Microsoft Entra ID Authentication Capabilities

Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

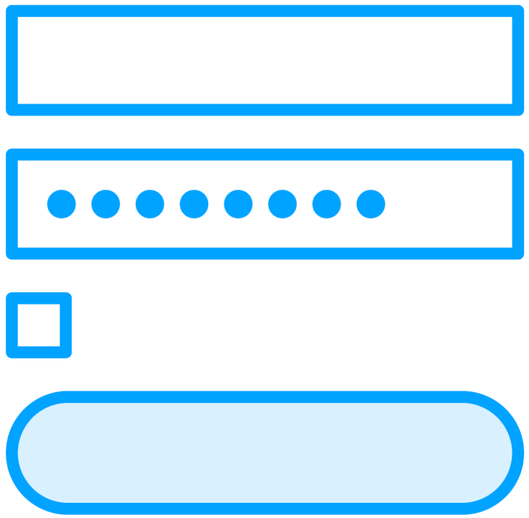
Overview

Entra ID authentication methods

Password protection and management in Entra ID

Entra ID Authentication Methods

Authentication



Authentication is the process of verifying an identity to be legitimate

Traditionally we have used passwords

- Passwords are not perfect
  - Users re-use passwords across services
  - Good passwords are difficult to remember
    - Decreasing productivity

Some Statistics Around Passwords

80%

Of hacking-related breaches involved the use of lost or stolen credentials
https://enterprise.verizon.com/resources/reports/dbir/

52%

Of people reuse the same password for multiple (but not all) accounts
https://services.google.com/fh/files/blogs/google_security_infographic.pdf

13%

Of people use the same password for *all* passworded accounts and devices
https://services.google.com/fh/files/blogs/google_security_infographic.pdf

Multi-factor Authentication (MFA)

MFA requires more than one form of verification

- Something you know (Ex: password)
- Something you have (phone, hardware key)
- Something you are (biometrics)

Microsoft studies show that enabling MFA can reduce the risk of identity compromise by as much as 99.9%

- https://bit.ly/MFA99Blog

This is always the first thing to enable in order to provide greater protection to user identities

