

NT KONF

25. – 27.
SEPTEMBER
2023
PORTOROŽ

**NT
KONF**
NT KONFERENCA



25. – 27.
SEPTEMBER
2023
PORTOROŽ

Microsoft Passwordless Authentication in Microsoft 365 - Azure AD - how to

Tomislav Lulić
World Bank Croatia



Tomislav Lulić

World Bank office in Croatia
IT analyst
Microsoft MVP, MCT



@tlulic
tlulic.wordpress.com
tomislav@tlulic.com
www.linkedin.com/tomislavlulic

Agenda

- Why password
- Zero Trust
- Passwordless authentication
- DEMO

Why password? ...or not?

- Passwords are a primary attack vector.
- Bad actors use social engineering, phishing, and spray attacks to compromise passwords.

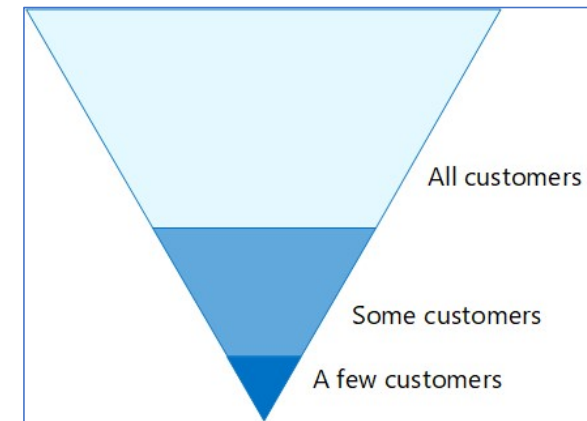
A passwordless authentication strategy mitigates the risk of these attacks.

Why Zero Trust - Zero Trust principles













- **Verify explicitly**
 - Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies
- **Use least-privilege access**
 - Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive policies, and data protection to help secure both data and productivity
- **Assume breach**
 - Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses

Zero Trust Security

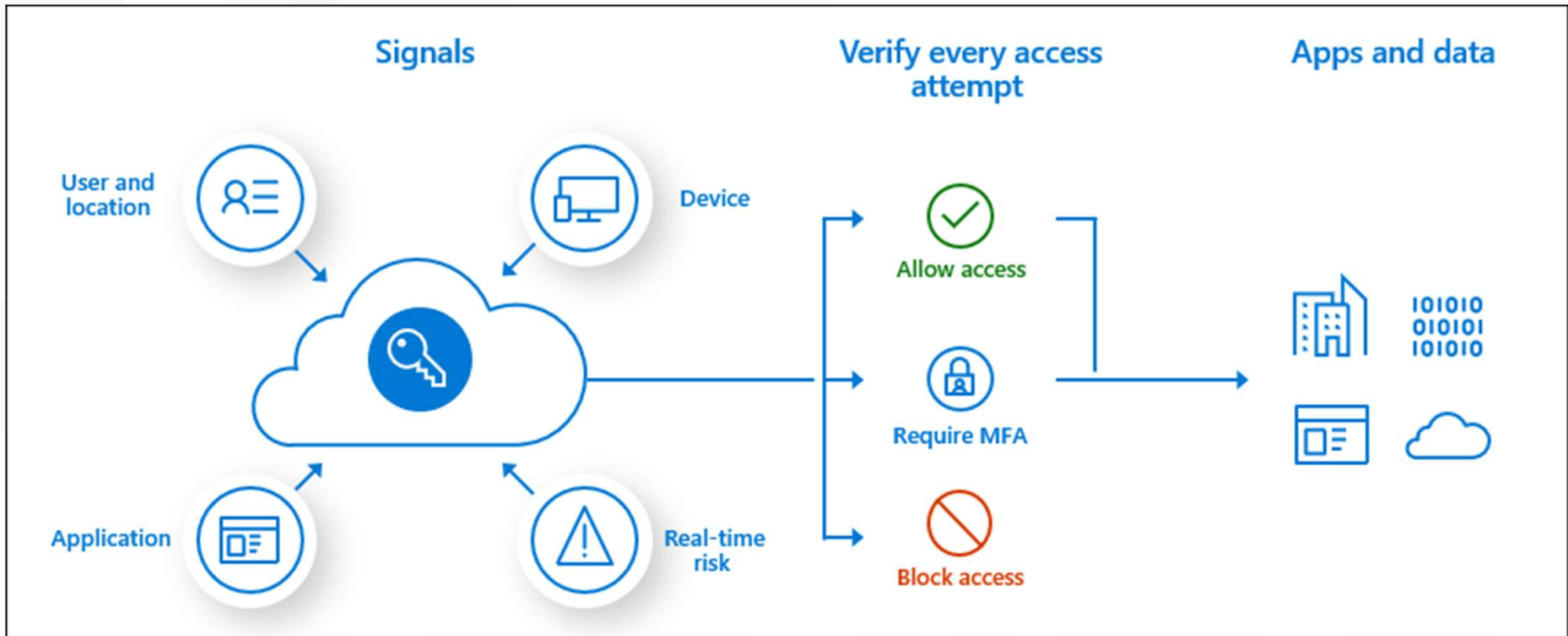
- Never trust, always verify 😊
- Possible to implement Zero Trust on all platforms
- Every request treated as originates from an untrusted network, regardless of its actual source or network location
- Data and apps remain secure even if a device or user's credential are compromised



