YubiKeys for Entra ID passwordless remote desktop guide

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

May 21, 2025

Version History

Version	Date	Changes
1.0	May 21, 2025	• Initial release

Introduction

This document provides guidance on enabling secure remote access to Windows devices using passkeys (FIDO2 credentials) on YubiKeys for authentication using Remote Desktop sessions for session-host and in-session authentication using Microsoft Entra.While remote desktop sessions can be initiated from various client operating systems, **this guide focuses specifically on Windows-based clients.**

Objectives

When using a passkey (FIDO2) on a YubiKey to authenticate to an Entra ID-protected resource, there are two authentication method types:

- **Session Host Authentication** – Used to sign into the Windows desktop at the Windows sign-in screen.
- **In-Session Authentication** – Used to authenticate within an active session, such as through a browser or application prompt.

Before you begin

Support for passkeys (FIDO2) and Remote Desktop connections depends on the client platform's ability to support passkey protocols, most notably the Client to Authenticator Protocol (CTAP) and WebAuthn. CTAP defines how external authenticators, such as FIDO2 security keys, communicate with a client platform. While most modern platforms support these protocols, there are exceptions. For example, dedicated thin clients running specialized operating systems may lack support; in such cases, it is recommended to consult the device vendor to confirm compatibility. For more information, refer to the official Microsoft guidance on client platform support.

Platform support

Microsoft Entra authentication can be used on the following operating systems for both the local and remote device:

- Windows 11 with the 2022-10 Cumulative Updates for Windows 11 (KB5018418) or later installed.
- Windows 10 versions 20H2 or later with the 2022-10 Cumulative Updates for Windows 10 (KB5018410) or later installed.
- Windows Server 2022 with the 2022-10 Cumulative Update for Microsoft server operating system (KB5018421) or later installed.

Minimum Requirements

To connect to a Windows device remotely, the following conditions must be met:

- The device is powered on
- It has active network connectivity
- Remote Desktop is enabled on the device
- The user has permission to initiate a Remote Desktop connection
- The remote device is Entra joined or Entra hybrid joined
- For in-session authentication, you are using a supported browser
- You have registered a passkey (FIDO2) on your YubiKey

There's no requirement for the local device to be joined to a domain or Microsoft Entra ID. As a result, this method allows you to connect to the remote Microsoft Entra joined device from:

- Microsoft Entra joined or Microsoft Entra hybrid joined device in the same tenant
- Active Directory joined device
- Non-joined

Hardware

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

Software

- The following The Remote Desktop Connection clients are supported for Windows:
    - MSTSC.exe for Windows Client 10+
    - MSTSC.exe for Windows Server 2022+

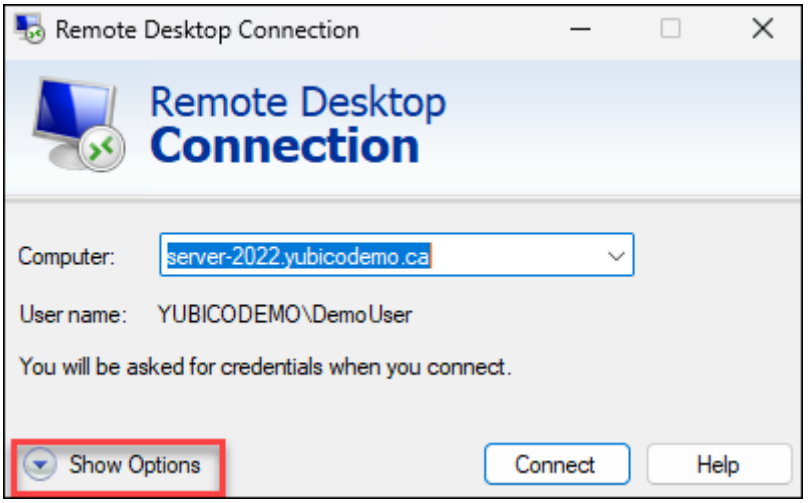
  For a full list of supported clients and platforms refer to the official Microsoft resource

