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

Copyright

Trademarks

Disclaimer

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

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

Contact Information

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

Original Document Release Date

March 25, 2025

Version History

Version	Date	Changes
1.0	May 22, 2025	Initial Release

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

Conditional Access 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

Authentication strengths 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.

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 Yubico support page 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 Break-glass Accounts 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.

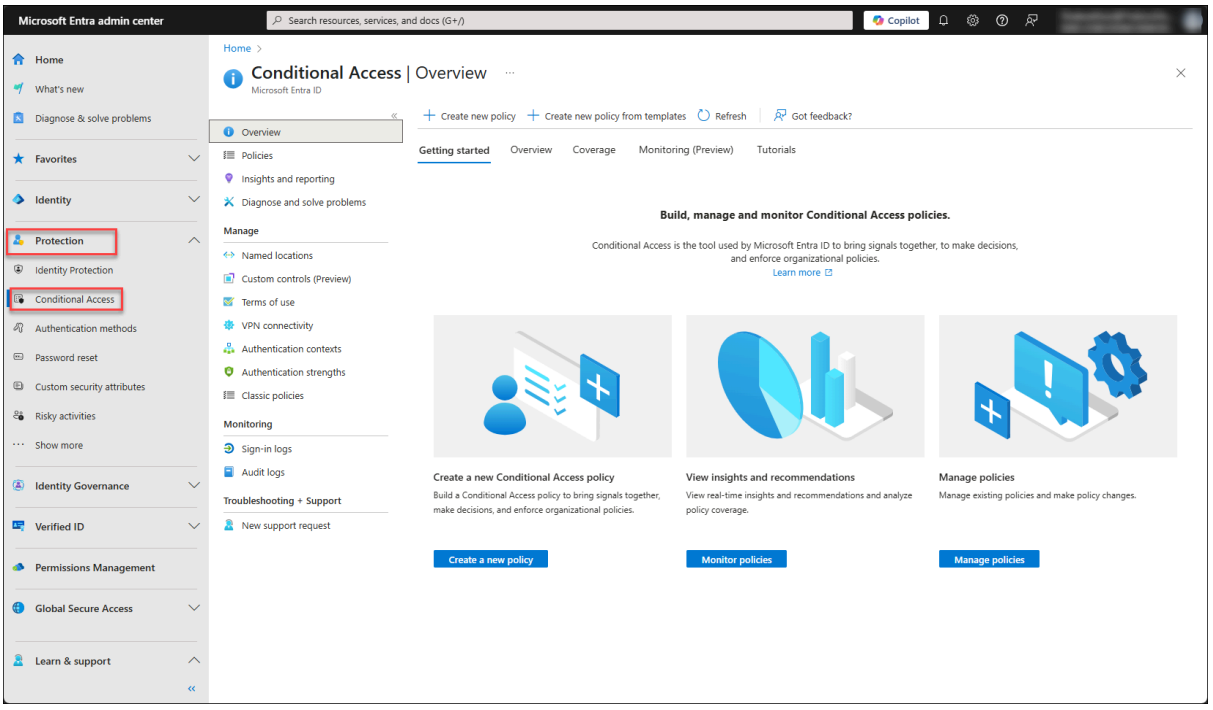
Authentication strength controls describe which authentication methods must be used when signing into an application where a Conditional Access Policy is applied. Depending on the requirements, admins may leverage Entra ID built-in coarse authentication strengths such-as Phishing-Resistant MFA or optionally 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.

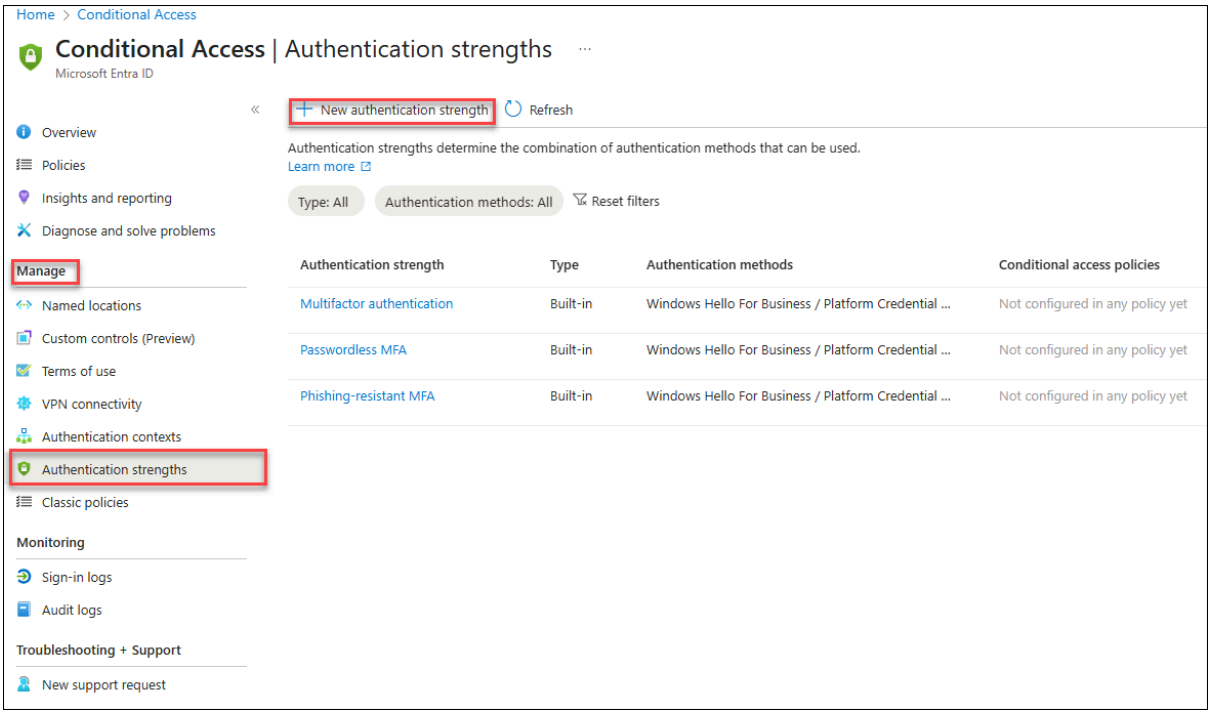
Yubico recommends first reviewing the Microsoft guidance and concepts about Conditional Access Policies and following Microsoft best practices.

Option 1: Using Entra Admin Portal

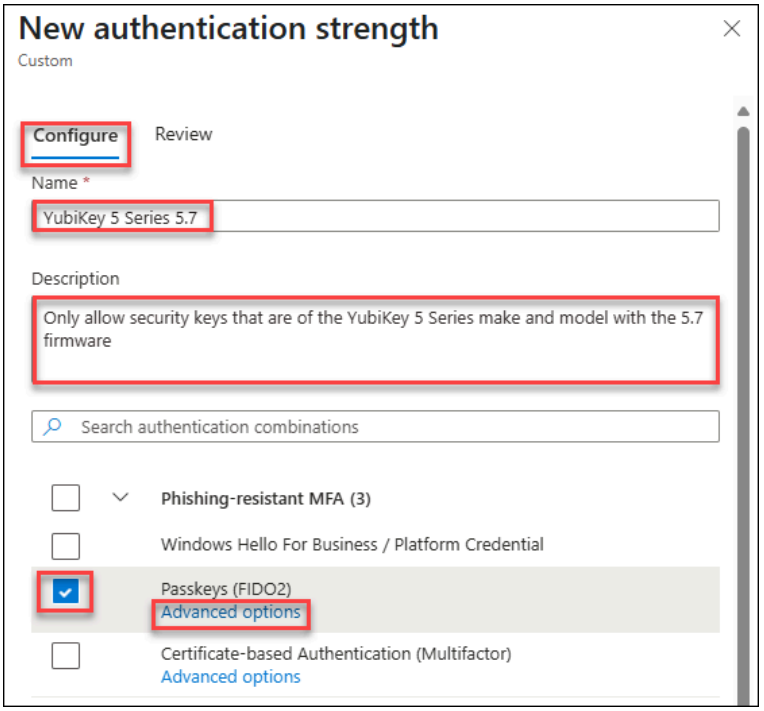
1. Navigate to the **Entra Admin Center**:https://entra.microsoft.com
2. Sign-in with an account that holds either the **Security Administrator** or **Conditional Access Administrator** role
3. In the menu pane on the left, expand the **Protection** blade and select **Conditional Access**



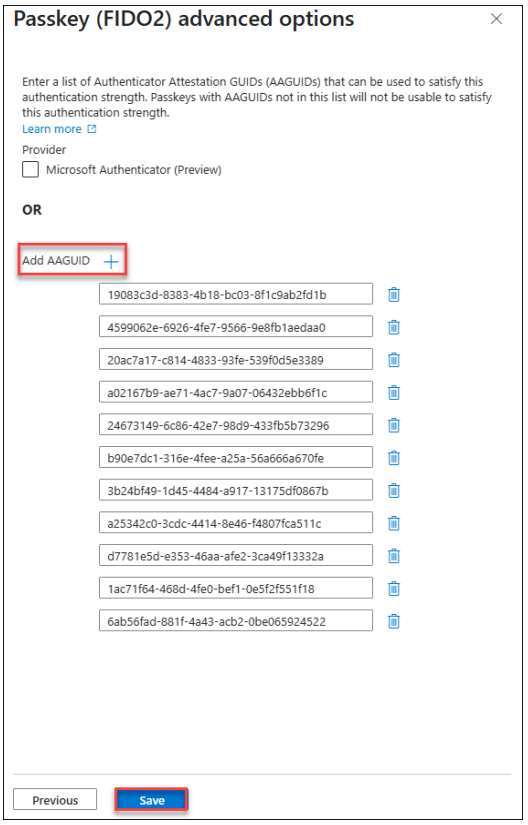
4. Navigate to **Manage -> Authentication strength** and select **New authentication strength**



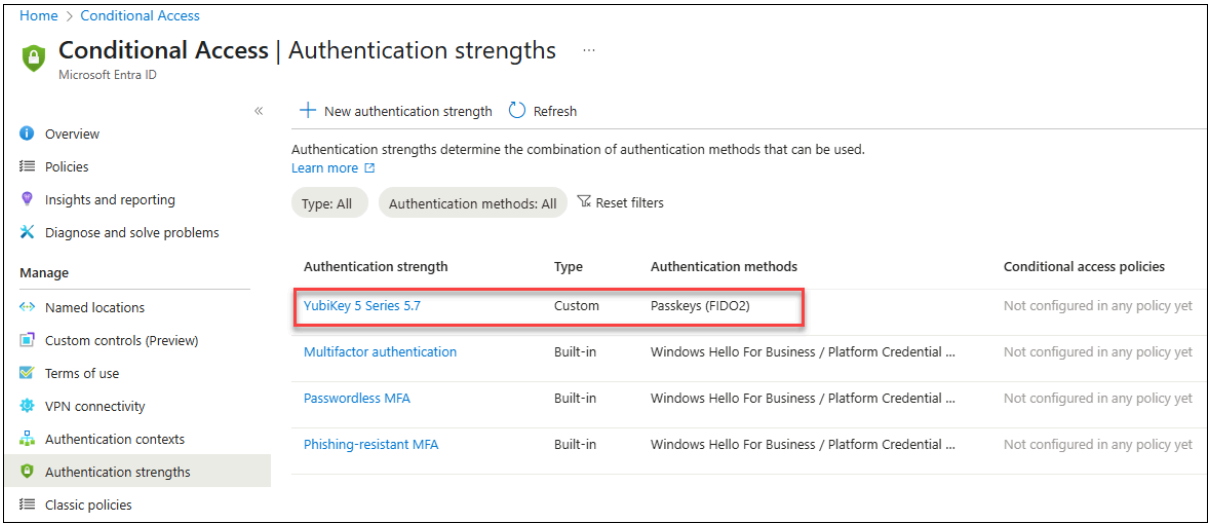
5. In the **New authentication strength** section enter the following details and make the following selections:
    a. **Name**: Name of the authentication strength
    b. **Description**: Descriptive name of the authentication strength
    c. Select the **checkbox** beside the **Passkeys (FIDO2)**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