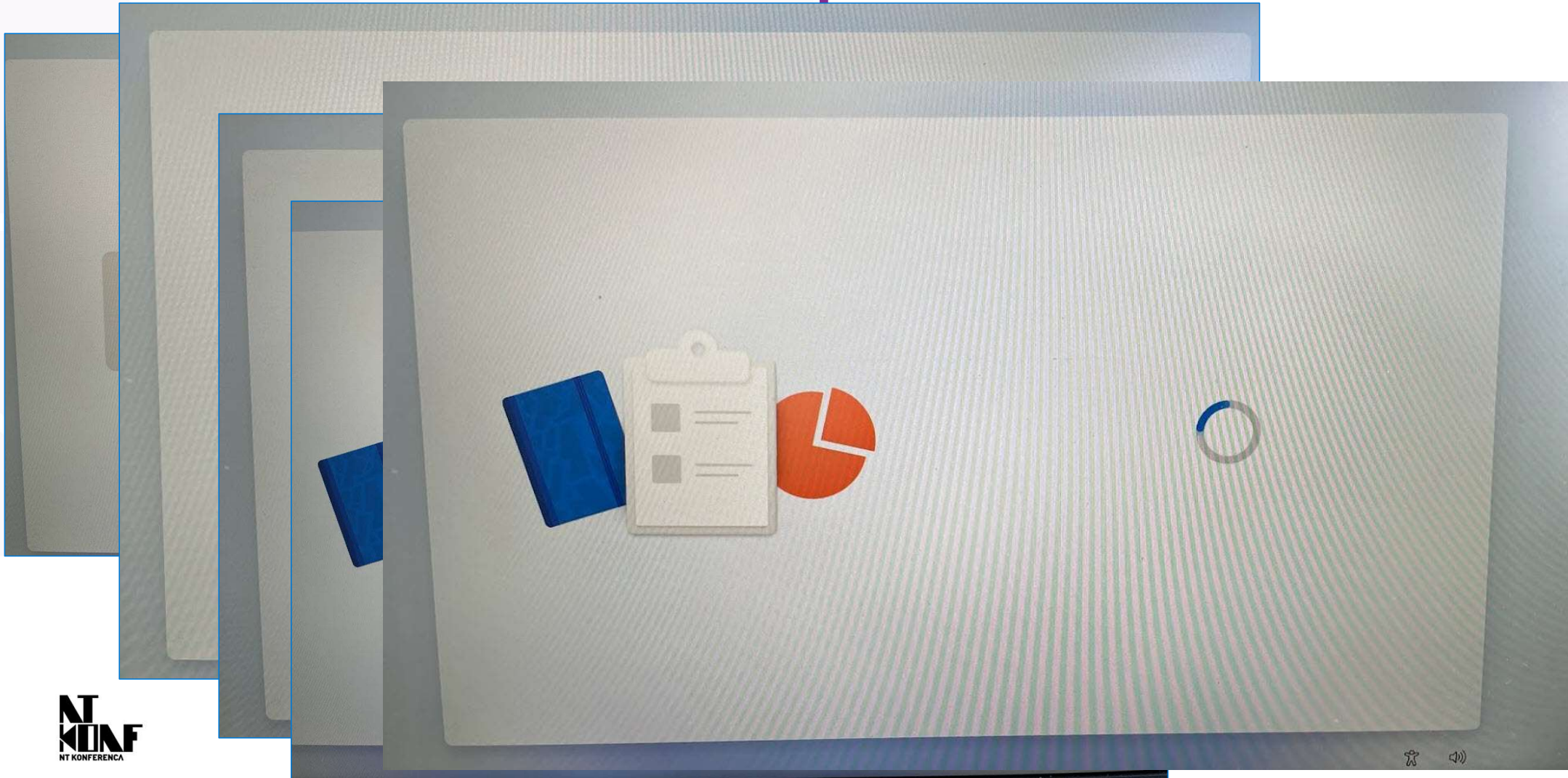
Zero Trust strategy in passwordless

Bad  Password (Only)	Good  Password +	Better  Password +	Best Passwordless 
123456	 SMS	 Authenticator (Push notifications)	 Windows Hello
qwerty			
