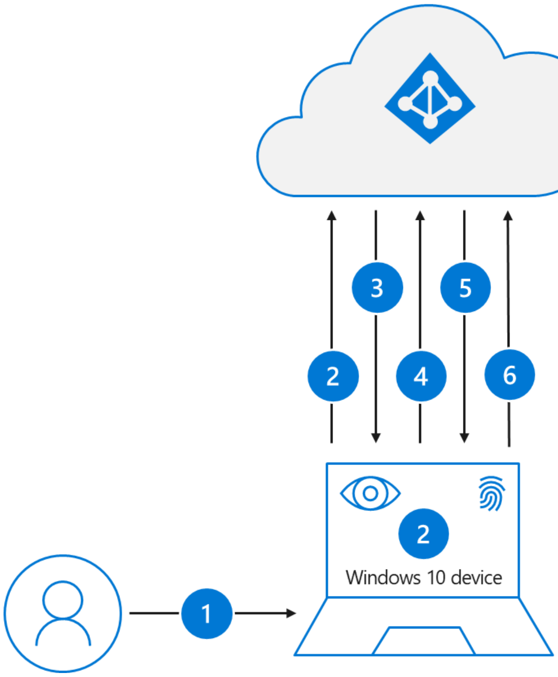
2- Authentication methods

- Windows Hello
- Authenticator App
- FIDO2 Security Keys

1. Single Sign-on
2. multi factor authentication
3. password less authentication
   password is removed and replaced with something you have, plus something you are, or something you know.
   1. windows Hello
   2. Microsoft authenticator app
   3. FIDO2 Security keys (Fast IDentity Online).

Windows Hello



1. **Unlock with Your Face or PIN:** You start by using your face or a PIN to unlock your device.
2. **Request for Special Code:** Your device asks a special service (Cloud AP provider) for a unique code (nonce) from Microsoft Entra ID.
3. **Receive the Code:** Microsoft Entra ID gives your device a special code that's valid for a short time.

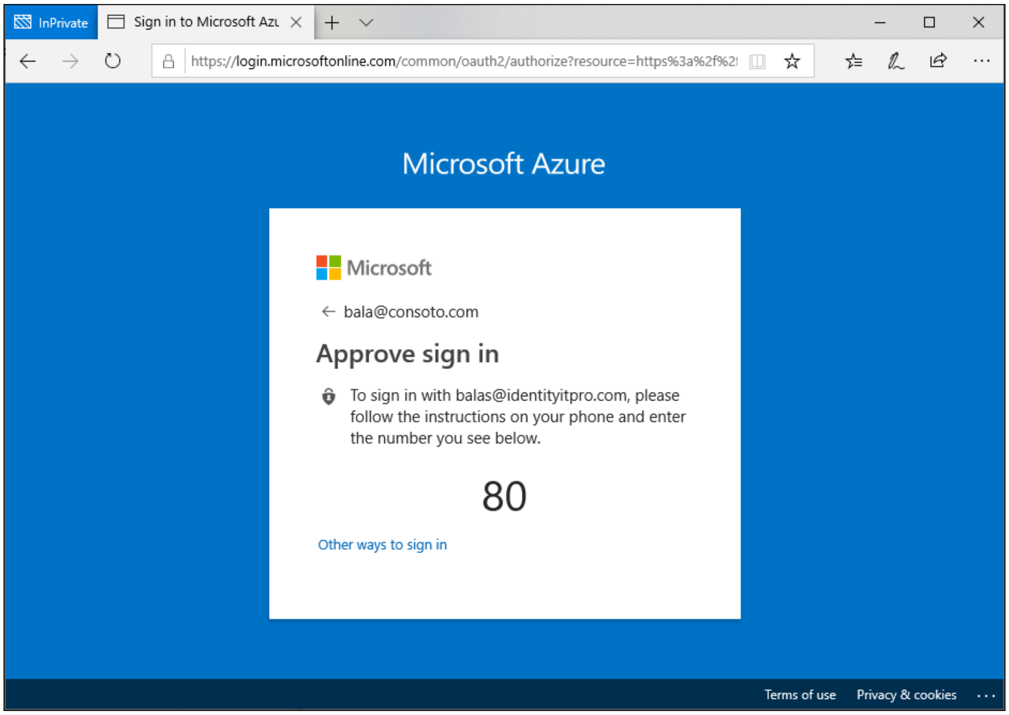
4. Prove Your Identity: The special service signs this code using your secret key to prove it's really you and sends it back to Microsoft Entra ID.

5. Check the Code: Microsoft Entra ID checks if the code is genuine by using your public key. If it's good, they create a *special key* and *token* (PRT) and send it back to the special service.

6. Protect the Key: The special service uses your device's private key to unlock this special key and keeps it safe in a special place called *Trusted Platform Module*(TPM).

7. Successful Login: The special service confirms that everything is okay, and you can now access your device and apps without having to log in again. It's like logging in just once for everything (Single Sign-On or SSO).

