Authentication Capabilities of Azure AD

Passwords

The most common form of authentication, but shoul always be mixed with some of the other methods below.

Phone

There are two optoins for phone-based authentication:

- SMS - a 6 digit code is texted to the users phone number which they must enter.

- Voice call - user must press #

These can be a secondary form of authentication when doing self-service password reset (SSPR) or Azure AD MFA.

OATH

Open Authentication (OATH) relates to time-based one-time password codes are used (TOTP).

- Software OATH tokens: Azure AD generates the seed/secret key and that gets input to the app and used to generate codes. Examples: Raivo OTP, Aegis, Tofu.

- OATH TOTP hardware tokens: small devices that display a code that refreshes every 30-60 seconds

Can only be used as a secondary authentication form

Passwordless authentication

The aim of removing passwords as part of sign-in. Azure AD provides ways to natively authenticate using passwordless methods.

Windows Hello for Business

Replaces passwords with strong two-factor authentication on devices - a combination of key or certificate tied to the device itself, and something the user knows/has (a PIN. or biometrics)

FIDO2

Typically USB or oher hardware devices (e.g. a phone with NFC). There is no password to be guessed, making them more secure. As a passwordless authentication method, it serves as the primary form, but it can also be used as a secondary form during MFA.

Microsoft Authenticator App

As a passwordless authentication method, it can be used as the primary form, or the secondary when doing SSPR

MFA in Azure AD

MFA requires more than one form of verification - a trusted device, a fingerprint etc so that even if the password is compromised, the account is not.

Azure AD MFA works by requiring:

- something you know: (a password or PIN)
- something you have: (trusted device e.g. phone or hardware key) or
- something you are: biometrics like a fingerprint or face scan

The following additoinal forms can be used with it:

- ms authenticator app
- Windows Hello for business
- FIDO2 security key
- OATH hardware token
- OATH software token
- SMS
- Voice call

Security defaults and multi-factor authentication

A set of basic identity security measures recommended by MS. When enabled, they will be automatically enforced in your organisation. The goal is to ensure that all orgs have a basic level of security at no extra cost. Some of these defaults include:

- Enforcing Azure AD MFA for all users

- Forcing admins to use MFA
- Requiring all users to complete MFA when needed.

Self Service Password Reset (SSPR) in Azure AD

Allows a user to change or reset their password without involvement from an admin. It works in the following scenarios:

- Password change: the user knows their password, but wants to change it to something new
- Password reset: the user does not know their password and needs to rest it
- Account unlock: user can't sign in because the account is locked

To be able to use the SSPR, users must be:

- Assigned an Azure AD license
- SSPR must be enabled by an Admin
- Registered authentication methods (two or more) must have been previously set

Password protection and management capabilities of Azure AD

Global banned password list

A list of known weak passwords is constantly updated by MS. These cannot be set by the user and they will get a prompt asking them to choose something else.

Custom banned password list

Admins can create a custom list if they so wish (e.g. brand names, product names, locations, company specific terms).

Protection against password spray

Password spraying is trying a few weak passwords across multiple accounts hoping to gain access. Azure AD Password Protection puts a stop to this.

Hybrid security

It is possible to intergrate Azure AD Password protection with on-prem AD. The on-prem environment then gets a copy of the global banned password and custom password protection policies from Azure AD.