password	 Voice	 Software Tokens OTP	 Authenticator (Phone Sign-in)
Iloveyou			
Password1		 Hardware Tokens OTP (Preview)	 FIDO2 security key

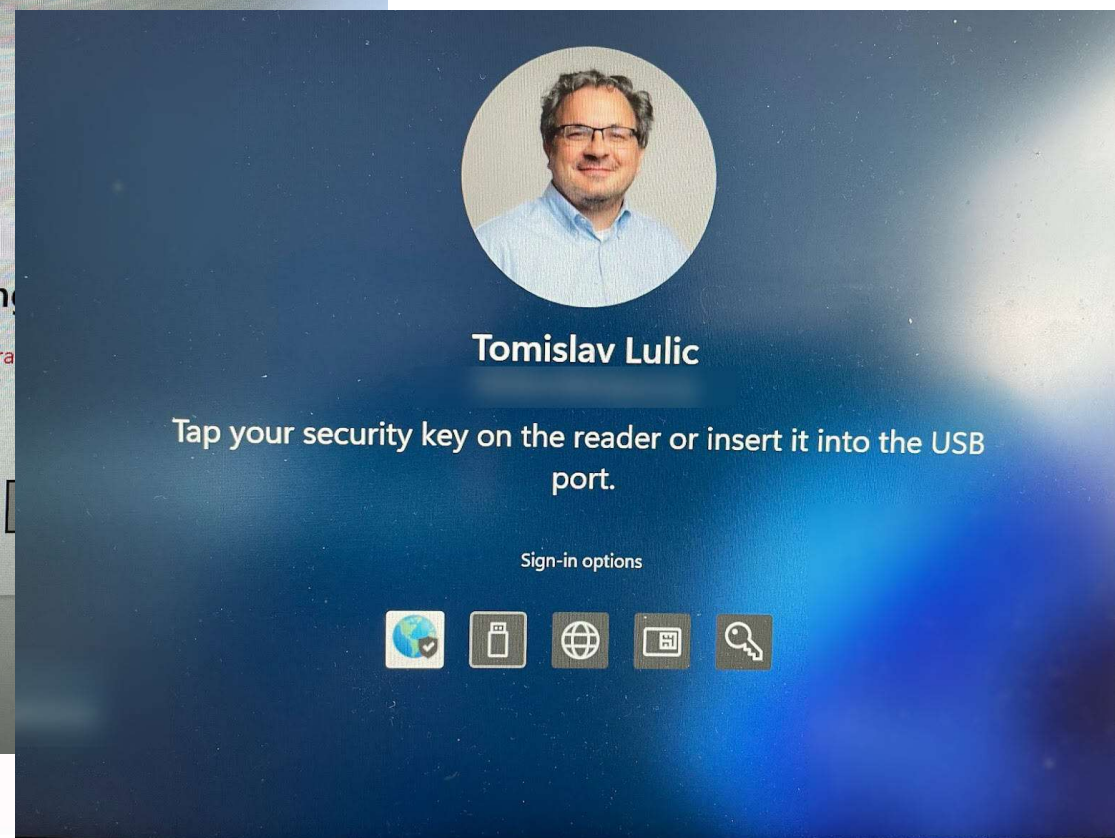
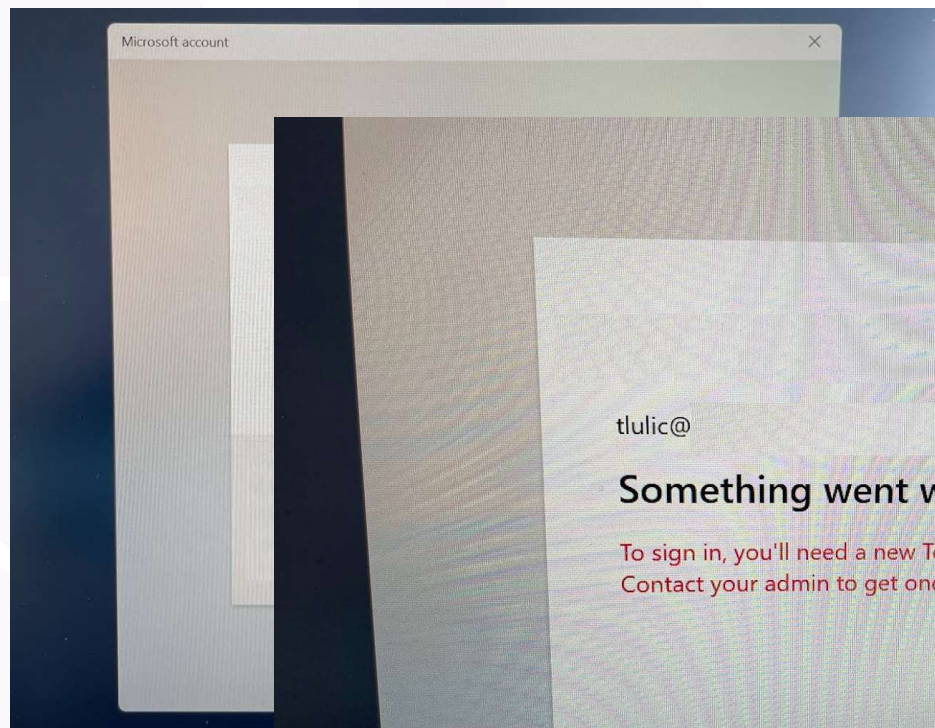
Plan Conditional Access policies