Authenticator App


InPrivate
Sign in to Microsoft Azu
https://login.microsoftonline.com/common/oauth2/authorize?resource=https%3a%2f%2f

Microsoft Azure

Microsoft

← bala@consoto.com

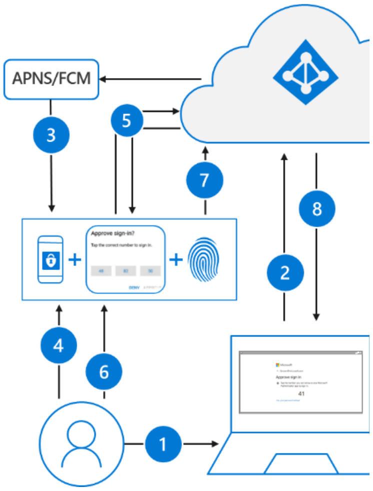
Approve sign in

To sign in with balas@identityitpro.com, please follow the instructions on your phone and enter the number you see below.

80

Other ways to sign in

Terms of use Privacy & cookies ...



1. The user enters their username.

2. Microsoft Entra ID detects that the user has a strong credential and starts the Strong Credential flow.

3. A notification is sent to the app via Apple Push Notification Service (APNS) on iOS devices, or via Firebase Cloud Messaging (FCM) on Android devices.

4. The user receives the push notification and opens the app.

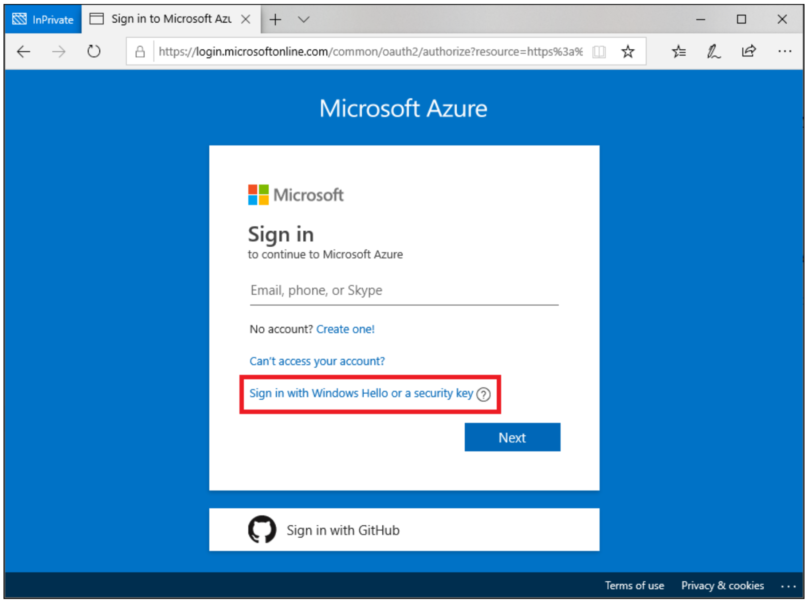
5. The app calls Microsoft Entra ID and receives a proof-of-presence challenge and nonce.

6. The user completes the challenge by entering their biometric or PIN to unlock private key.

7. The nonce is signed with the private key and sent back to Microsoft Entra ID.

8. Microsoft Entra ID performs public/private key validation and returns a token.

FIDO2 Security Keys


InPrivate
Sign in to Microsoft Azu
https://login.microsoftonline.com/common/oauth2/authorize?resource=https%3a%

Microsoft Azure

Microsoft

Sign in

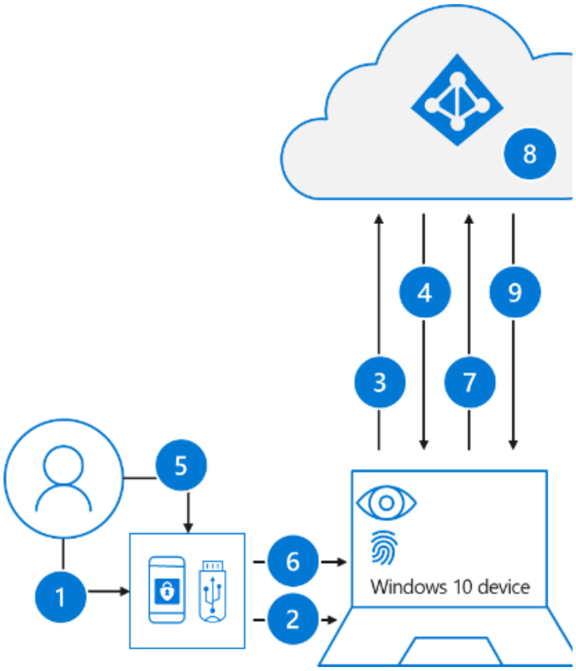
to continue to Microsoft Azure

Email, phone, or Skype

No account? Create one!

Can't access your account?

Sign in with Windows Hello or a security key



1. The user plugs the FIDO2 security key into their computer.
2. Windows detects the FIDO2 security key.
3. Windows sends an authentication request.
4. Microsoft Entra ID sends back a nonce.
5. The user completes their gesture to unlock the private key stored in the FIDO2 security key's secure enclave.
6. The FIDO2 security key signs the nonce with the private key.
7. The primary refresh token (PRT) token request with signed nonce is sent to Microsoft Entra ID.
8. Microsoft Entra ID verifies the signed nonce using the FIDO2 public key.
9. Microsoft Entra ID returns PRT to enable access to on-premises resources.