6. Refer to the Yubico support article 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 Retrieve a YubiKey AAGUID 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 entered
        i. **Note:** There is a maximum of 15 AAGUIDs.
    c. Click **Save**
    d. Click **Next**
    e. Click **Create**



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



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 Yubico support page for the current list of Yubico AAGUIDs

```
# Sample Auth Strength using the YubiKey AAGUIDs that are applicable to your
Entra ID tenant
$params = @{
    displayName                                = "YubiKey 5 Series 5.7"
    requirementsSatisfied                      = "mfa"
    allowedCombinations                        = @(
        "fido2"
    )
    "combinationConfigurations@odata.context" =
"https://graph.microsoft.com/v1.0/$metadata#policies/authenticationStrengthPolici
es('77e39147-6170-4910-8c4c-790b50e79802')/combinationConfigurations"
    combinationConfigurations                  = @(
        @{
            "@odata.type"         =
"#microsoft.graph.fido2CombinationConfiguration"
            id                    = "8aef4369-f04b-4296-9347-7304ec5a1764"
            appliesToCombinations = @(
                "fido2"
            )
            allowedAAGUIDs        = @(
                "19083c3d-8383-4b18-bc03-8f1c9ab2fd1b",
                "4599062e-6926-4fe7-9566-9e8fb1aedaa0",
                "20ac7a17-c814-4833-93fe-539f0d5e3389",
                "a02167b9-ae71-4ac7-9a07-06432ebb6f1c",
                "24673149-6c86-42e7-98d9-433fb5b73296",
                "b90e7dc1-316e-4fee-a25a-56a666a670fe",
                "3b24bf49-1d45-4484-a917-13175df0867b",
                "a25342c0-3cdc-4414-8e46-f4807fca511c",
                "d7781e5d-e353-46aa-afe2-3ca49f13332a",
                "1ac71f64-468d-4fe0-bef1-0e5f2f551f18",
                "6ab56fad-881f-4a43-acb2-0be065924522"
            )
        }
    )
}

New-MgPolicyAuthenticationStrengthPolicy -BodyParameter $params
```

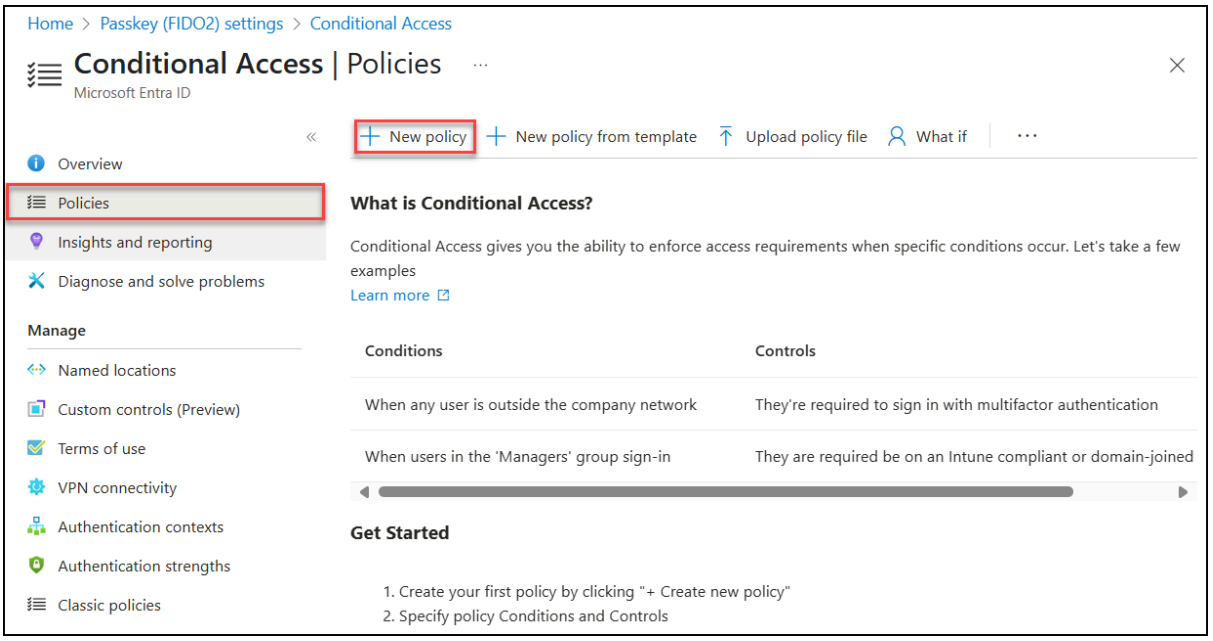
3. Record the output id that is returned, this id will be referred to as "authenticationStrengthID" later in this guide.

Create a Conditional access policy

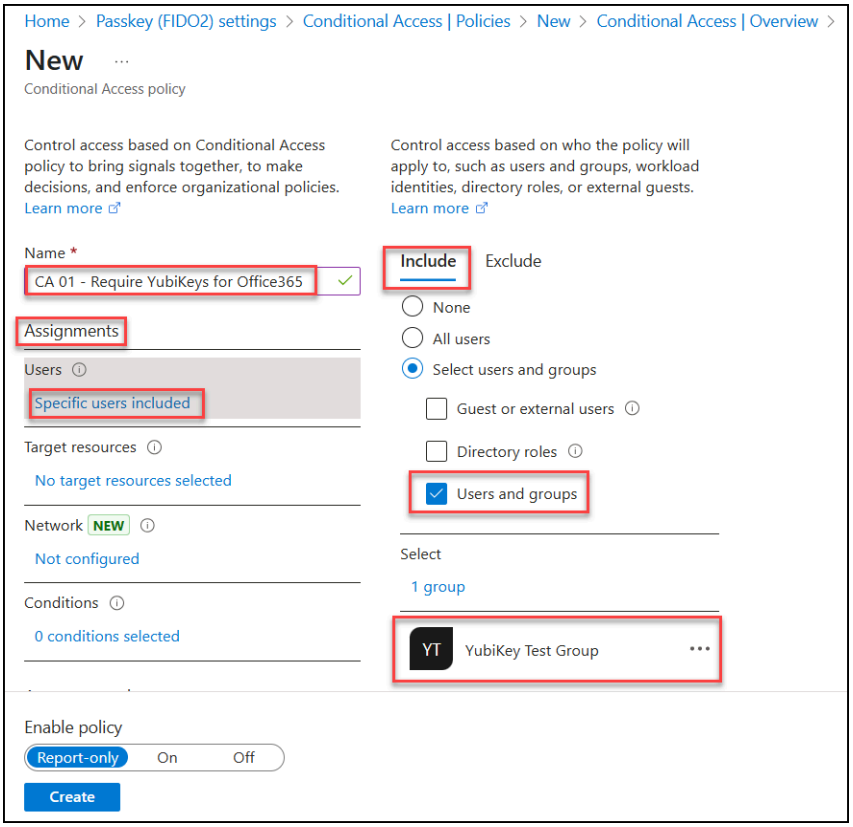
This section will demonstrate how the custom authentication strength can be applied to a Conditional access policy. The policy will target specific users for the Office 365 application and apply the Authentication Strength created above named 'YubiKey 5 Series 5.7' authentication strength.

Option 1: Using the Entra admin portal

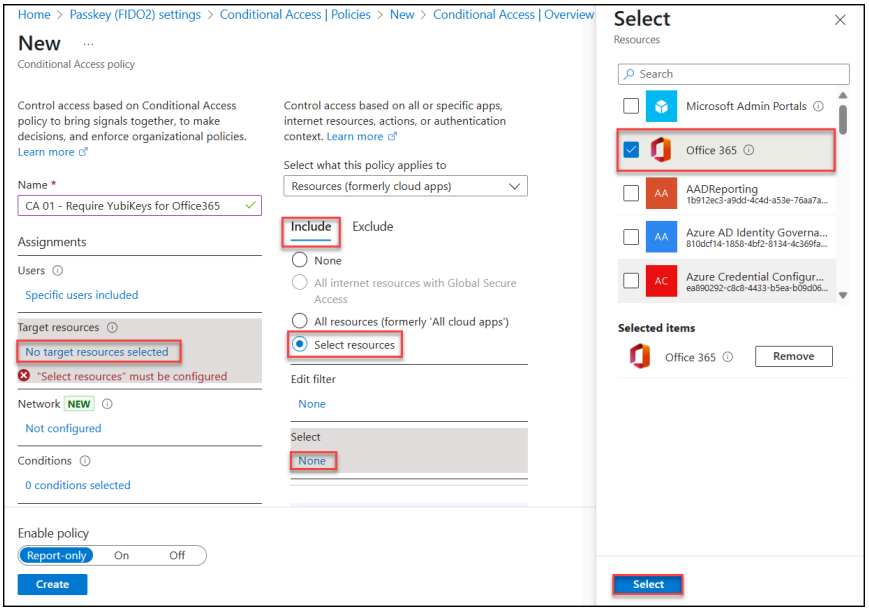
1. In the **Conditional Access Overview** section:
    a. Select **Policies > New policy**



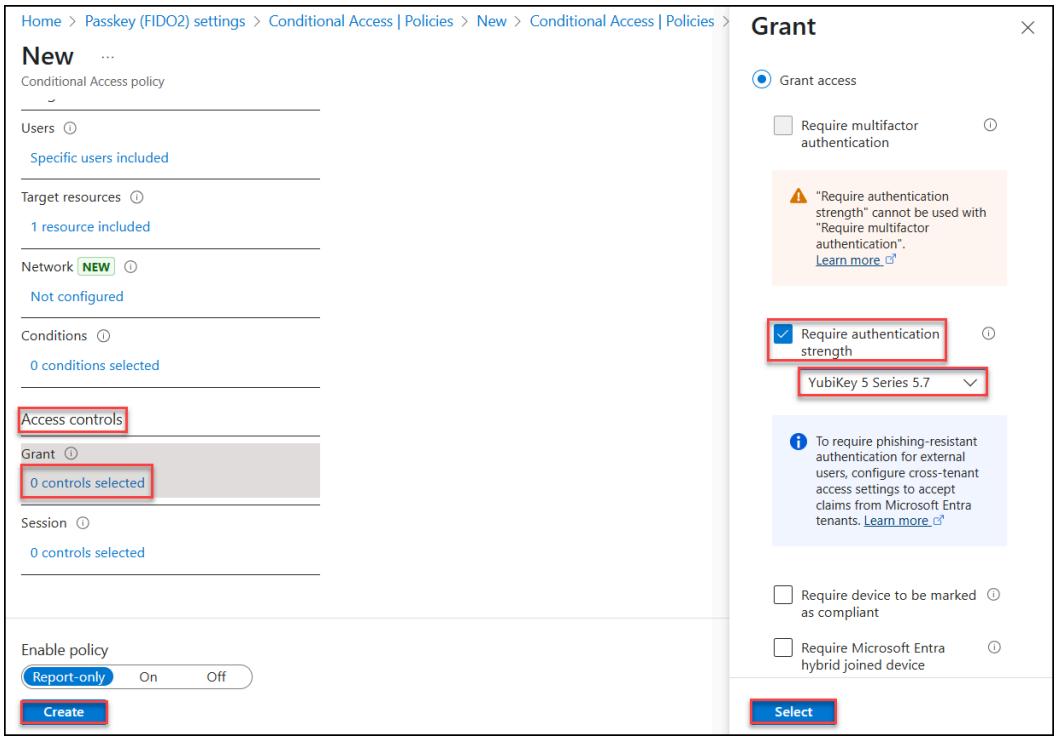
2. Provide the following:
    a. Under **Name**: Provide a name for the policy
    b. Under **Assignments**, click **Specific users included**
        i. Under **Include**, click **Users and groups** and select the a test group