Prerequisites

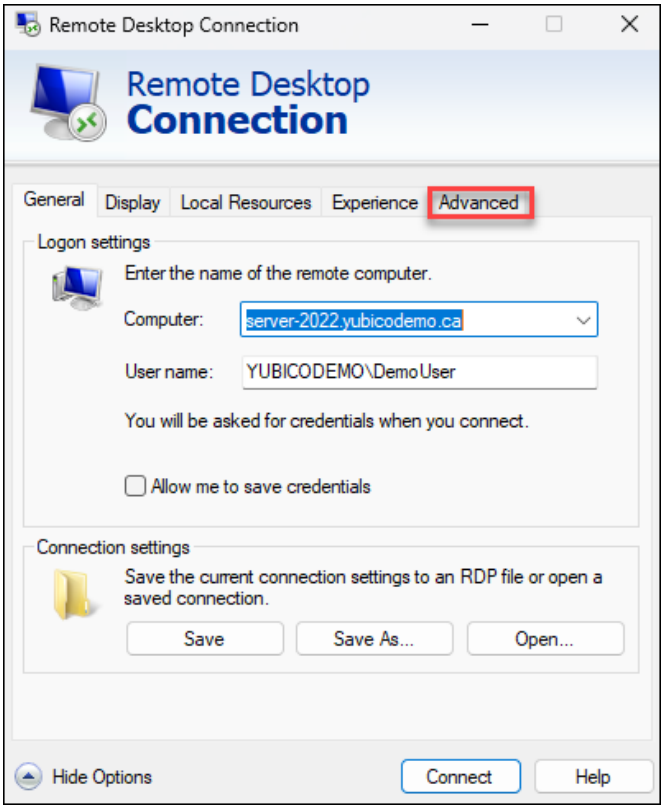
- Both devices (local and remote) must be running a supported version of Windows.
- Follow the instructions to enable Remote Desktop for your device
- If the user who joined the device to Microsoft Entra ID is the only one who is going to connect remotely, no other configuration is needed. To allow more users or groups to connect to the device remotely, you must add users to the Remote Desktop Users group on the remote device.
    - Follow the instructions to add cloud-only users created in Entra ID to Entra joined devices
- The remote device must be accessible using its hostname preferably the FQDN
- Ensure Remote Credential Guard is turned off on the device you're using to connect to the remote device.

Session host authentication

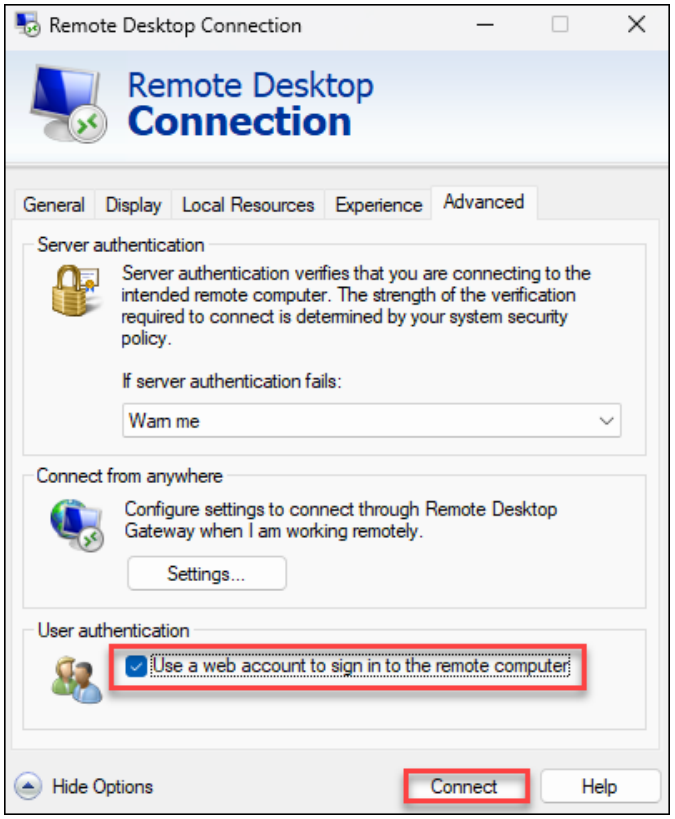
1. Insert the YubiKey
2. Launch the **Remote Desktop Connection** app on the local device
    a. Enter the **FQDN** of the remote device
    b. Click the drop-down menu beside **Show Options**