Four supported methods of additional verification

- Microsoft authenticator app
- OATH hardware token
- SMS
- Voice call

Administrators can disable certain methods

SMS/voice call are considered the least secure MFA methods

- But still way better than no MFA

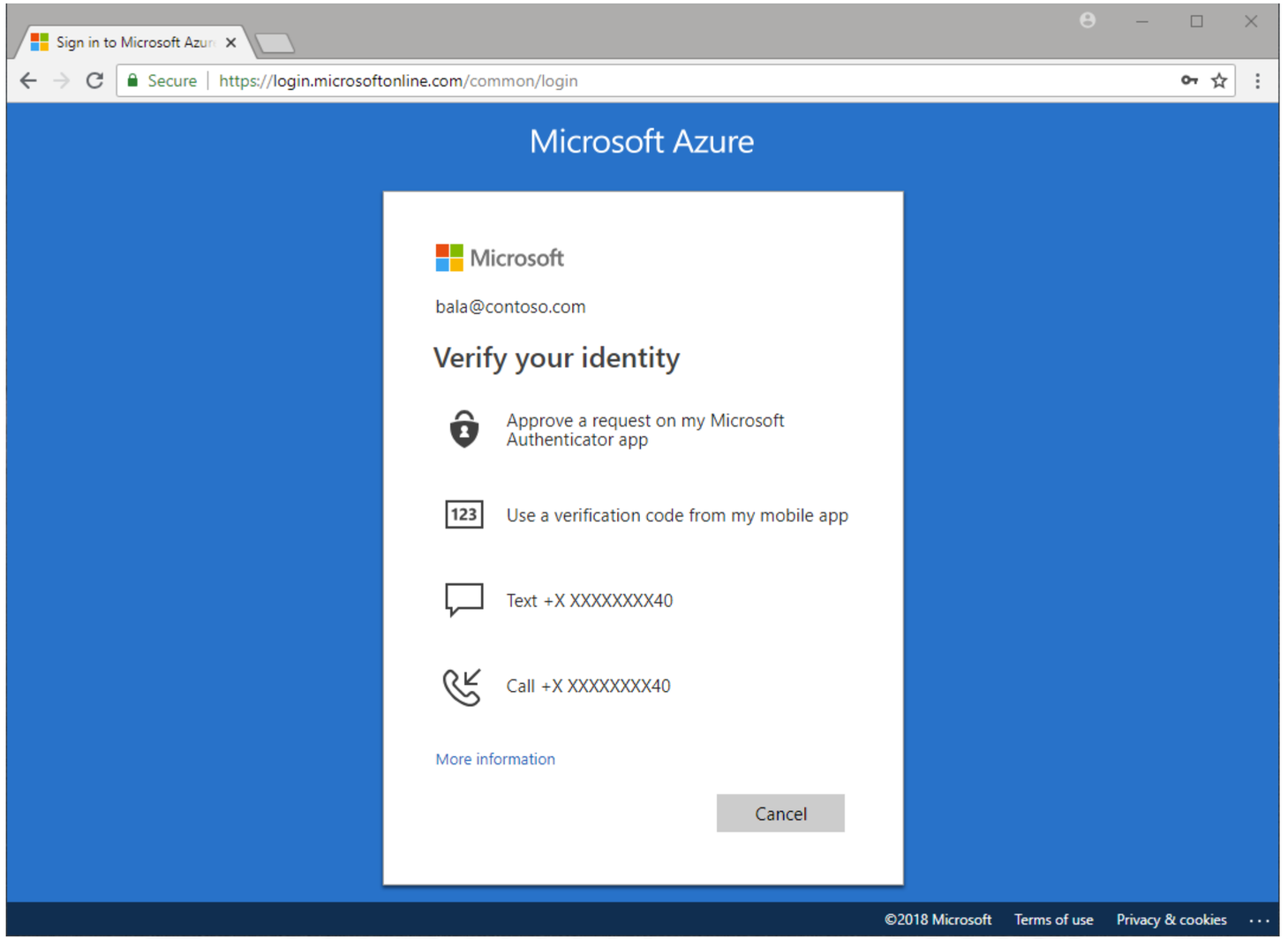


Image Source: https://learn.microsoft.com/en-us/training/modules/explore-authentication-capabilities/3-describe-multi-factor-authentication