Passwordless with Autopilot – from field



Continuing setup



Passwordless authentication - options

Microsoft offers the following three passwordless authentication options that integrate with Azure Active Directory (Entra ID):

- **Microsoft Authenticator** - turns any iOS or Android phone into a strong, passwordless credential by allowing users to sign into any platform or browser.
- **FIDO2-compliant security keys** - useful for users who sign in to shared machines like kiosks, in situations where use of phones is restricted, and for highly privileged identities.
- **Windows Hello for Business** - best for users on their dedicated Windows computers.

Common policies for Azure AD Multi-Factor Authentication

Common use cases to require Azure AD Multi-Factor Authentication include:

- For [administrators](#)
- To [specific applications](#)
- For [all users](#)
- For [Azure management](#)
- From [network locations you don't trust](#)

Authentication methods

Authentication method	Manage from	Scoping
Microsoft Authenticator (Push notification and passwordless phone sign-in)	MFA settings or Authentication methods policy	Authenticator passwordless phone sign-in can be scoped to users and groups
FIDO2 security key	Authentication methods policy	Can be scoped to users and groups
Software or Hardware OATH tokens	MFA settings	
SMS verification	MFA settings Manage SMS sign-in for primary authentication in authentication policy	SMS sign-in can be scoped to users and groups.
Voice calls	Authentication methods policy	

How to go passwordless

If my account doesn't have a password, how will I sign in?

- Once you remove your password from your account, you will need to sign in using a passwordless method like the Microsoft Authenticator app, Windows Hello, physical security keys, or SMS codes.

Will my account be secure?

- Yes!
- Using alternative sign-in methods like the Microsoft Authenticator App, physical security keys, and biometrics are more secure than traditional passwords which can be stolen, hacked, or guessed.

Can I use passwordless everywhere?

NO!