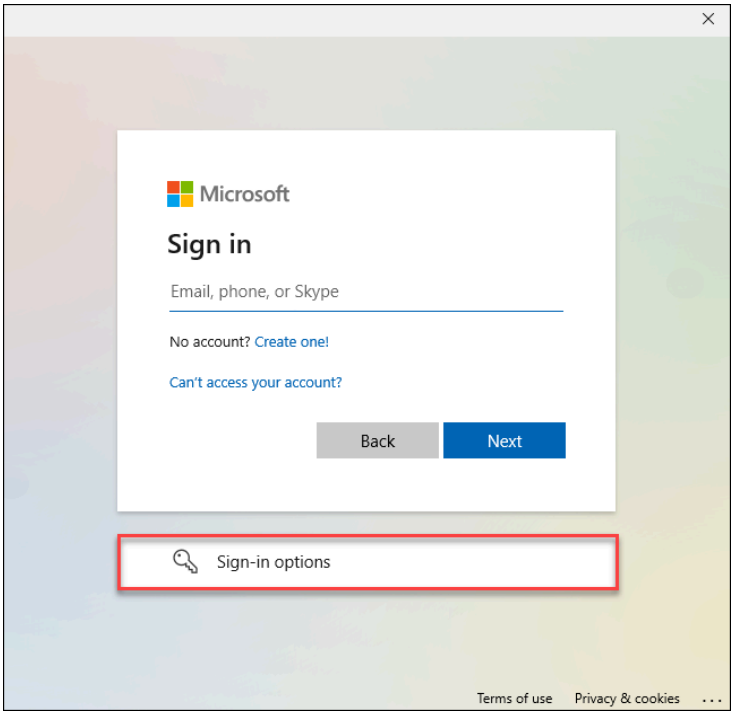
3. Select **Advanced**



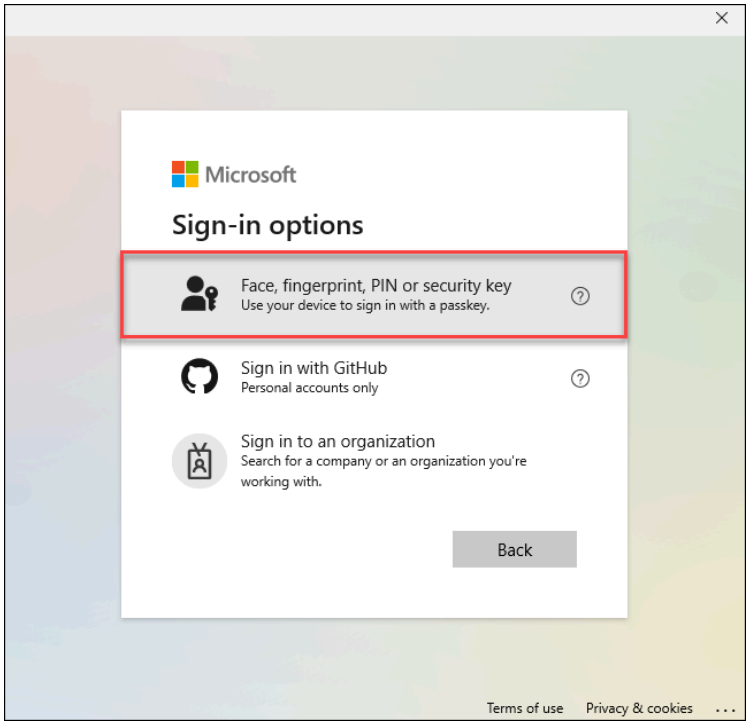
4. Under **User authentication**, click the checkbox besides the **Use a web account to sign in to the remote computer**
    a. Click **Connect** to establish a connection