    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**

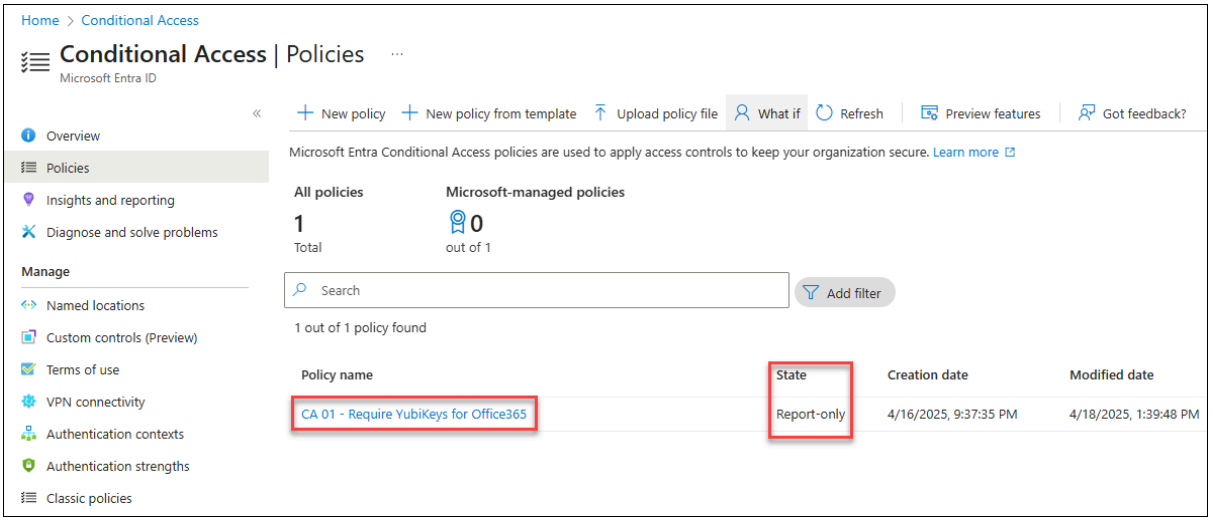


d. Under **Access Controls**, select **0 controls selected** under the **Grant** option
    i. In the **Grant** menu:
        1. Click in the **Require authentication strength** checkbox to enable it
        2. From the drop-down menu select the custom authentication strength option created in the previous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



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.



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

1. Sign-in to the Entra ID tenant

```
Connect-MgGraph -Scopes "Policy.ReadWrite.AuthenticationMethod",
"Policy.ReadWrite.ConditionalAccess"
```

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.

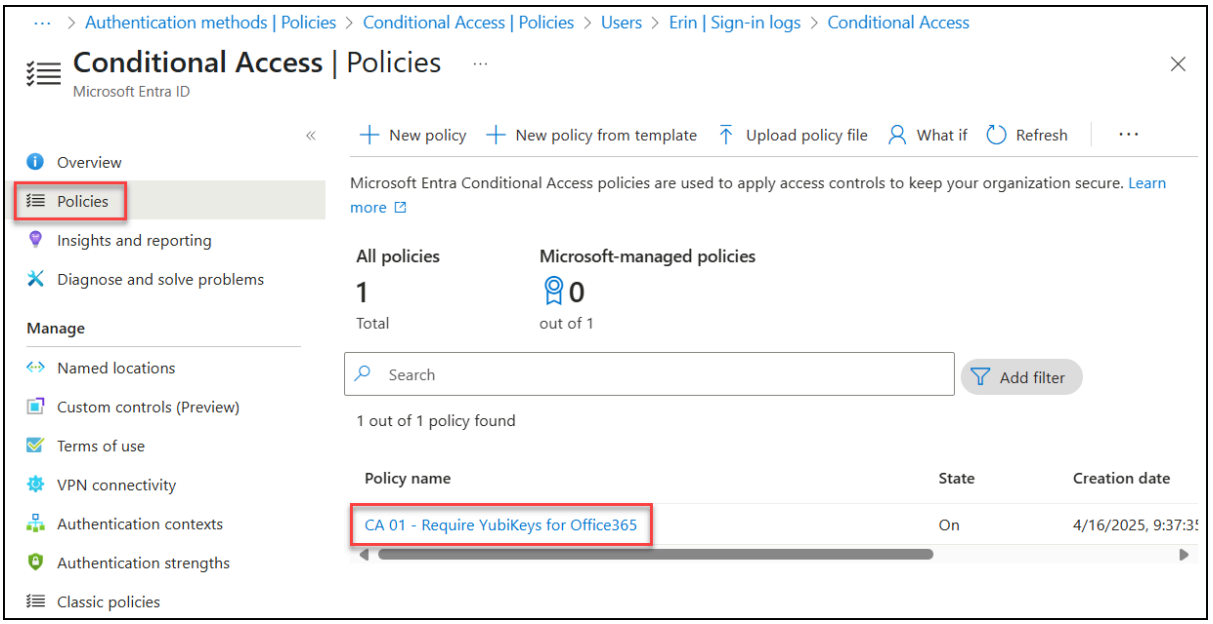
```
#Create a Conditional Access Policy
# - Creates a Conditional Access Policy in Report Only mode.
# - which applies to a specific group of users.  Set the groupID.
# - which applies only to the Office365 app
# - grants access only if a specific authentication strength is satisfied. Set
the authenticationStrengthID.
$body = @{
    displayName   = "CA 01 - Require YubiKeys for Office 365"
    state         = "enabledForReportingButNotEnforced"
    conditions    = @{
        applications   = @{
            includeApplications = @(
                "Office365"
            )
        }
        users          = @{
            includeGroups = @(
                "{groupID}"
            )
        }
        clientAppTypes = @(
            "all"
        )
    }
    grantControls = @{
        operator               = "OR"
        authenticationStrength = @{
            id = "{authenticationStrengthID}"
        }
    }
}

New-MgIdentityConditionalAccessPolicy -BodyParameter $body
```

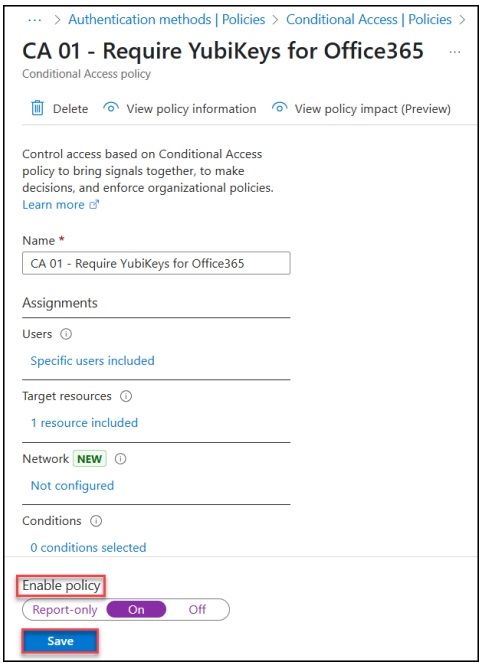
Testing the policy

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



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

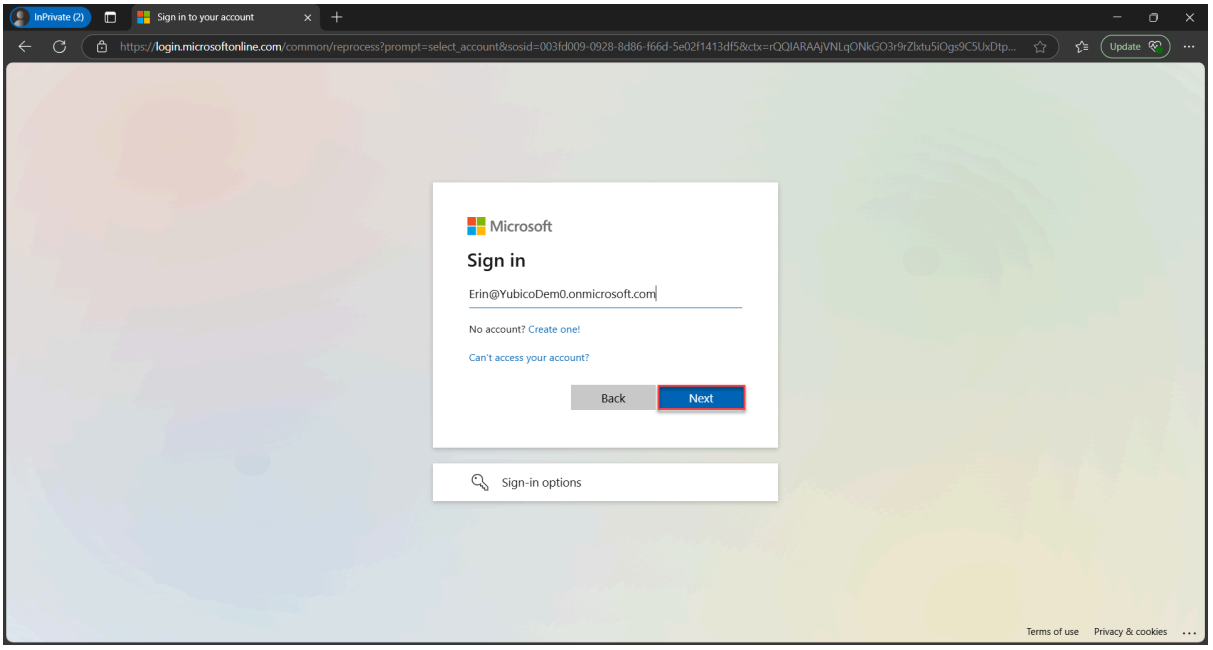


In the following scenarios, MFA Capable refers to a user who has either already registered for multi-factor authentication or is signing in using a credential such as a Temporary Access Pass. A user must be MFA Capable before they can register a FIDO2 credential.

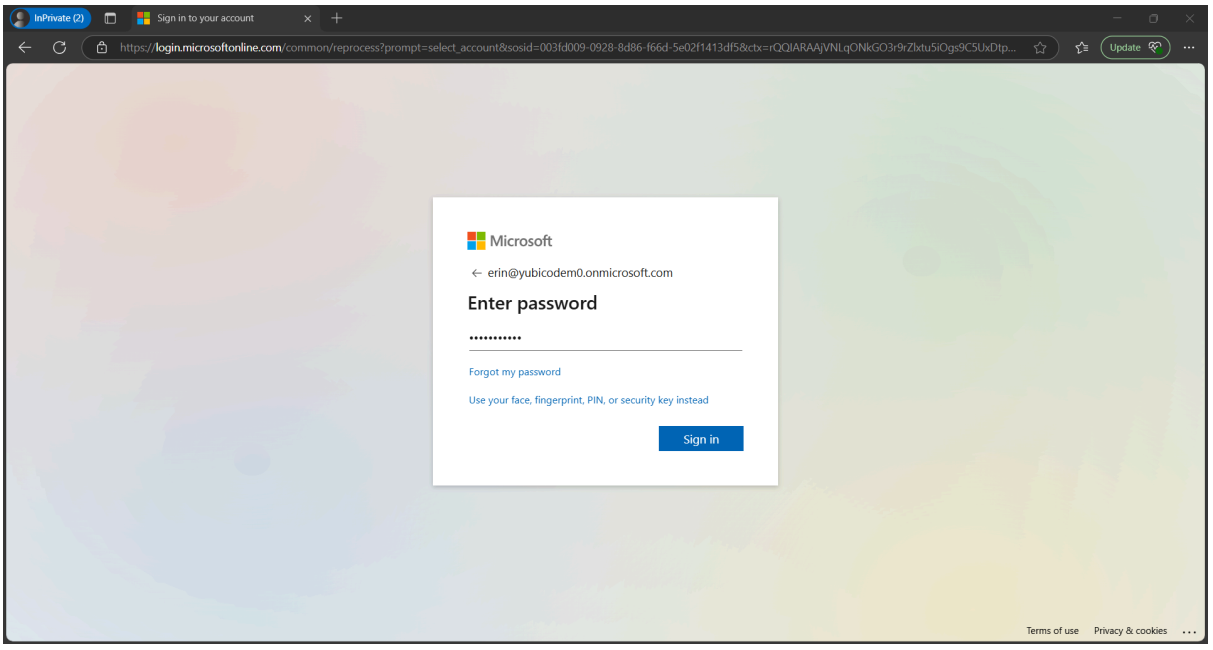
Scenario 1: Step-up Authentication - User has already registered approved YubiKey and begins sign-in with a password

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.