- After you enable two-step verification and go passwordless, some apps or older devices (including Outlook 2010, Xbox 360, and mail-sending devices like security cameras) will each need an app password.
- Use app password...

<https://account.live.com/proofs/AppPassword>

Temporary Access Pass (TAP)

- is a time-limited passcode that can be configured for single use or multiple.
- Users can sign in with a Temporary Access Pass to onboard other authentication methods including passwordless methods such as Microsoft Authenticator, FIDO2 or Windows Hello for Business.
- A TAP also makes recovery easier
 - when a user has lost or forgotten their strong authentication factor
 - FIDO2 security key
 - Microsoft Authenticator app
 - or needs to sign in to register new strong authentication methods.

Create a Temporary Access Pass

Roles and Actions related to a Temporary Access Pass (TAP).

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

Direct Phone Sign-in registration

- Directly within the Microsoft Authenticator app without the need to first registering Microsoft Authenticator with their account, all while never accruing a password. Here's how:
 1. Acquire a [Temporary Access Pass](#) from your Admin or Organization.
 2. Download and install the Microsoft Authenticator app on your mobile device.
 3. Open Microsoft Authenticator and click **Add account** and then choose **Work or school account**.
 4. Choose **Sign in**.
 5. Follow the instructions to sign-in with your account using the Temporary Access Pass provided by your Admin or Organization.
 6. Once signed-in, continue following the additional steps to set up phone sign-

How to enable TAP

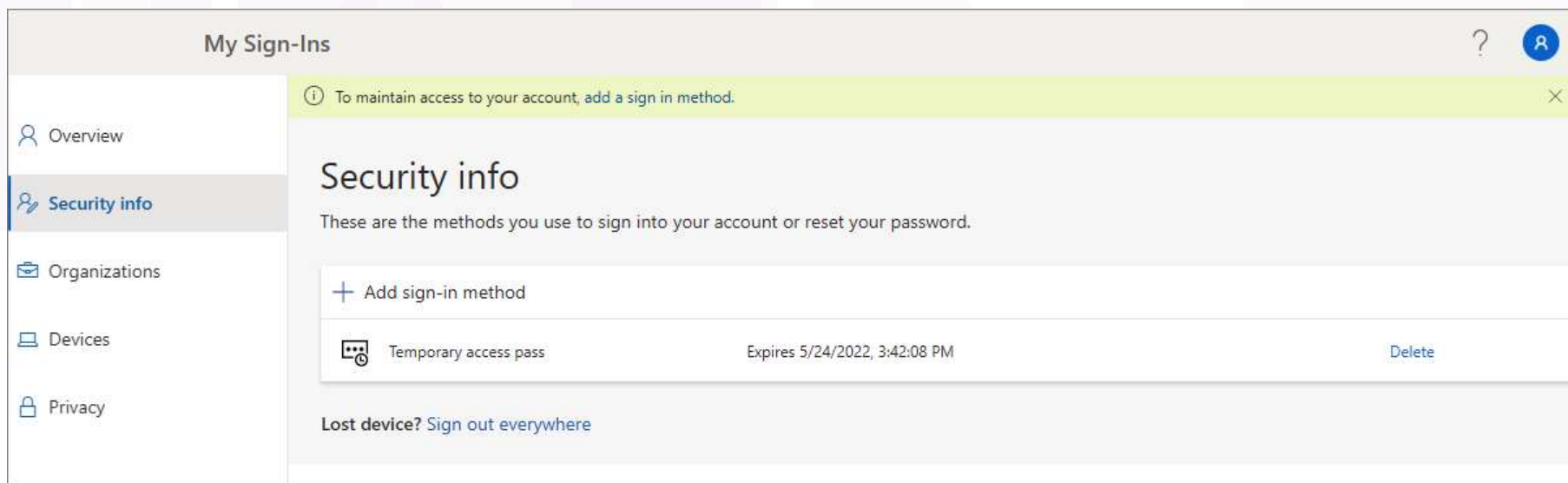
1. Sign in to the [Azure portal](#) using an account with *global administrator* permissions.
2. Search for and select **Azure Active Directory**, then choose **Security** from the menu on the left-hand side.
3. Under the **Manage** menu header, select **Authentication methods > Policies**.
4. From the list of available authentication methods, select **Temporary Access Pass**.