Passwordless

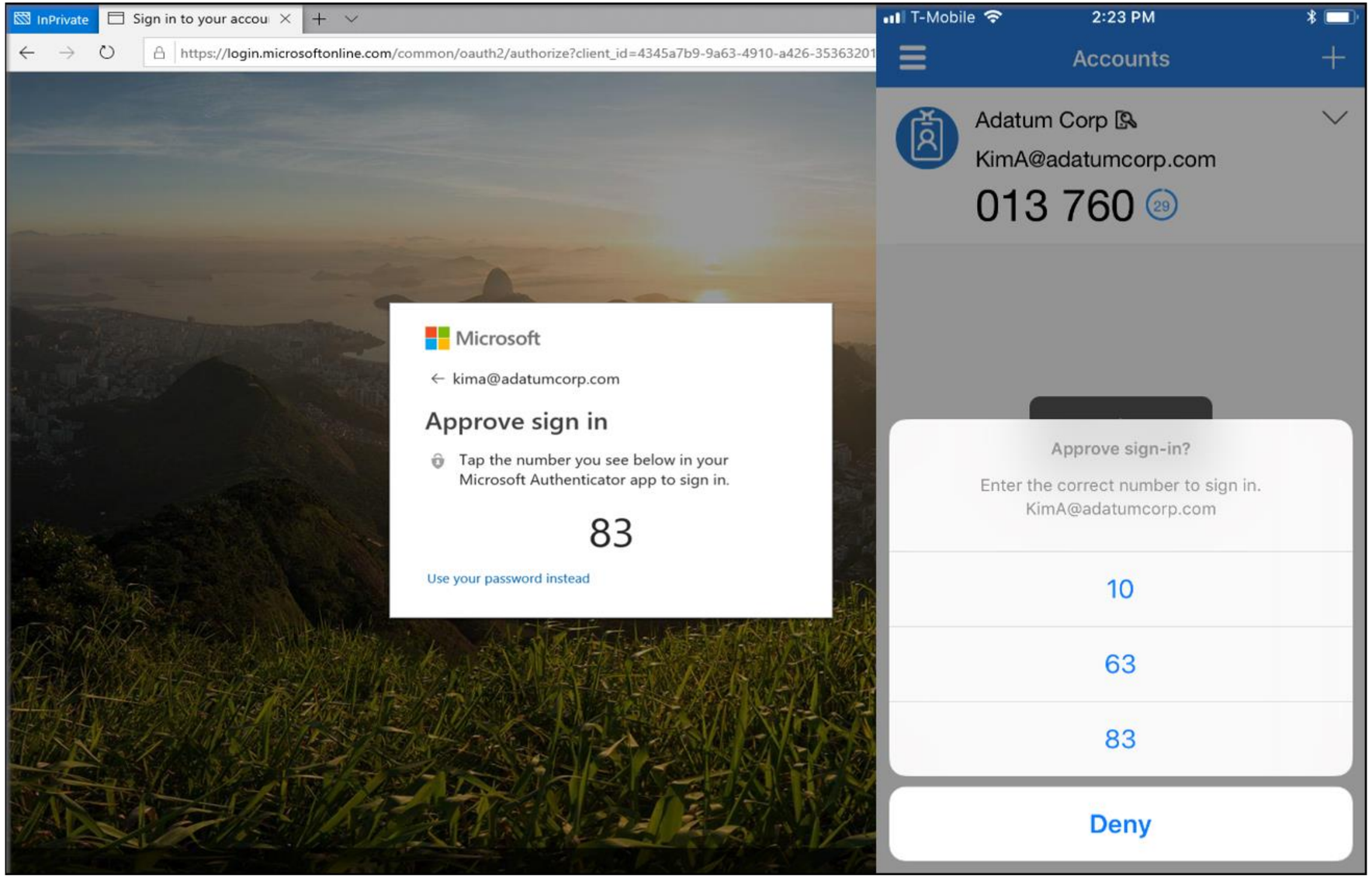
Based on something you are

- Rather than something you know

Passwordless options

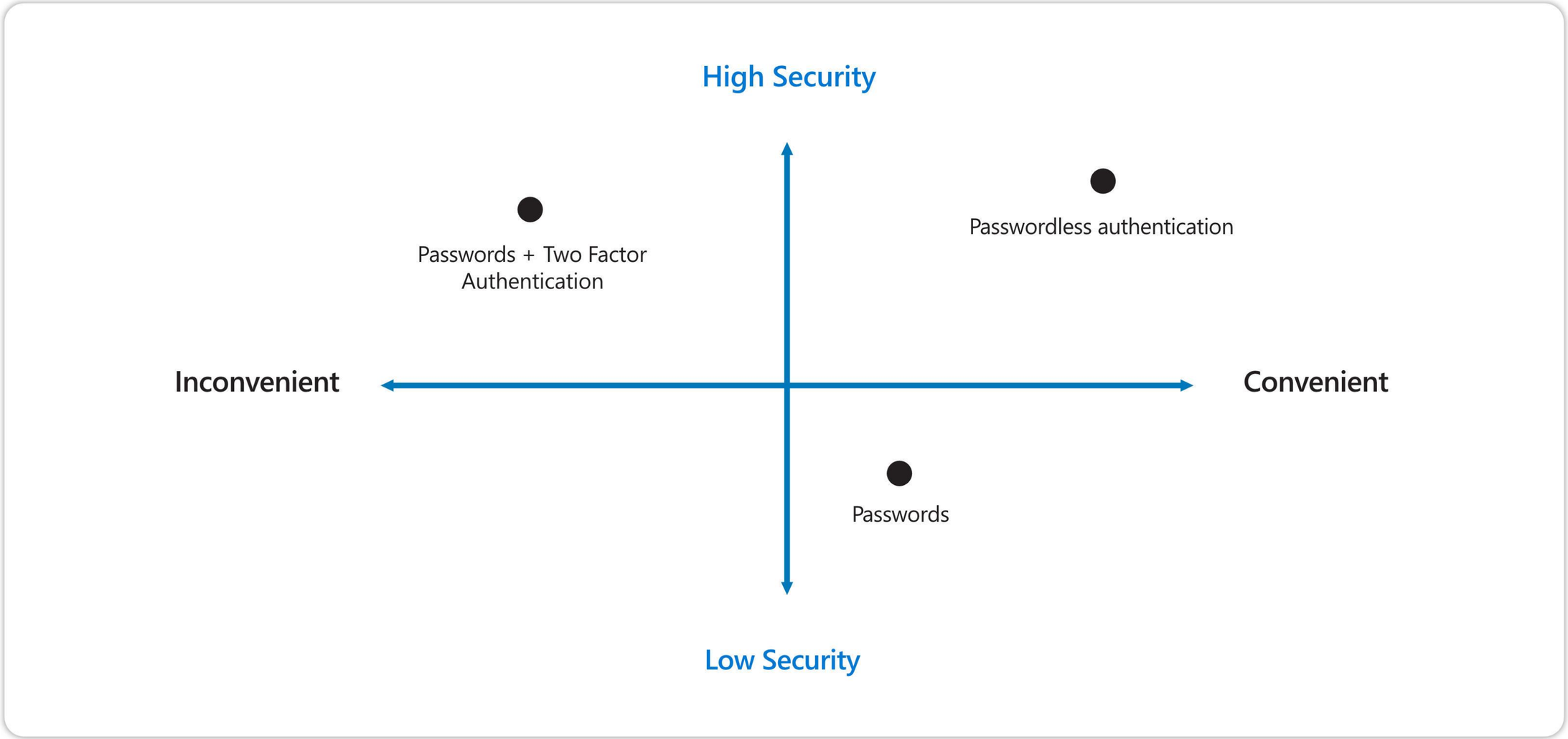
- Microsoft Authenticator Fingerprint Scan
- FIDO2 Security Key
- Windows Hello

Passwordless Prompt



https://learn.microsoft.com/en-us/training/modules/explore-authentication-capabilities/2-describe-authentication-methods

Passwordless as Positioned by Microsoft



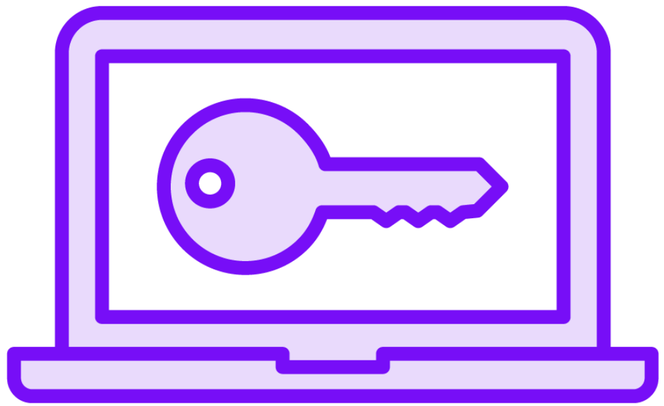
https://www.microsoft.com/en-us/security/business/identity-access-management/passwordless-authentication

Putting It All Together

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

https://www.microsoft.com/en-us/security/business/identity-access-management/passwordless-authentication

Windows Hello



Authentication feature built into Windows 10/11

- Positioned as more secure than MFA
- Uses a biometric verification (fingerprint, face) or Pin
- Tied to a device

Windows Hello can authenticate to

- Microsoft account (personal)
- Active Directory / Entra ID account
- Any Identity Provider that supports FIDO v2.0

How Is Windows Hello More Secure?