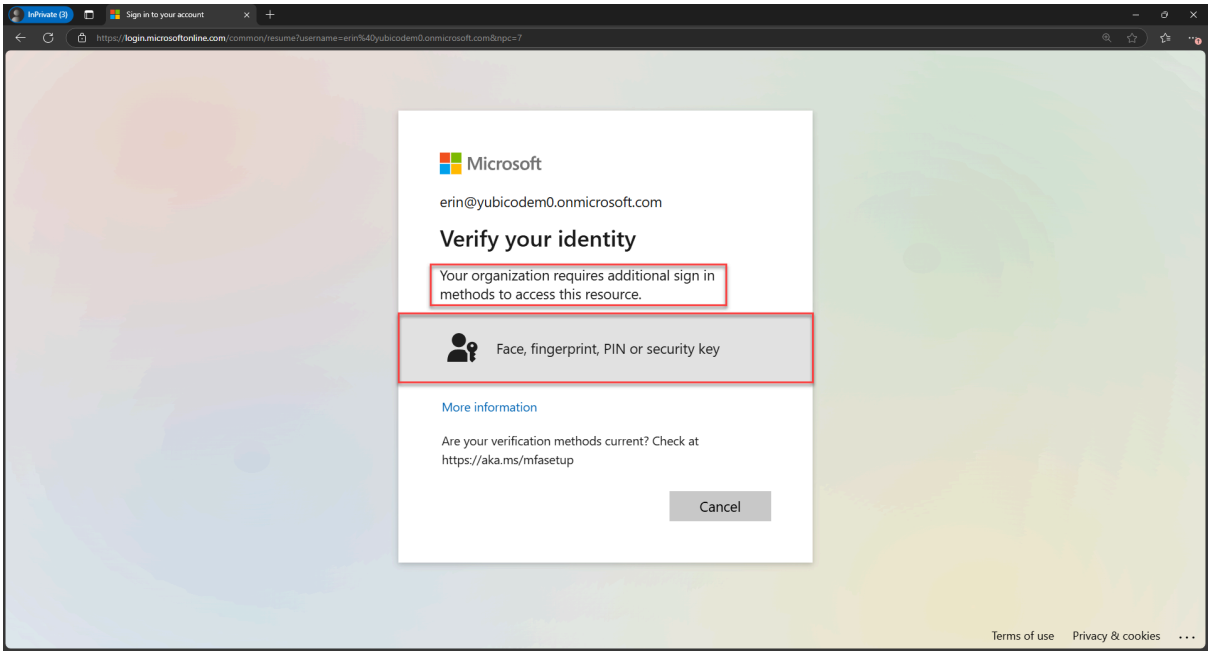
1. Enter the username and click **Next**



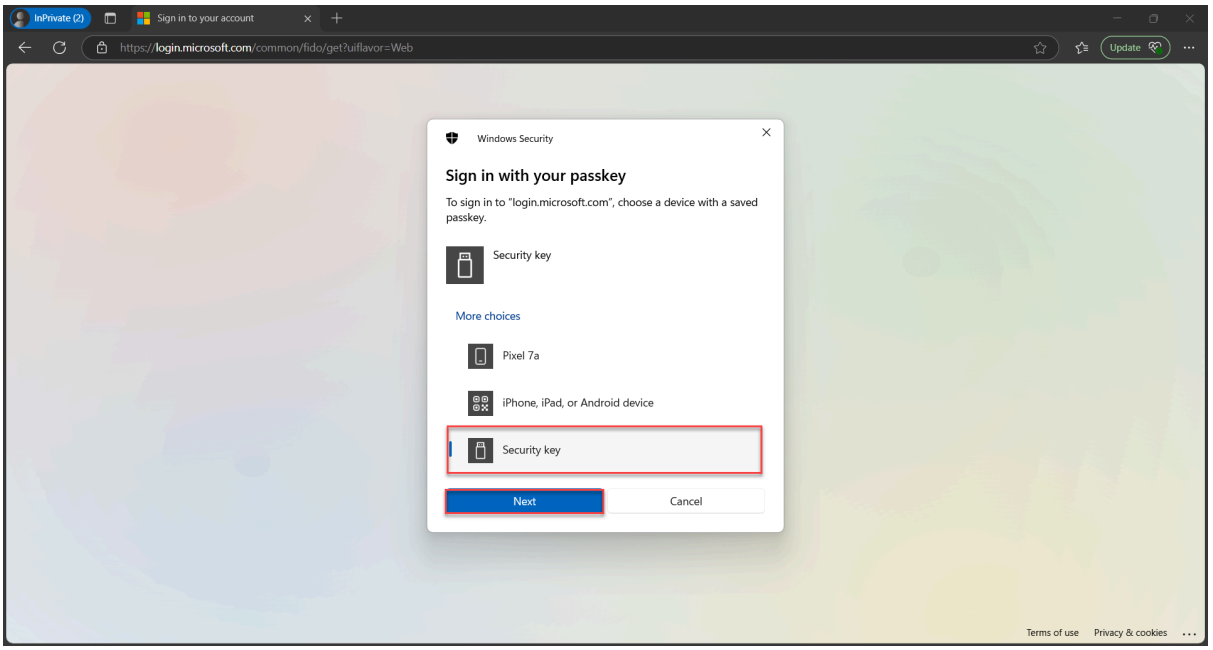
2. Enter the password and click **Sign in**



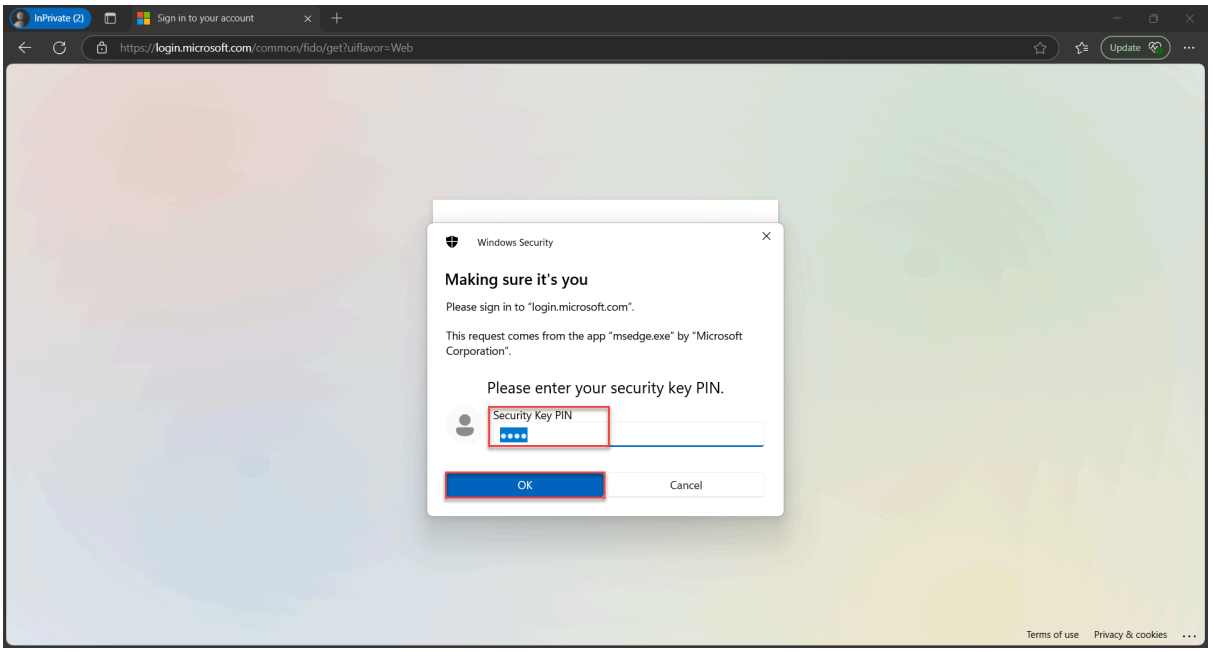
3. You will be prompted to step-up your authentication. Click the **Face, Fingerprint, PIN or security key** option



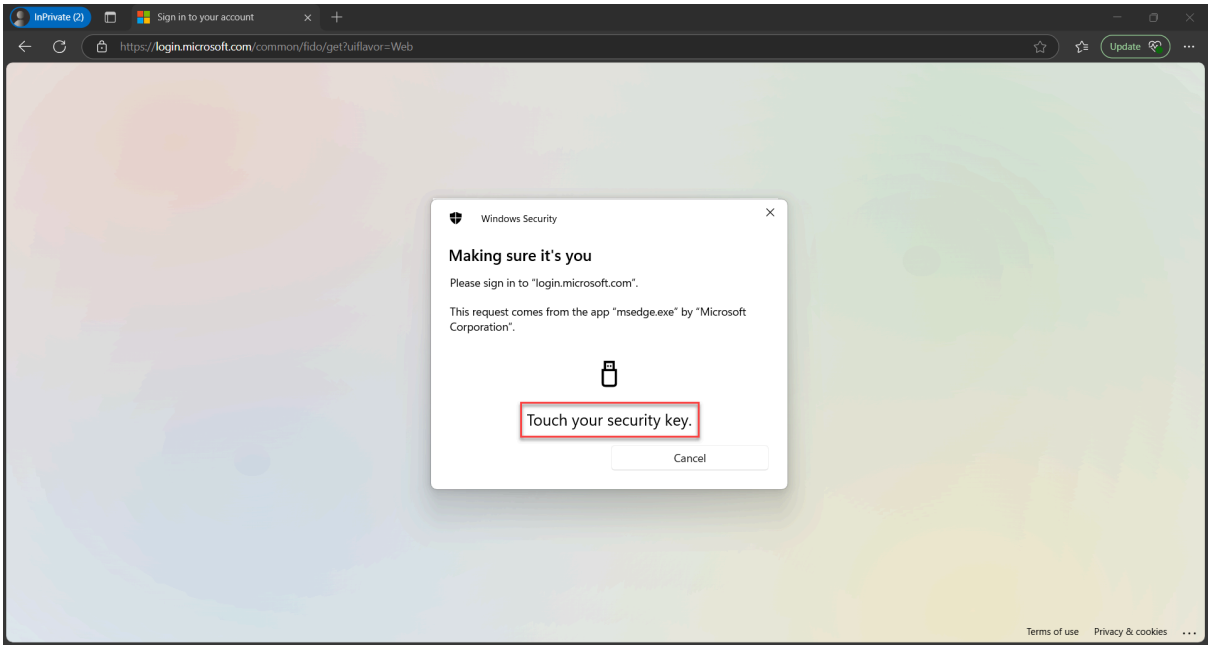
4. Select **Security Key** and click **Next**