Default value and the range of values

Setting	Default values	Allowed values	Comments
Minimum lifetime	1 hour	10 – 43,200 Minutes (30 days)	Minimum number of minutes that the Temporary Access Pass is valid.
Maximum lifetime	8 hours	10 – 43,200 Minutes (30 days)	Maximum number of minutes that the Temporary Access Pass is valid.
Default lifetime	1 hour	10 – 43,200 Minutes (30 days)	Individual passes within the minimum and maximum lifetime configured by the policy can override default value.
One-time use	False	True/False	When the policy is set to false, passes in the tenant can be used either once or more than once during its validity (maximum lifetime). By enforcing one-time use in the Temporary Access Pass policy, all passes created in the tenant are one-time use.
Length	8	8-48 characters	Defines the length of the passcode.

User management of Temporary Access Pass

- Users managing their security information at <https://aka.ms/mysecurityinfo> see an entry for the Temporary Access Pass.
- If a user does not have any other registered methods, they get a banner at the top of the screen that says to add a new sign-in method.
- Users can also see the TAP expiration time and delete the TAP if it's no longer needed.



Windows device setup

- Users with a TAP can navigate the setup process on Windows 10 and 11 to perform device join operations and configure Windows Hello for Business.
- TAP usage for setting up Windows Hello for Business varies based on the devices joined state.

For joined devices to Azure AD:

- During the domain-join setup process, users can authenticate with a TAP (no password required) to join the device and register Windows Hello for Business.

Windows device setup (cont.)

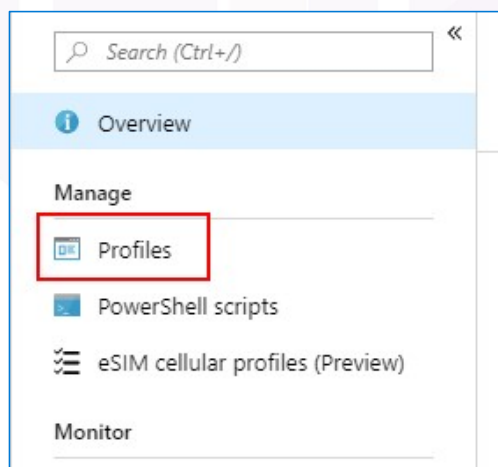
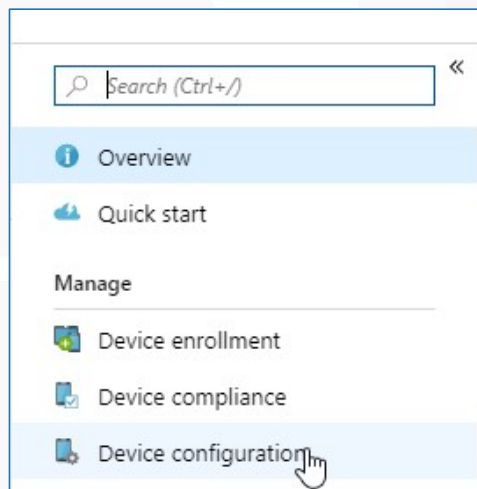
On already-joined devices:

- users must first authenticate with another method such as a password, smartcard or FIDO2 key, before using TAP to set up Windows Hello for Business

If the [Web sign-in](#) feature on Windows is also enabled, the user can use TAP to sign into the device. This is intended only for completing initial device setup, or recovery when the user doesn't know or have a password.

For hybrid-joined devices, users must first authenticate with another method such as a password, smartcard or FIDO2 key, before using TAP to set up Windows Hello for Business.

Web sign-in



A screenshot of the 'Create profile' dialog box. It contains several fields for configuring a new profile:

- Name:** 'Web sign-in' (with a green checkmark icon).
- Description:** 'Enter a description...' (with a green checkmark icon).
- Platform:** 'Windows 10 and later' (dropdown menu).
- Profile type:** 'Custom' (dropdown menu).
- Settings:** 'Configure' (button with a right arrow).
- Scope (Tags):** '0 scope(s) selected' (button with a right arrow).