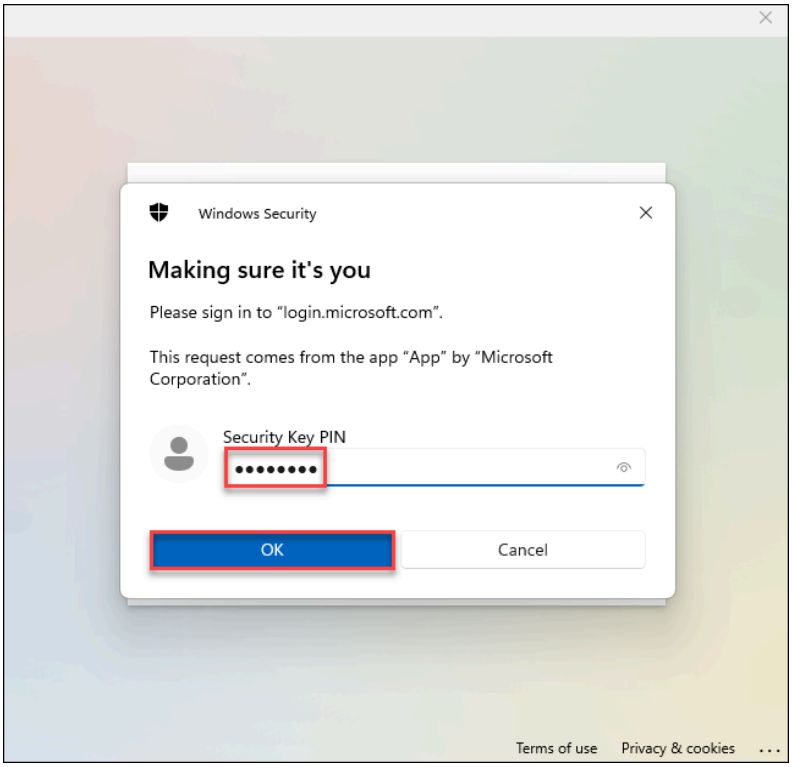
5. The modern authentication prompt will appear
    a. Click **Sign-in options**



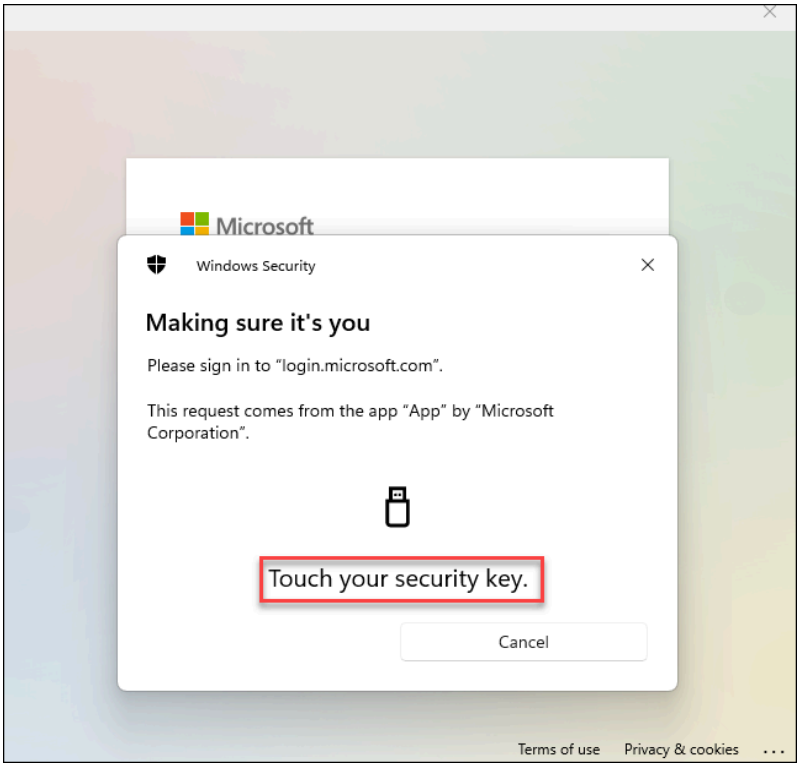
6. Select the **Face, fingerprint, PIN or security key** option