The biometric/pin is tied to the device

Hacker would need both hardware and pin/biometric proof to unlock

Biometric data/pin is stored on the local device

It doesn't need to travel over the network where a hacker could intercept it

Windows Hello pin is backed by a Trusted Platform Module (TPM) chip

Tamper resistant

Windows Hello Versions

Windows Hello

Configured by a user on their personal device

Uses a PIN or biometric gesture

PIN is not backed by key or certificate-based authentication

Windows Hello for Business

Configured by group policy or MDM

Always uses key-based or certificate-based authentication

By default, PIN is disabled

Demo

Multi-factor authentication

Passwordless authentication

Password Protection and Management in Entra ID

Microsoft Entra Self-service Password Reset (SSPR)

SSPR allows users to change/reset their password

- Without admin/help desk involvement

Main advantages

- Increases security
- Saves the organization money
- Increases user productivity

With SSPR users can

- Change their password
- Reset their password
- Unlock their account

How It Works

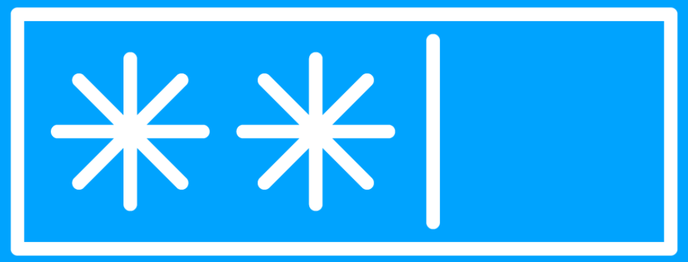
When enabled for SSPR – users must specify at least another authentication method

- Mobile app notification
- Mobile app code
- Email
- Mobile phone number
- Office phone
- Security question

Users need access to at least one of them to reset their password

Demo

Microsoft Entra self-service password reset



Microsoft Entra Password Protection

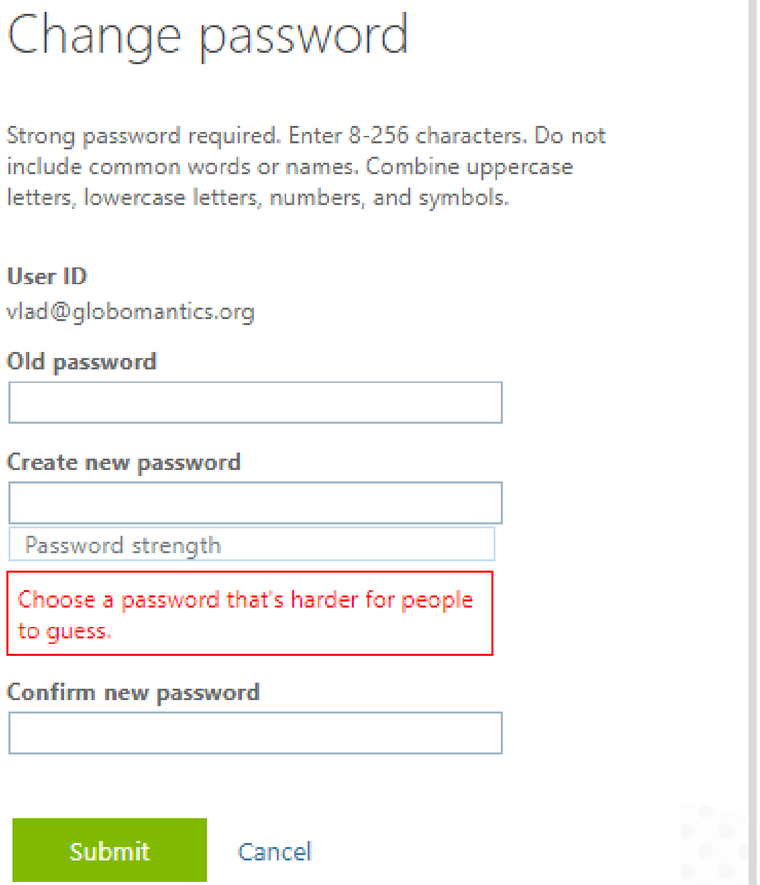
Microsoft Entra Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization.

