	1 out of 1 policy	found				
\checkmark	Terms of use						
尊	VPN connectivity	Policy name			State	Creation date	
4	Authentication contexts	CA 01 - Require	YubiKeys for Office365		On	4/16/2025, 9:37:35	
0	Authentication strengths					Þ	
1	Classic policies						

- 2. Under Enable Policy, toggle the option to Enable
 - a. Click Save

··· > Authentication methods Policies > 0	Conditional Access Policies >
CA 01 - Require YubiKeys	for Office365
🗓 Delete 💿 View policy information 💿	View policy impact (Preview)
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more d	
Name *	
CA 01 - Require YubiKeys for Office365	
Assignments	
Users 🛈	
Specific users included	
Target resources ①	
1 resource included	
Network NEW ①	
Not configured	
Conditions ①	
0 conditions selected	
Enable policy	
Report-only On Off	
Save	

In the following scenarios, MFA Capable refers to a user who has either already registered for multi-factor authentication or is signing in using a credential such as a Temporary Access Pass. A user must be MFA Capable before they can register a FIDO2 credential.

Scenario 1: Step-up Authentication - User has already registered approved YubiKey and begins sign-in with a password

In this scenario a user has already registered a YubiKey that meets the authentication strength requirements. They authenticate with a lower assurance authentication method such as a password and they are prompted for step-up authentication.

💽 InPrivate (2) 🔲 🚦 Sign in to your account x +		- o ×
← C	ect_account&sosid=003fd009-0928-8d86-f66d-5e02f1413df5&ctx=rQQIARAAjVNLqONkGO3r9rZlxtu5iOgs9C5UxDtp	☆ ☆ Update �� …
	Microsoft Sign in Erin@YubicoDem0.onmicrosoft.com	
	No account? Create one!	
	Can't access your account?	
	Back Next	
	Sign-in options	
		Terms of use Privacy & cookies

1. Enter the username and click Next

2. Enter the password and click Sign in

() InPrivate (2) 🗇 💾 Sign in to your account x +	- o ×
C C https://login.microsoftonline.com/common/reprocess?prompt=select_account&sosid=003/d009-0928-8486-6664-5e02/1413df5&ctx=rQQIARAAJVNLqONkGO3/97Zktu5iOgs9C5UkDtp	۲≝ Update 😵 ···
Attps://logit.microsoftonline.com/common/reprocess?prompt=select_account&cosid=003/d009-0228-8486-f66d-5e0211413df5&ctx=rQQIARAA4yNLqONAGO319dZbtu5F0qs9C5UxDp.	
	-fun- Brivary & cookier
lems	of use Privacy & cookies

3. You will be prompted to step-up your authentication. Click the **Face, Fingerprint, PIN** or security key option

(🔰 InPrivate (3) 🔲 📲 Sign in to your account x +			-	ð ×
← C (a) https://login.microsoftonline.com/common/resume?username=erin%40yubid				
	Microsoft			
	erin@yubicodem0.onmicrosoft.com			
	Verify your identity			
	Your organization requires additional sign in methods to access this resource.			
	Face, fingerprint, PIN or security key			
	More information			
	Are your verification methods current? Check at https://aka.ms/mfasetup			
	Cancel			
		Terms of use Pri	ivacy & cookie	s

4. Select Security Key and click Next

() InPrivate (2) 🔲 🚦 Sign in to your account x +		
← C		☆ ੯≌ Update 😵 …
Individue (2) Image: Sign in the your account x + C	Windows Security Sign in with your passkey To sign in to "togin.microsoft.com", choose a device with a saved passkey. Security key More choices More choices Pixel 7a Pixel 7a Pixel 7a Pixel 7a	- • × ☆ ☆
	Security key Next Cancel	
		erms of use Privacy & cookies

5. Enter your security **PIN** and click **Ok** to continue

(2) InPrivate (2) 🔲 🚦 Sign in to your account x +		- o ×
← C (☆ ☆ Update 😵 …
	Windows Security × Making sure it's you	
	Please sign in to "login.microsoft.com".	
	This request comes from the app "msedge.exe" by "Microsoft Corporation".	
	Please enter your security key PIN.	
	OK Cancel	
		Terms of use Privacy & cookies

6. Touch the YubiKey when prompted

InPrivate (2)		- a ×
← C		🖒 🏠 Update 🏹 …
C C https://login.microsoft.com/common/filds/get?uflavor=Web	Windows Security × Making sure it's you Please sign in to "login.microsoft.com". This request comes from the app "msedge.exe" by "Microsoft Corporation". Image: Corporation Terms of the app and the app	يُنُ (Update P)
		Terms of use Privacy & cookies

- yubico
- 7. You have satisfied the authentication strength and will be signed-in to Office 365



Scenario 2: User is MFA Incapable and begins sign-in with password

- Signing-in to access the Office 365 protected by the Conditional Access Policy and Authentication Strength with a user account that is not MFA capable, meaning the user has not previously registered for multifactor authentication, you will receive the following notification:
 - a. Click Next

Note: In 2025, Microsoft will be rolling out a new UI exhibited to the right of the screen.