7. When prompted to enter your **PIN** or if you have a YubiKey Bio, you will be prompted to provide your **fingerprint**
    a. Click **Ok**



8. **Touch** the YubiKey when prompted

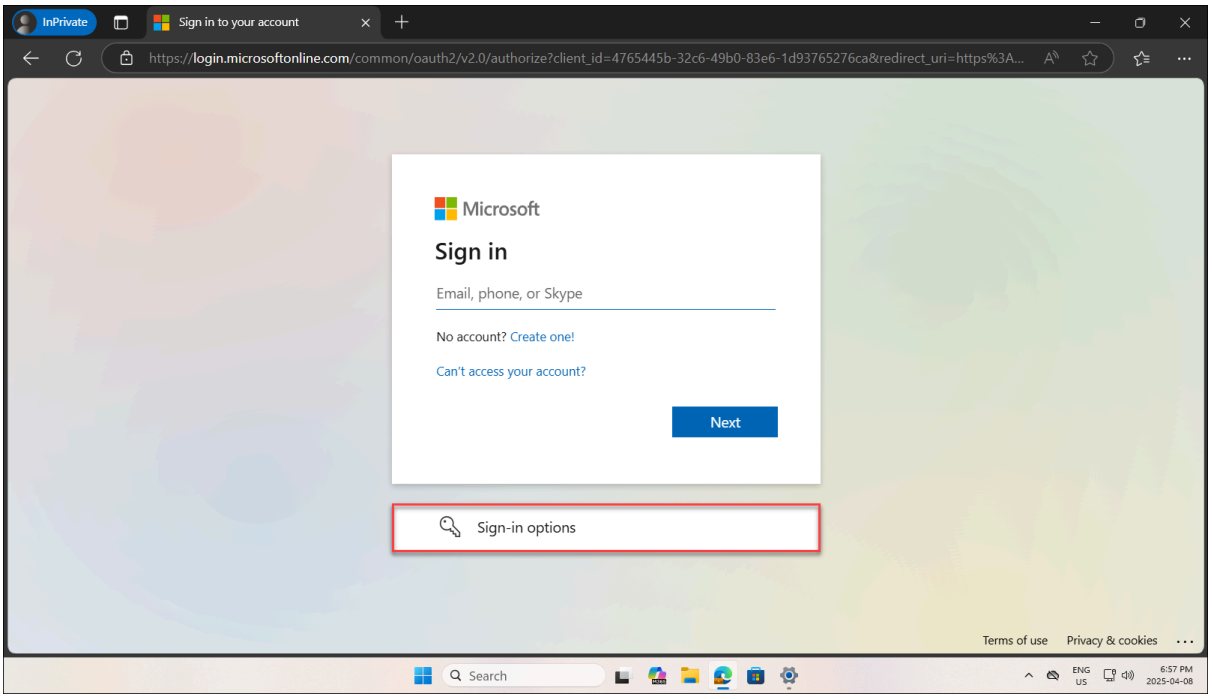


9. You will be signed-in to the remote session

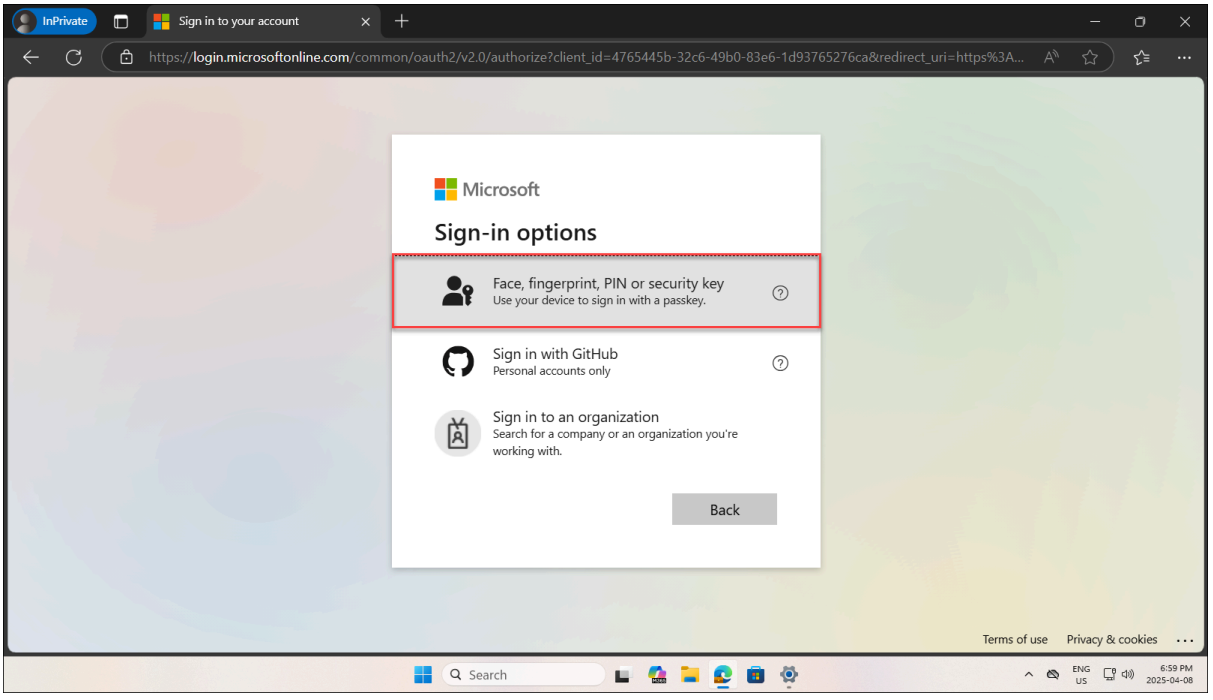
In-session authentication