At the OMA-URI Settings click add and enter the following values

```
Name: Web Sign In
OMA-URI: ./Device/Vendor/MSFT/Policy/Config/Authentication/EnableWebSignIn
Data Type: Integer
Value: 1
```

Use the passwordless methods wizard

- The Microsoft Entra admin center has a passwordless methods wizard that will help you to select the appropriate method for each of your audiences. If you haven't yet determined the appropriate methods, see <https://aka.ms/passwordlesswizard>
- You need administrator rights to access this wizard.



25. – 27.
SEPTEMBER
2023
PORTOROŽ

*This is not school, but we
love to get grades.
Please fill out our
questoineers and leave
us your feedback.
You may even **win** some
cool rewards.*



Account

Enter Temporary Access Pass

rory.larson_0416@woodgrove.ms

Other ways to sign in

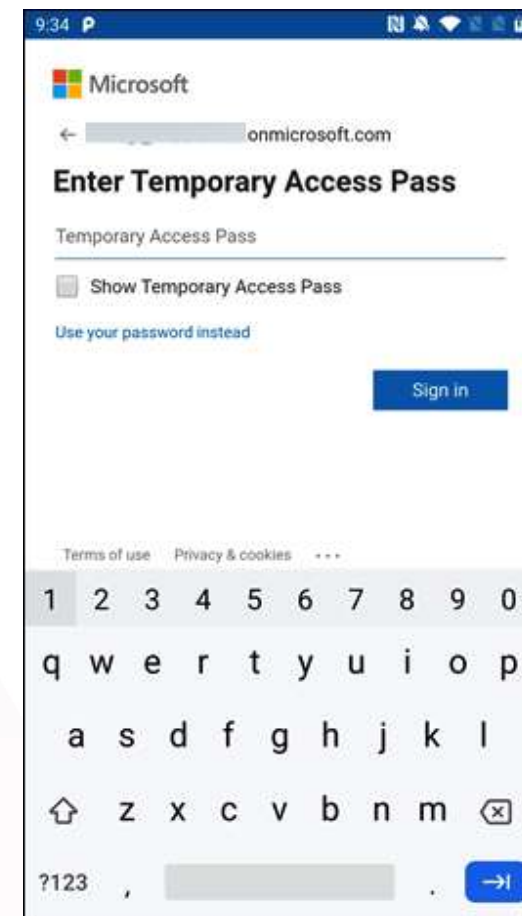
Back

Next



Passwordless phone sign-in

- Users can also use their Temporary Access Pass to register for Passwordless phone sign-in directly from the Authenticator app.



Guest access

- Guest users can sign-in to a resource tenant with a Temporary Access
- If MFA is required for the resource tenant, the guest user needs to perform MFA in order to gain access to the resource.

Replace a Temporary Access Pass

A user can only have **one** Temporary Access Pass.

- The passcode can be used during the **start and end time** of the Temporary Access Pass.

Replace a Temporary Access Pass (cont.)

User requires a new Temporary Access Pass:

- If the existing Temporary Access Pass is valid
 - the admin can create a new Temporary Access Pass to override the existing valid Temporary Access Pass
- If the existing Temporary Access Pass has expired
 - a new Temporary Access Pass will override the existing Temporary Access Pass

Limitations

- When using a one-time TAP to register a Passwordless method such as FIDO2 or Phone sign-in, 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.
- Users in scope for Self Service Password Reset (SSPR) registration policy or [Identity Protection Multi-factor authentication registration policy](#) are required to register authentication methods after they've signed in with a Temporary Access Pass using a browser.

Limitations (cont.)

- Users in scope for Self Service Password Reset (SSPR) registration policy or [Identity Protection Multi-factor authentication registration policy](#) are required to register authentication methods after they've signed in with a TAP using a browser.
- Users in scope for these policies are redirected to the [Interrupt mode of the combined registration](#). This experience doesn't currently support FIDO2 and Phone Sign-in registration.

Limitations (cont.)

- A Temporary Access Pass can't be used with the Network Policy Server (NPS) extension and Active Directory Federation Services (AD FS) adapter.
- It can take a few minutes for changes to replicate
 - Because of this, after a TAP is added to an account it can take a while for the prompt to appear. For the same reason, after a Temporary Access Pass expires, users may still see a prompt for TAP.

• Sad je stvarno kraj