🕽 hoffrieate (3) 🗈 📲 Sign in to your account 🛛 🗙 +	- 0 ×
← C (Δ https://login.microsoftonline.com/common/login	 क्षे के
 	Microsoft test@organization.net Let's keep your account secure Well help you set up another way to verify it's you. Learn more about account verification. Use a different account
	Terms of use Privacy & cookies

2. The following page will be presented notifying you that **you will need to sign-in with multifactor authentication to create a passkey**. Note that you will not be able to proceed from this point

👔 InPrinzte (3) 🔲 📲 My Sign-Ins Register Microsoft 🗴 +	- 0 ×
← C (e 🖒 👍 🗝
Demo	?
Keep your account secure	
Contact your admin To create a passkey, you need to sign in using multi-factor aut admin to enable additional methods to support this. Sign in using a different account	hentication Contact your

Scenario 3: MFA Capable - Signing-in with MFA using an approved security key

In this scenario, the user is signing-in while satisfying MFA either through an existing MFA verification method or using the Temporary Access Pass (TAP) and has a YubiKey that **does meet** the authentication strength requirements. The security key in this scenario has not been previously registered.

1. Sign-in using a TAP or after satisfying MFA, you will receive one of the two following notifications:

() Linkinger (a) 💼 📓 Sign in to your account x +	- 0 X
View of the provide value o	Microsoft Test@organization.net Let's keep your account secure We'l help you set up another way to verify it's you. Learn more about account verification. Use a different account Next
	Terms of use Privacy & cookies ····

a. Click Next

- 2. You will be guided through the **interrupt-mode** experience of registering an approved security key. You can click on **Specific passkeys** to view supported AAGUIDs.
 - a. Click Next

() [abhinde ()] 🗈 🚆 My Sopoles (Register (Microsoft 🗴 +	- 0 ×
🗧 🖸 http://mylignina.microsoft.com/register?authMethods=328authMethodsCount=1	९ 🕁 🖆 🗝
Demo	?
Keep your account secure	
Add a passkey for more secure sign-in Image: A passkey is a replacement for your password that lets you sign in with your face, fingerprint, or PIN. Your device will open a security window and ask where you would like to save your passkey. Vour organization allows: Image: Secure passkey using another device	
Having trouble? Next	

3. Click Ok

DaPrinate (2) 🗖 💾 Sign in to your account x +		- o >	¢
← C (ର୍ଜ୍ <u>ମ</u> 🗘	Update 😵 …	
Windows Security X Continue setup Use your device to sign in to login.microsoft.com? Sign-in data will be stored on this device after you exit Incognito mode. You'll be able to sign to this website with your device again later. OK Cancel			
	Terms of use	Privacy & cookies	

4. Select Use another device



5. Select Security Key

InPrivate (2) In Figure 1 Sign in to your account × +		i .	- o ×
← C (≜ https://login.microsoft.com/cd658da5-8603-4e65-9666-4ec2109		☆ 😭	Update 😵 …
← C ▲ https://login.microsoft.com/cd558da5-8603-4e65-9666 4ec2105	93139/fido/create?cid=a13368eb-2741-494d-a675-2457af942b3a		i Update 🕅
	IPhone, iPad, or Android device Image: Security key Image: This Windows device Next Cancel		
		Terms of use	Privacy & cookies

6. Click Ok to allow you to setup you YubiKey to sign-in to Entra ID

InPrivate (2) In Figure 3 Sign in to your account × +			- o ×
← C (≜ https://login.microsoft.com/cd658da5-8603-4e65-9666-4ec210			Update 😵 …
	♥ Windows Security × Security key setup Set up your security key to sign in to login.microsoft.com as Erin@*\ubicoDemOonmicrosoft.com. This request comes from the app *msedge.exe* by *Microsoft Coporation*. OK Cancel	Terra dra 🦉	Privacy & cookies

7. Click **Ok** to allow Entra ID to see the make and model of your YubiKey

() InPrivate (2) 🗇 💾 Sign in to your account x +	- o ×
← C	từ the transformation that the transformation the transformation the transformation that the transformation the
C Material Control of Co	☆ ☆ (update *) ···
	remis or use privacy & Cookles