These instructions demonstrate how to sign-in to the Office 365 portal, however you can sign-in to any web application you have access to that is connected to Entra ID.

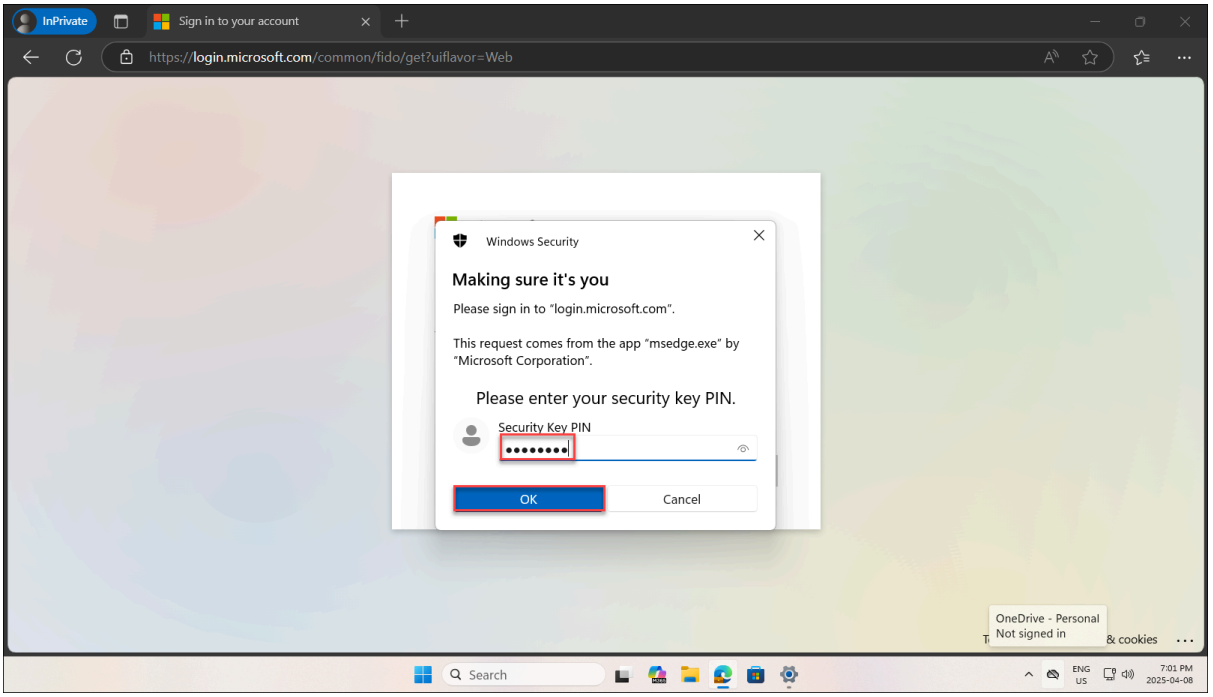
1. Within the remote session, launch a browser and navigate to https://portal.office.com
2. At the Sign in prompt select **Sign-in options**