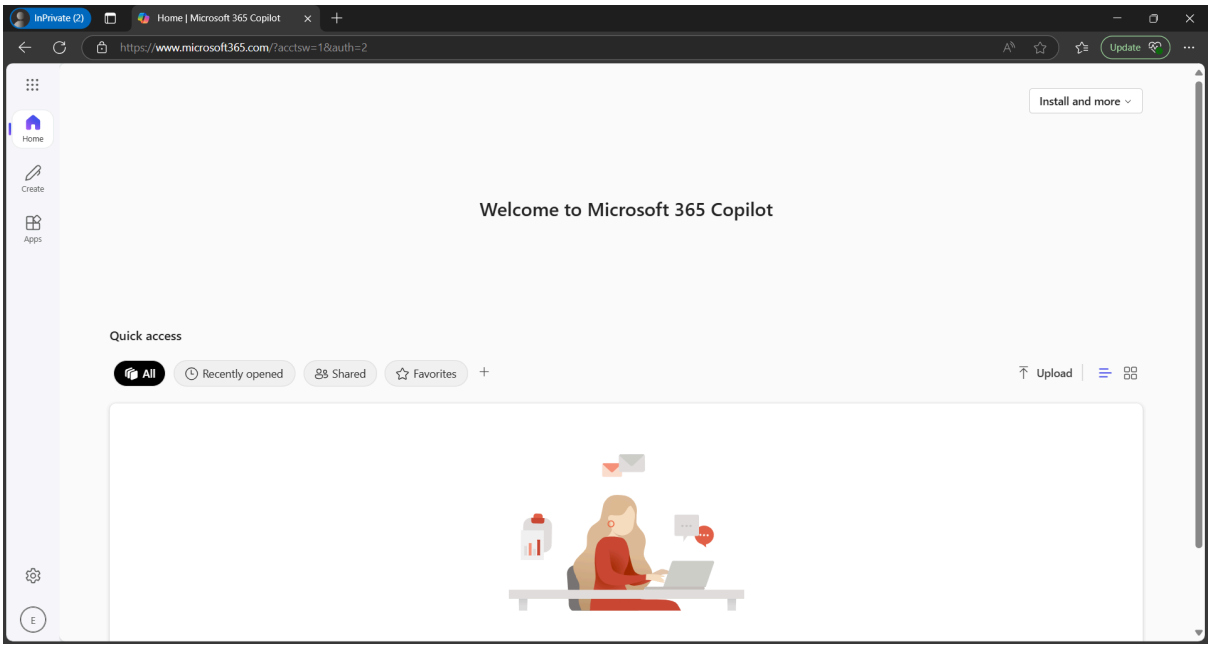
5. Enter your security **PIN** and click **Ok** to continue



6. **Touch** the YubiKey when prompted



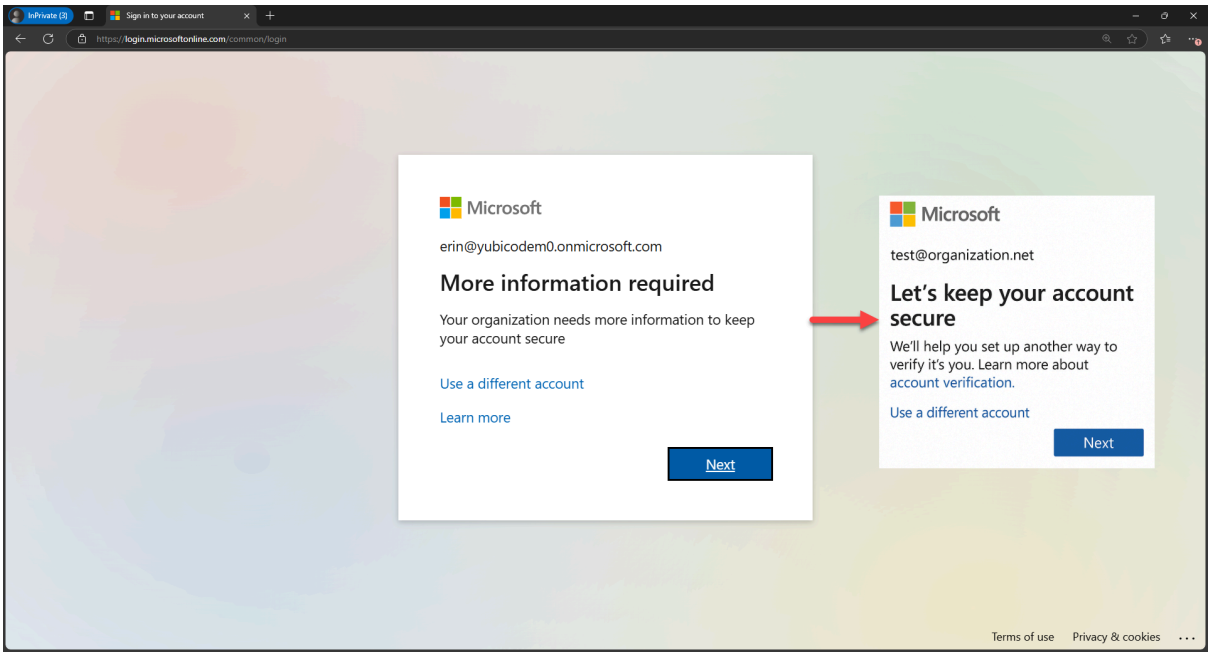
7. You have satisfied the authentication strength and will be signed-in to Office 365



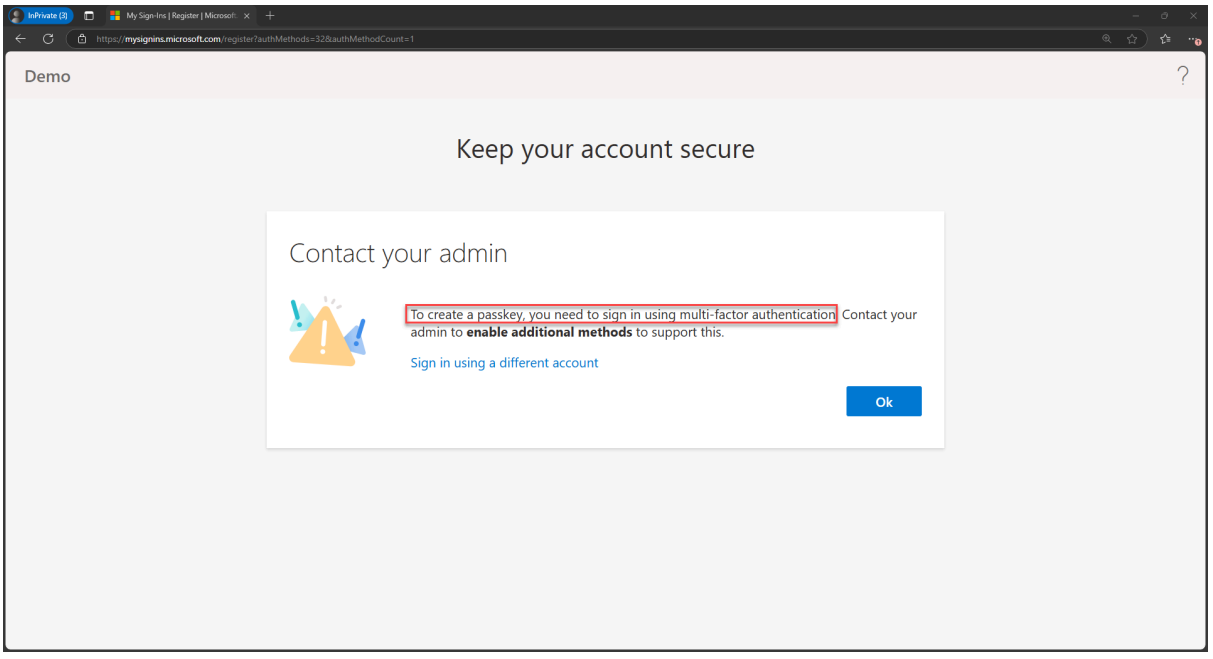
Scenario 2: User is MFA Incapable and begins sign-in with password

1. 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.



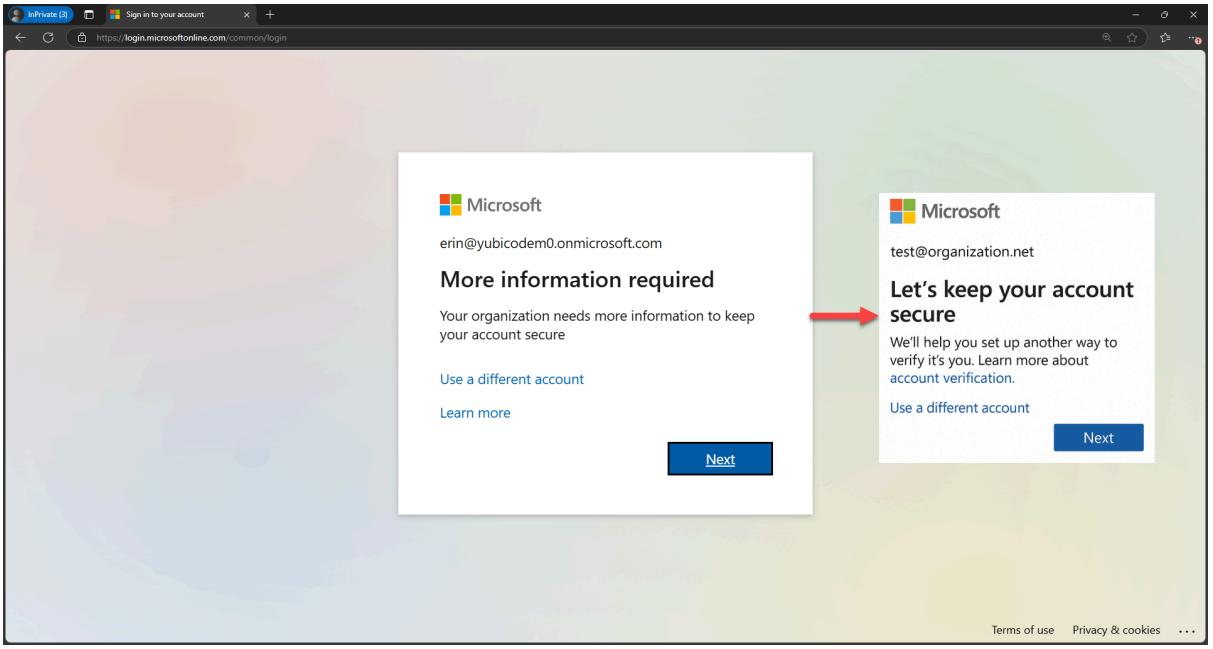
2. The following page will be presented notifying you that **you will need to sign-in with multifactor authentication to create a passkey**. Note that you will not be able to proceed from this point



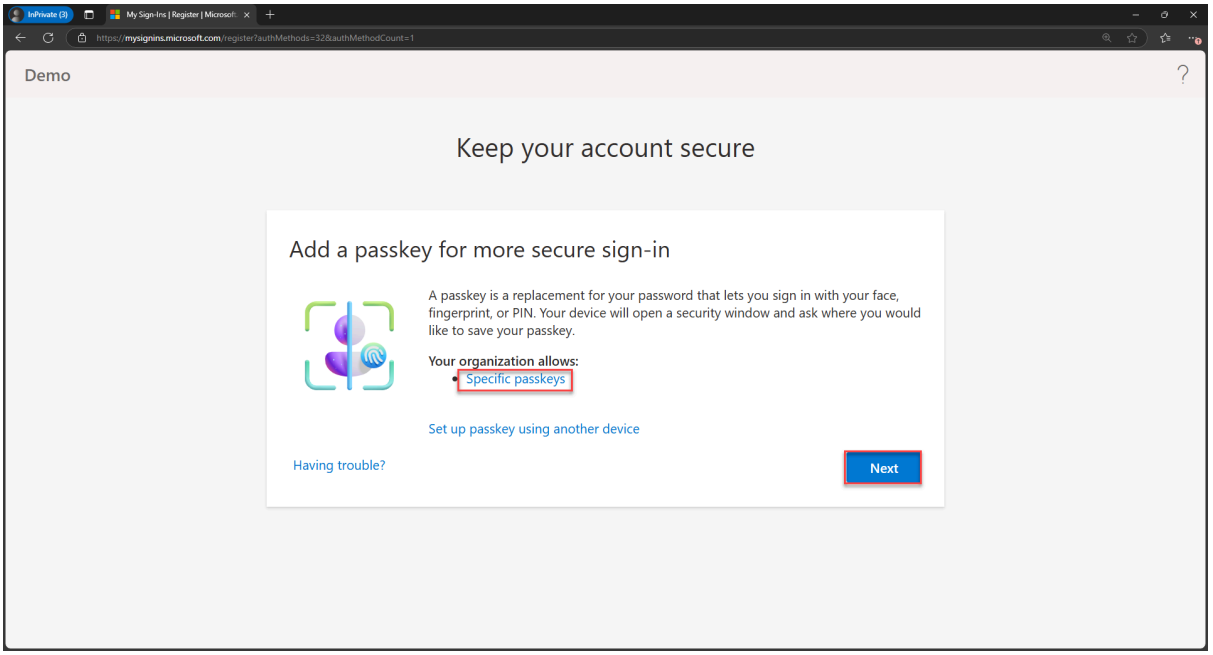
Scenario 3: MFA Capable - Signing-in with MFA using an approved security key

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.