8. Enter a **PIN** and confirm it and click **Ok**

🌔 InPrivate (2) 🛅 🚦 Sign in to your account 🛛 🗙 🕂		- • ×
← C	10993139/fido/create?cid=0c909bab-f51b-430d-b0a1-93c2c9cd0758	☆ f (Update) …
	Windows Security Continue setup You'll need to create a PIN for this security	

9. Touch the YubiKey twice when prompted

() InPrivate (2) 🔲 🚦 Sign in to your account x +		- o ×
\leftarrow C \triangle https://login.microsoft.com/cd658da5-8603-4e65-9666-4ec210993139/fido/create?c		Update 😵 …
Windows Se Continue se	earity × etup Couch your security key. Cancel	vacy & cookies

10. The Passkey has been created and saved on the YubiKey. Click **Ok.**

() InPrivate (2) 🗖 🚦 Sign in to your account x +		- o ×
← C	9993139/fido/create?cid=0c909bab-f51b-430d-b0a1-93c2c9cd0758	☆ ¢≣ (Update 😵) …
	Windows Security X Passkey saved You can now use your security key to sign in to "login.microsoft.com". Cancel Nox	
		Terms of Lise Privacy & cookies

11. Provide a name for your YubiKey and click Next

(InPrivate (2) 🔲 📕 My Sign-Ins Register Microsoft. 🗙	+) ×
← C	isOobe=False&brkr=&brkrVer=&clientSku=&personality=&authMethods=32&authMethodCount=1	습 🖆 Update 🤆	e)
Demo			?
	Keep your account secure		
	Let's name your passkey Give your passkey a name to help distinguish it from others you might have added. Improved Yubikey 5 Series 5.7		

12. Click Done



13. Click **Done**. The YubiKey has been successfully registered.

InPrivate (2) 🔲 👫 My Sign-Ins Register Microsoft. 🗙	+	- o ×
← C		the second seco
Demo		?
	Keep your account secure	
	SUCCESS! Great job! You have successfully set up your security info. Choose "Done" to continue signing in. Default sign-in method:	
	Done	

Scenario 4: User is MFA Capable and begins sign-in with MFA and tries register an unapproved security key

In this scenario, the user is signing-in while satisfying MFA either through an existing MFA verification method or using the Temporary Access Pass (TAP) and is attempting to register a security key that **does NOT meet** the authentication strength requirements. This could be a security key that is not a YubiKey or a YubiKey that has not been approved for use as defined in the authentication strengths. The security key in this scenario has also not been previously registered.

- 1. Signing in using a TAP or after satisfying MFA, you will receive one of the two following notifications that may look similar to:
 - a. Click Next

🕐 InPrivate (3) 🗖 🚦 Sign in to your account x +	- 0 ×
← C	
C C Mitrov/loginumicrosofterilme.com/common/login Microsoft erin@yubiccodem0.onmicro More informatic Your organization needs m your account secure Use a different account Learn more	esoft.com In required ore information to keep We'll help you set up another way to verify it's you. Learn more about account verification. Use a different account Next
	Terms of use Privacy & cookies ••••

- 2. You will be guided through the in-line registration experience and guided to registering an approved security key. You can click on Specific passkeys to view supported AAGUIDs.
 - a. Click Next

🜔 InPrivate (3) 🔲 🚦 My Sign-Ins Register Microsoft 🗙 🚽	+	
← ♂	hMethods=32&authMethodCount=1	e 🕁 📬 📷
Demo		?
	Keep your account secure	
	Add a passkey for more secure sign-in Image: Secure Sign-in	ld

3. The wizard will guide you through the security key set up, however once the passkey on the YubiKey is saved, the following screen will appear notifying you that the **passkey does not meet the organization's requirements** and preventing you from proceeding. Note: A passkey has been created on the YubiKey but it has not been registered with the user account. The user will need to go through the process again to register with a security key that meets the organization's requirements.

🕒 InPrivate (3) 📄 🚦 My Sign-Ins Register Microsoft 🗙 🕂					
← C	be=False&brkr=&brkrVer=&clientSku=&pers	onality=&authMethods=32&authMethodCount=1	२ क्वे	ť≡	
Demo		Keen vour account secure		(?
	Passkey pot regi	stered			
		passkey doesn't meet your organization's requirements Contact your admin for port.			
	Lear	e: If this passkey has been saved to your device, delete it and try again. n how to delete your passkey			
	Having trouble?	Try again			