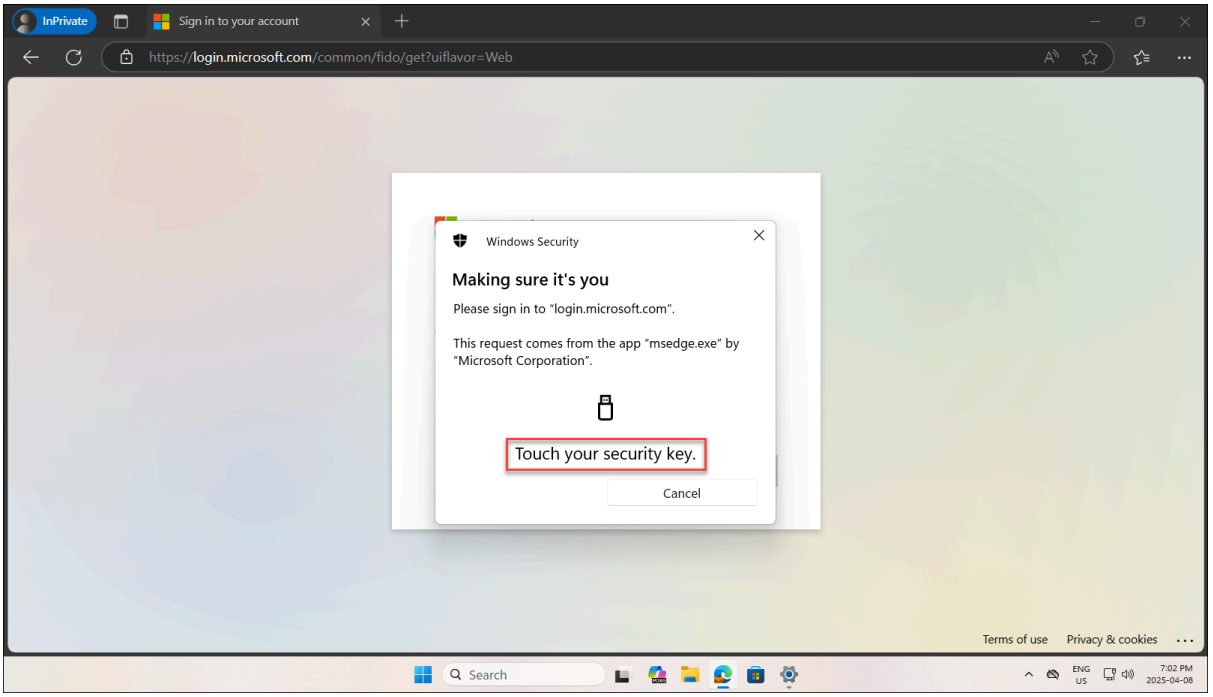
3. At the Sign-in options screen select the **Face, fingerprint, PIN or security key** option



4. Enter your **PIN** and click **Ok.** Note if you are using a YubiKey Bio, you will be prompted to touch your key and provide your fingerprint.



5. **Touch** your YubiKey to complete the authentication



6. You should now be signed in to Office 365