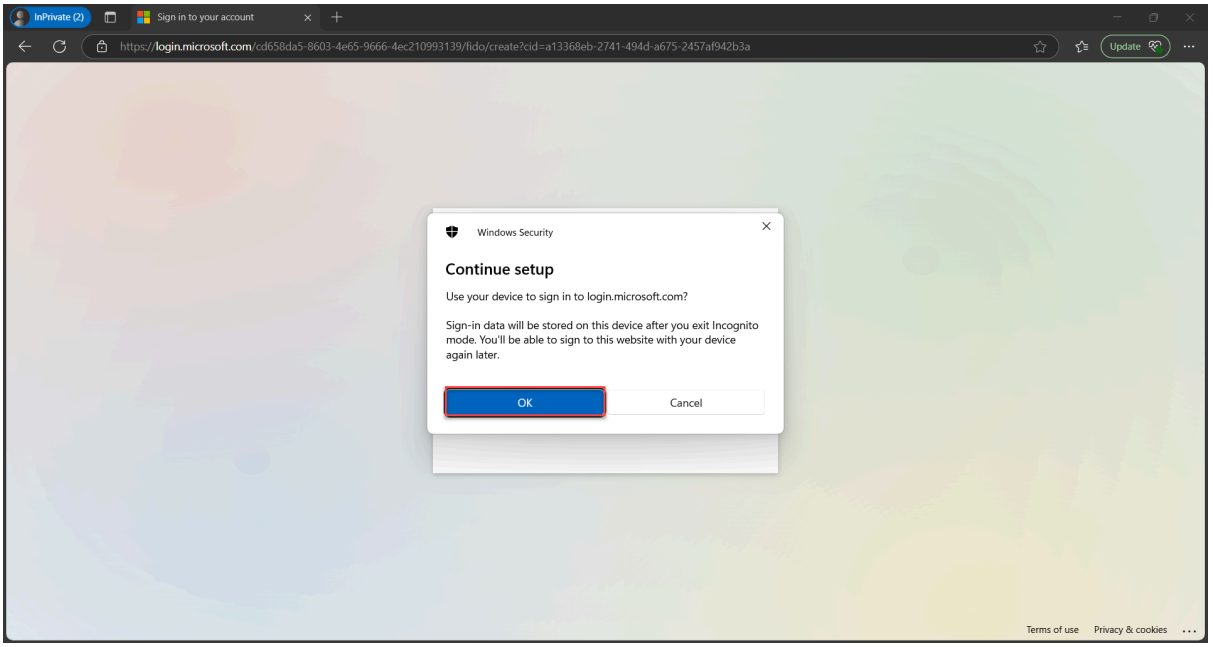
1. Sign-in using a TAP or after satisfying MFA, you will receive one of the two following notifications:
    a. Click **Next**



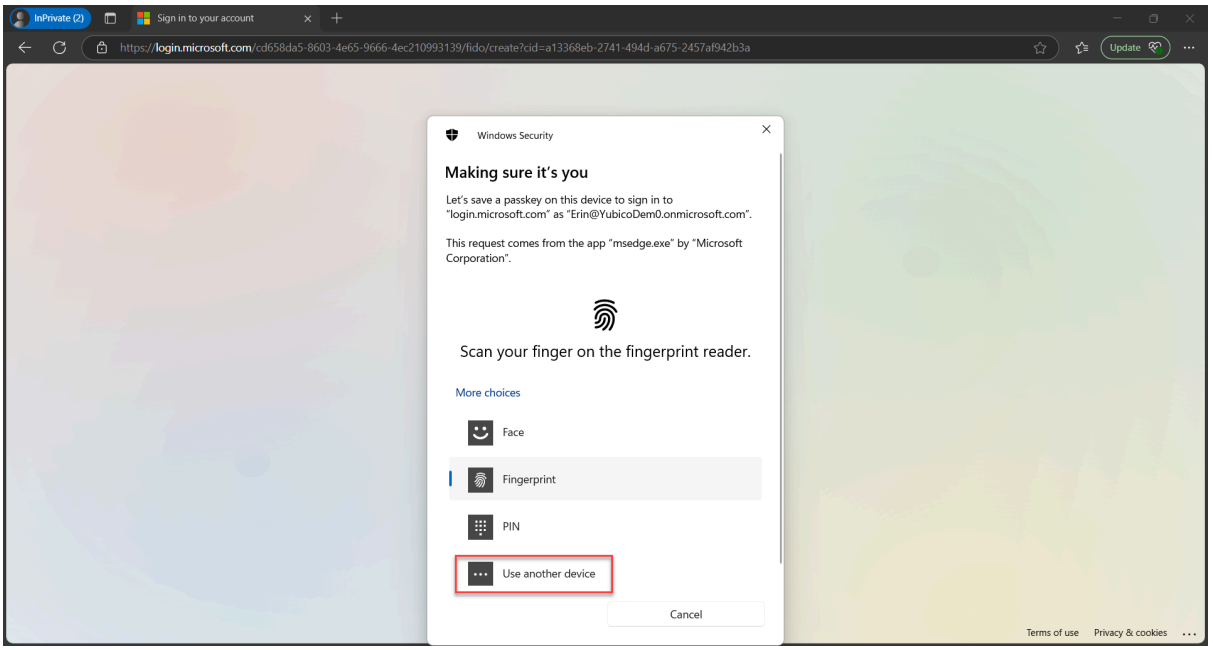
2. You will be guided through the **interrupt-mode** experience of registering an approved security key. You can click on **Specific passkeys** to view supported AAGUIDs.
    a. Click **Next**