Microsoft Entra Password Protection

Global Banned Password List

Custom Banned Password List

Global Banned Password List



List of weak or compromised passwords maintained by Microsoft

- Ex: the famous P@$$w0rd
  - Also checked for variations

Users not allowed to set their password to any of the passwords on the list

Custom Banned Password Lists

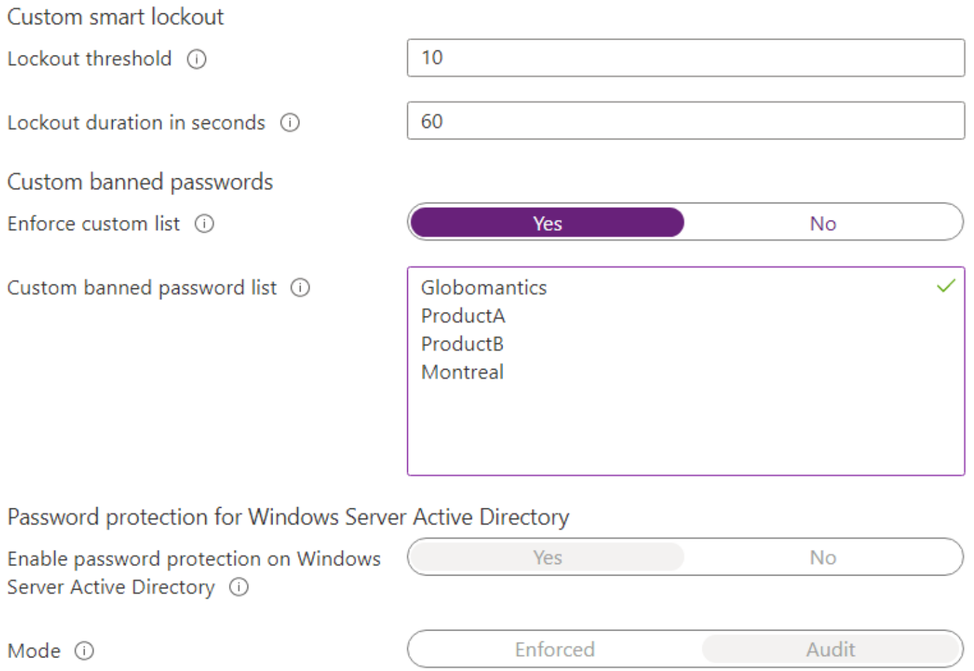
Create a custom banned password list

Create a list of

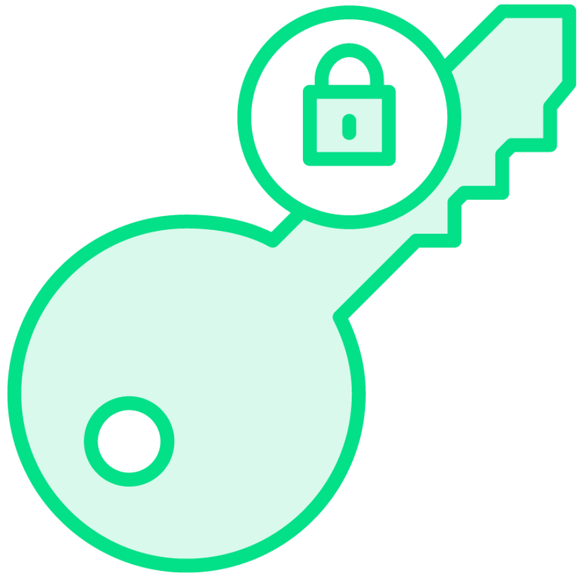
- Brand names
- Product names
- Locations
- Company acronyms

Microsoft algorithm automatically blocks weak variations and combinations

This is combined with Microsoft's global banned password list



Microsoft Entra Password Protection



Helps defend from password spray

Microsoft keeps the global list up to date

- Less work for your IT team

Can also integrate with your on-premises Active Directory environment

- Agent installed on-premises
- Same protection applied to on-premises / hybrid identities

Module Conclusion

Entra ID authentication methods

- Multi-factor authentication
- Passwordless
- Windows Hello and Windows Hello for Business

Password protection and management in Entra ID

- Self-service password reset (SSPR)
- Microsoft Entra Password Protection

Up Next:

Microsoft Entra ID Access Management Capabilities