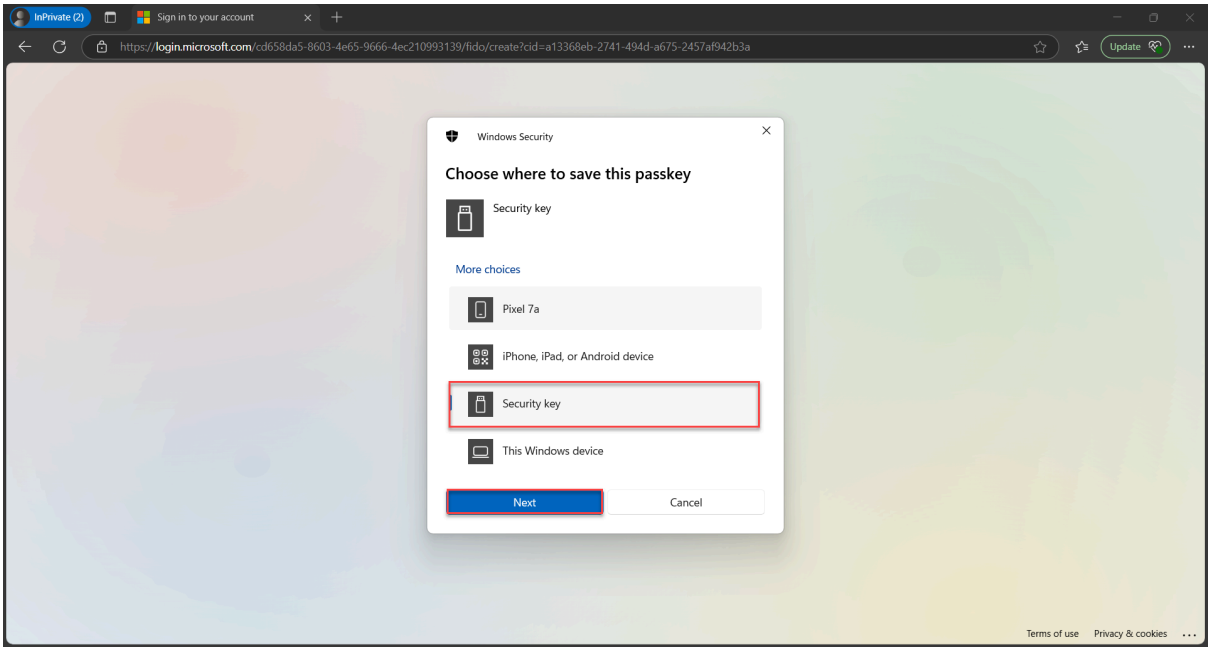
3. Click **Ok**



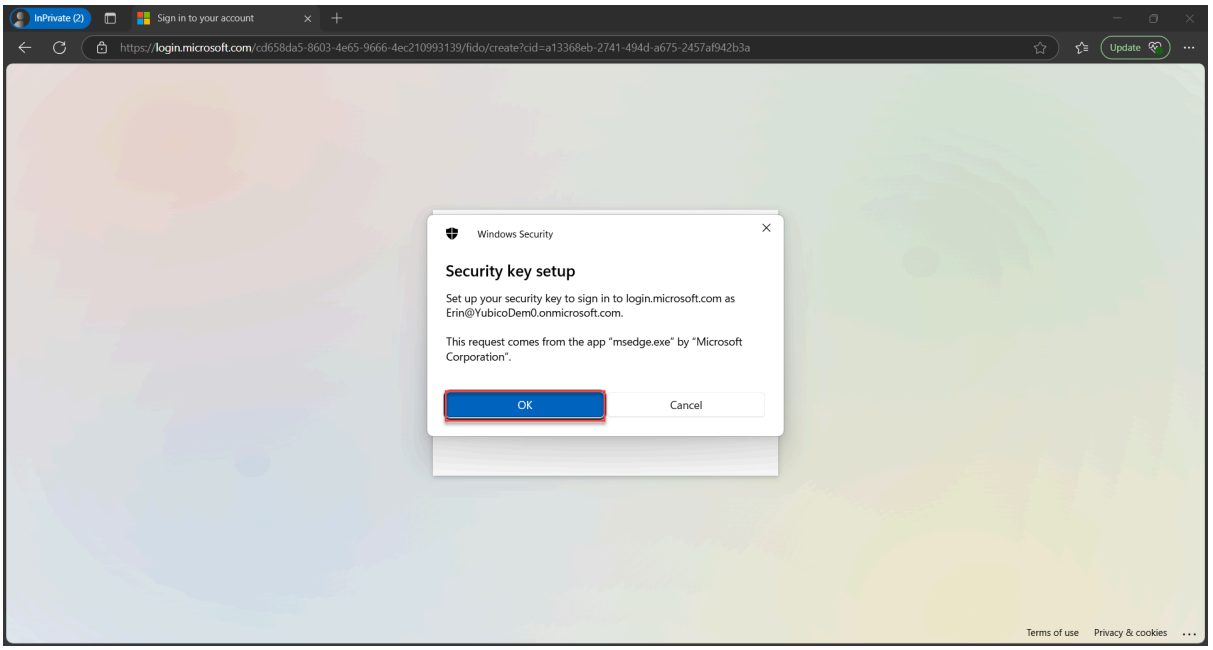
4. Select **Use another device**



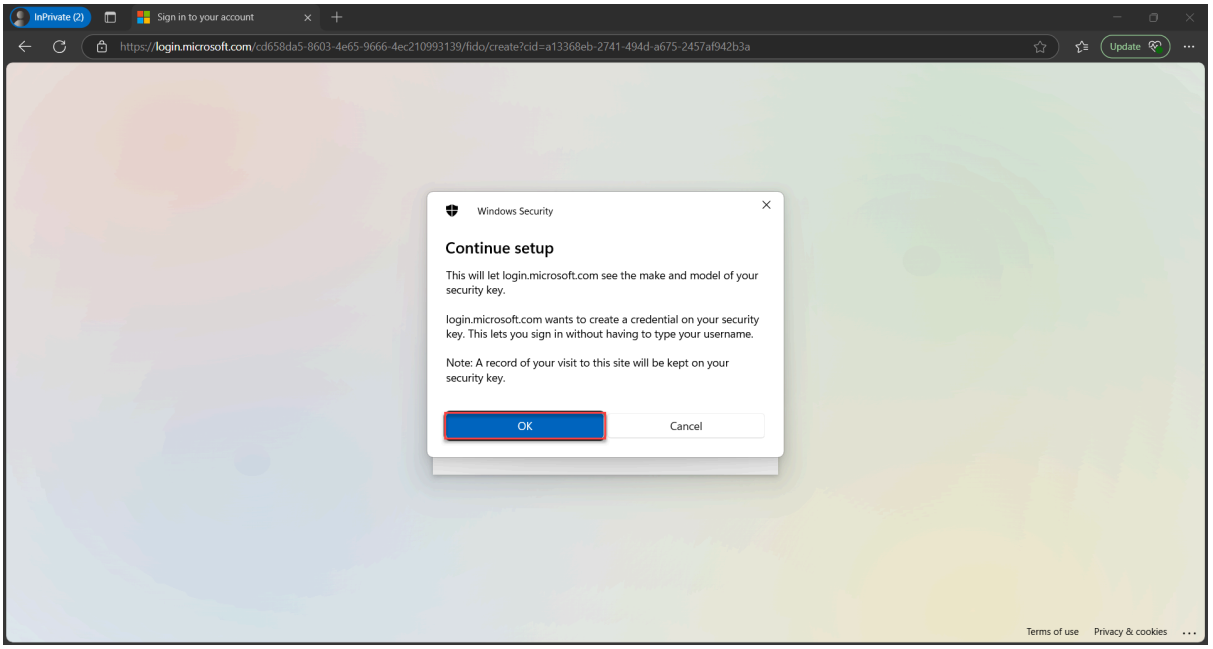
5. Select **Security Key**



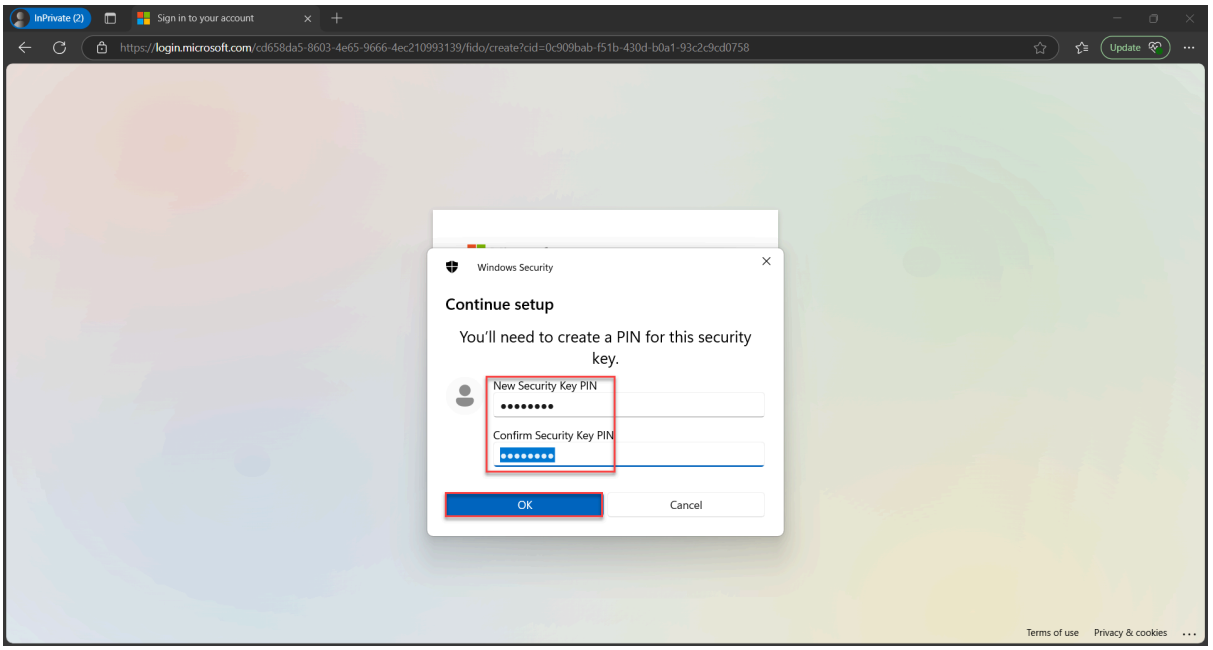
6. Click **Ok** to allow you to setup you YubiKey to sign-in to Entra ID



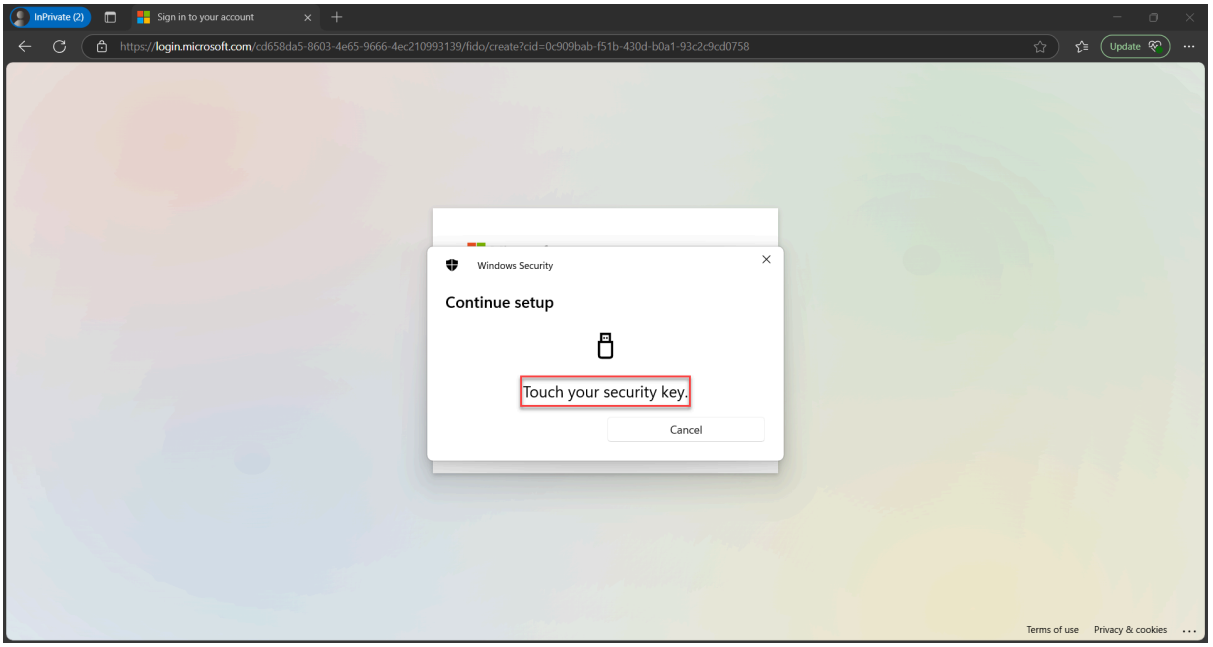
7. Click **Ok** to allow Entra ID to see the make and model of your YubiKey



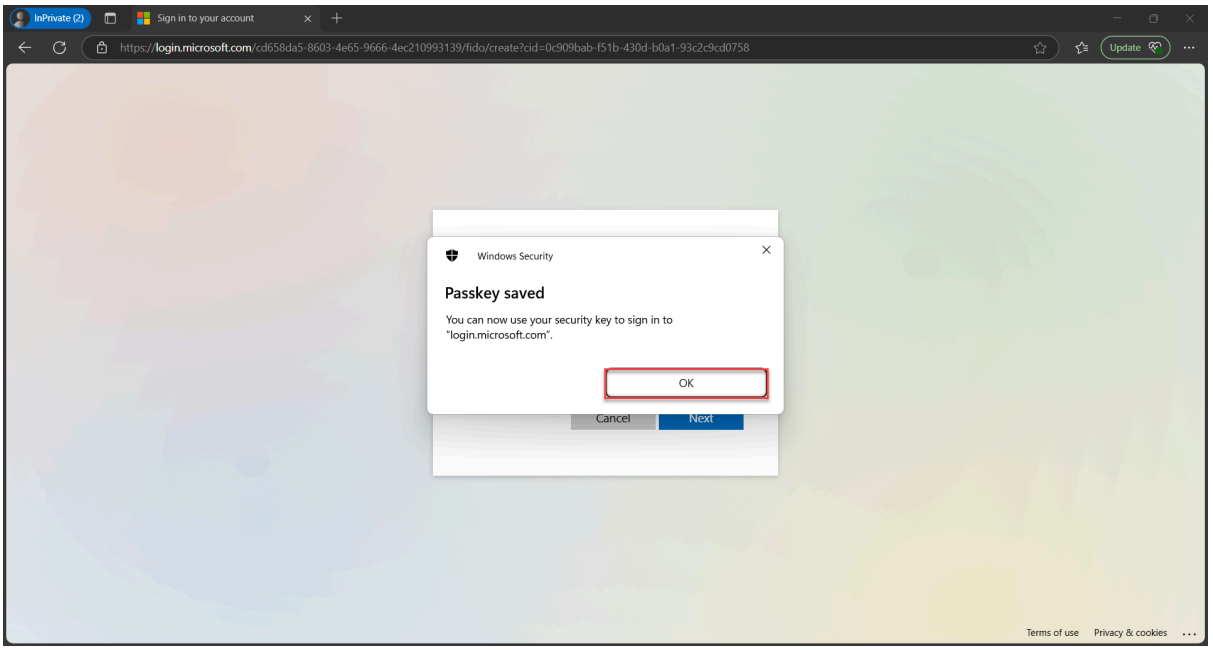
8. Enter a **PIN** and confirm it and click **Ok**



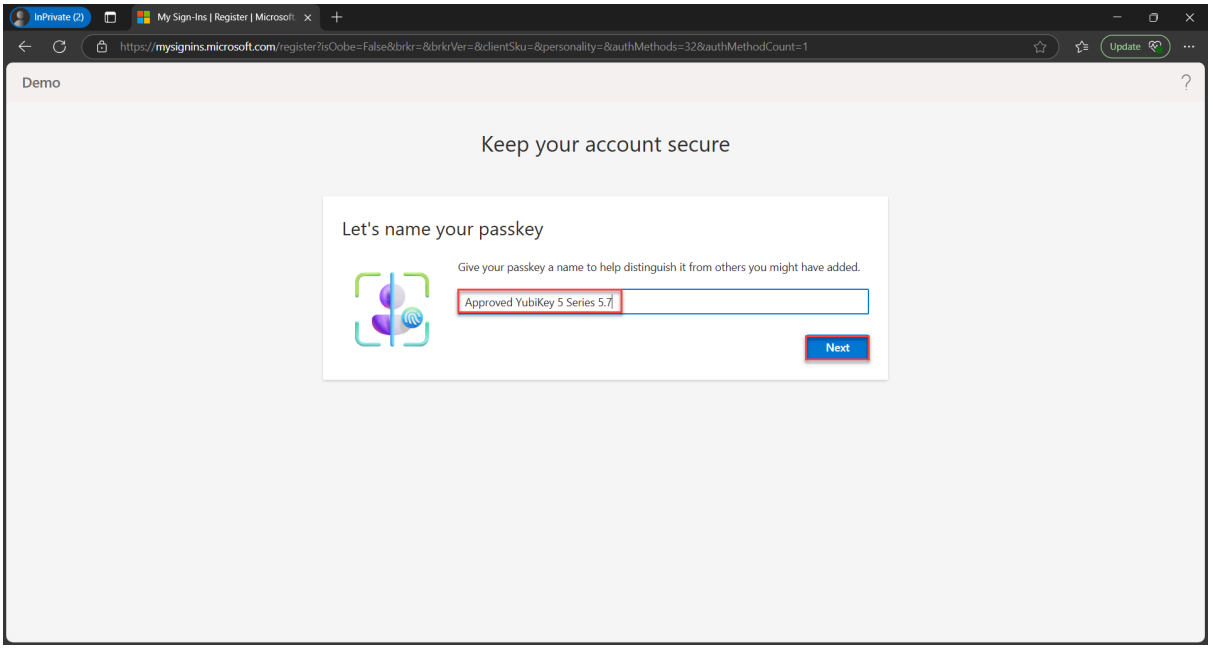
9. **Touch** the YubiKey twice when prompted



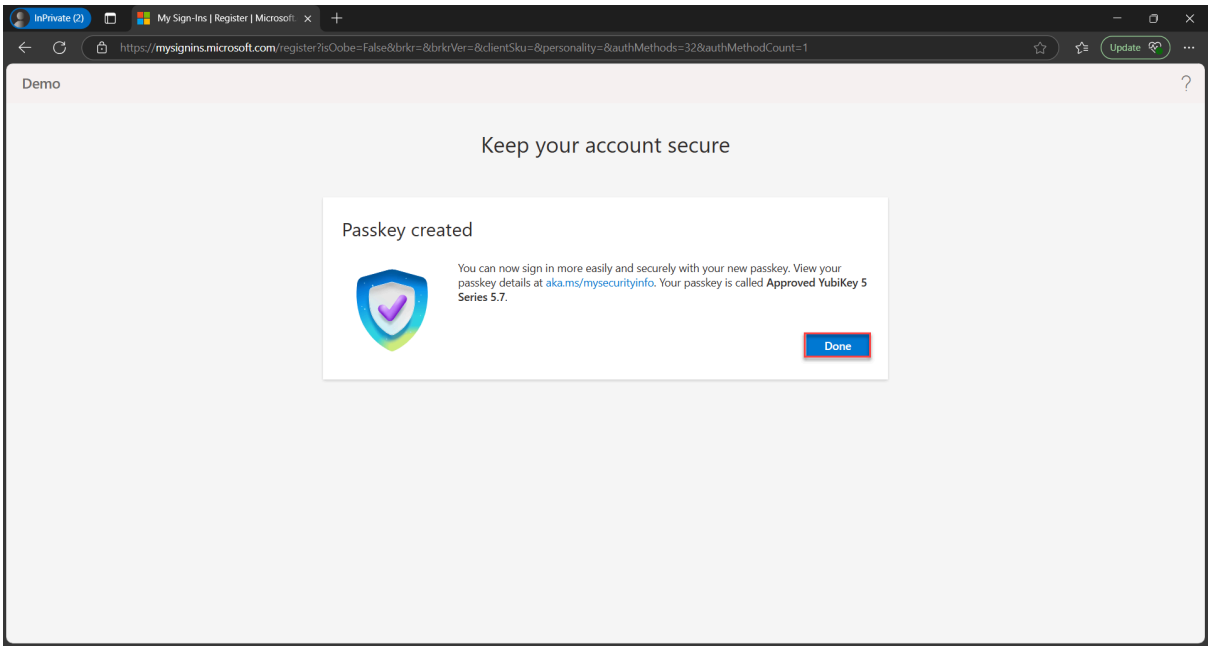
10. The Passkey has been created and saved on the YubiKey. Click **Ok.**



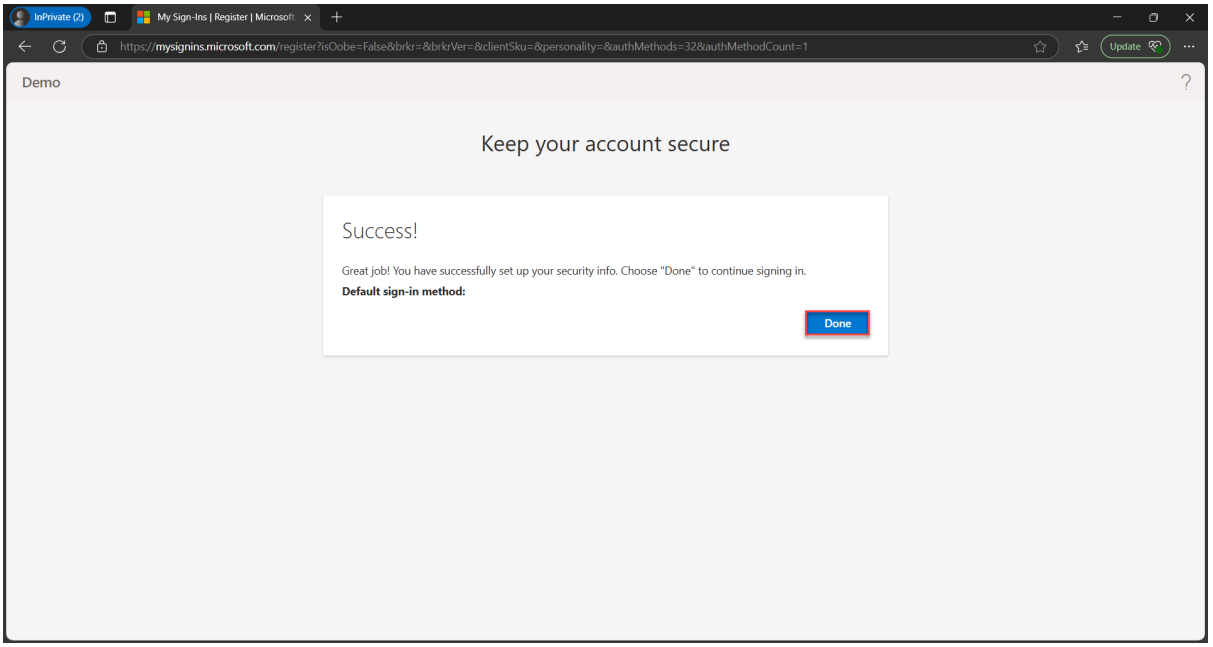
11. Provide a name for your YubiKey and click **Next**



12. Click **Done**



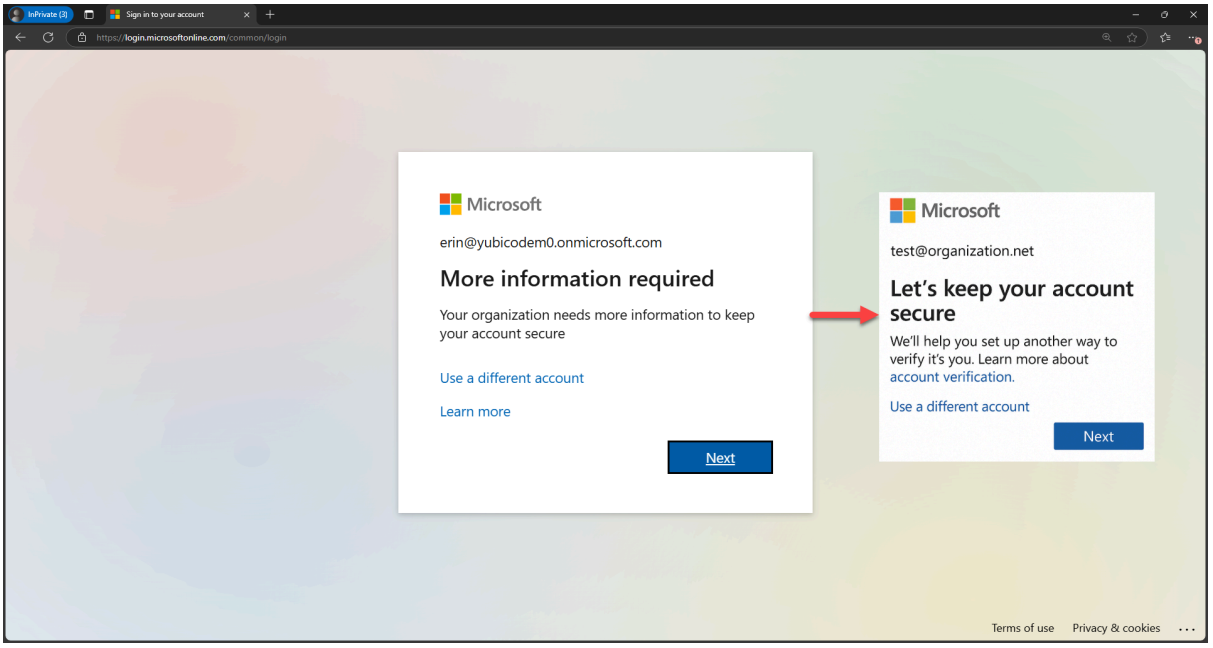
13. Click **Done**. The YubiKey has been successfully registered.



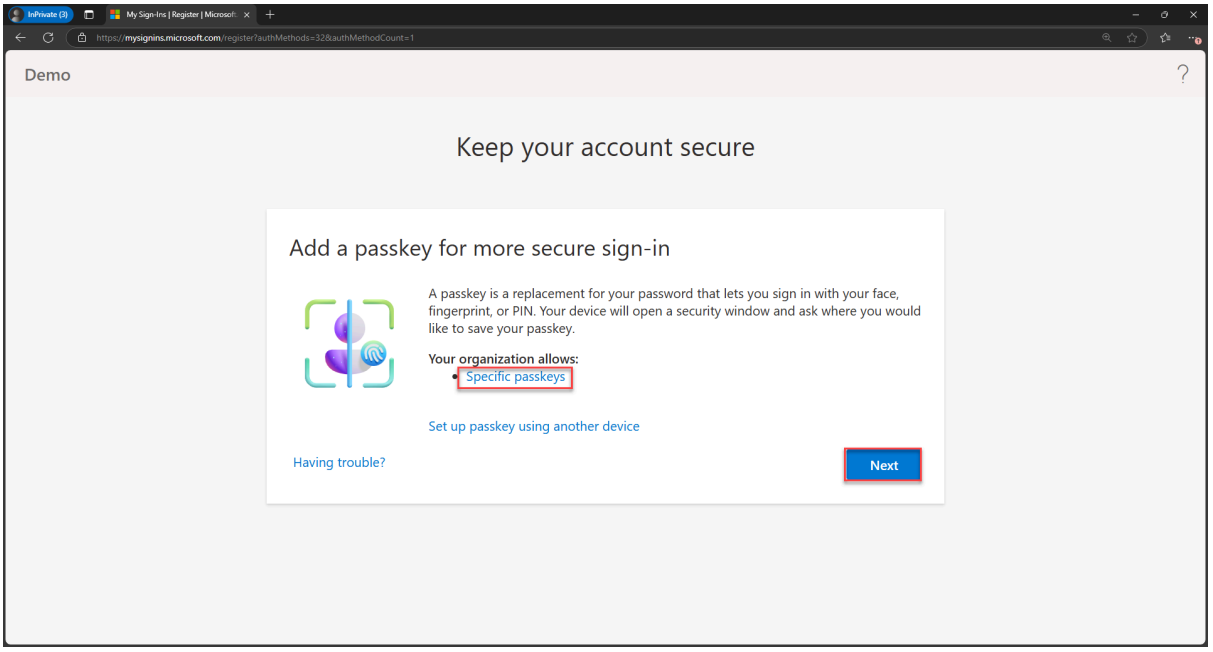
Scenario 4: User is MFA Capable and begins sign-in with MFA and tries register an unapproved security key

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**



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**



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.