PASSWORDS AND SIGN-IN METHODS

Contoso Legal LLP

Harbour IT

PREPARED BY	DATE	DATA COLLECTED	MICROSOFT 365 TENANT
Harbour IT	29 Nov 2026	29 Nov 2026, 18:57 UTC	contoso.onmicrosoft.com

How people sign in and how strong that is: methods by strength, admins without phishing-resistant MFA, the methods policy, and password age and expiry.

Filtered view. Sign-in methods by person: 1 of 20 rows, Methods is Security key or passkey (FIDO2). Password age: 20 of 20 rows, 1 column hidden. The headline figures cover every row.

Phishing-resistant
5 of 20
Passkey, security key, Windows Hello or certificate

Admins without phishing-resistant
1
Admin roles should need a passkey or security key

Phone is the only second factor
3
Text message or voice call

Passwordless ready
1 of 20
Can sign in without a password

No self-service reset
0
Can't reset a forgotten password themselves

Password never expires
20
Fine with MFA: expiry is no longer advised

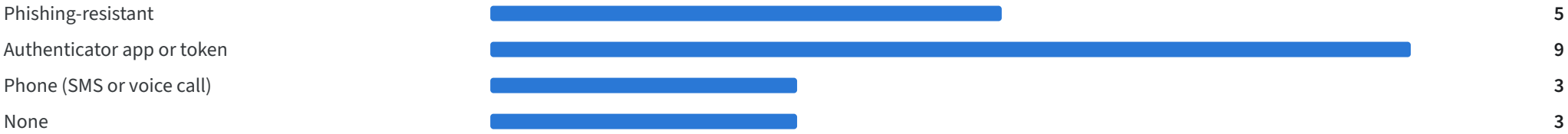
Password over a year old
4
Matters most without MFA

Never signed in, old password
1
Probably still the first password

Strongest method 4 2 to review

Each enabled member counted once, by the strongest method they have.

By strength

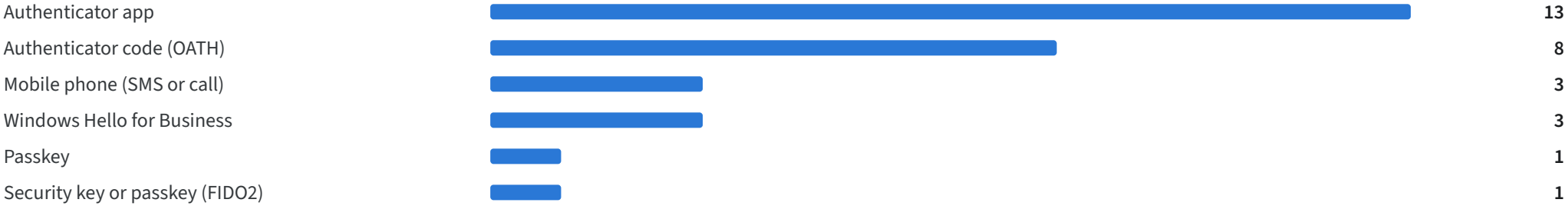


Flag	Strength	People	Admins	Share of members	What it means
	Phishing-resistant	5	1	25%	Bound to the real Microsoft sign-in page, so a fake page can't relay it.
	Authenticator app or token	9	1	45%	Strong, but a convincing fake sign-in page can relay a code or push approval.
Medium	Phone (SMS or voice call)	3	0	15%	Weakest second factor: texts and calls can be intercepted or moved to another SIM.
Medium	None	3	0	15%	No second factor: the password alone gets in.

Methods registered 6

How many enabled members have each method. People usually have more than one.

By method



Flag	Method	Strength	People	Admins
	Windows Hello for Business	Phishing-resistant	3	0
	Passkey	Phishing-resistant	1	0
	Security key or passkey (FIDO2)	Phishing-resistant	1	1
	Authenticator app	Authenticator app or token	13	1
	Authenticator code (OATH)	Authenticator app or token	8	0
● Low	Mobile phone (SMS or call)	Phone (SMS or voice call)	3	0

Sign-in methods by person 1

Enabled members and what they can sign in with, weakest first and admins at the top. Who hasn't set up MFA at all, and whether it's required, is in MFA coverage.

Account	Admin	Admin roles	Strongest method	Methods	Asked for first	Passwordless	Self-service reset	What to do
breakglass@contoso.example	Yes	Global Administrator	Phishing-resistant	Security key or passkey (FIDO2)	–	Yes	Yes	Nothing

Sign-in methods policy 12

Which methods people may register and use, from the tenant's authentication methods policy, against what's recommended for a small business.

Flag	Setting	Current	Recommended	Why
	Passkeys and security keys (FIDO2)	On for Break glass	On	Needed for phishing-resistant sign-in, which admins should use.
	Microsoft Authenticator	On for All users	On	The second factor most people should use.
	Authenticator shows which app is signing in	Microsoft managed	On (Microsoft managed turns it on)	Helps people spot a sign-in that isn't theirs.
● Low	Authenticator shows where the sign-in is from	Off	On (Microsoft managed turns it on)	Helps people spot a sign-in that isn't theirs.
● Low	Text message (SMS)	On for All users except Break glass	Off, once people use Authenticator	Texts can be intercepted or moved to another SIM.
	Voice call	Off	Off	Calls can be redirected, and are easy to approve by mistake.

Flag	Setting	Current	Recommended	Why
	Email one-time passcode	On for All users	Off, unless guests or password reset need it	Not a second factor for members; only for password reset and guests.
	Temporary Access Pass	Off	On, for setting up passkeys	A time-limited pass for setting up a new phone or passkey.
	Registration campaign (asks people to set up Authenticator at sign-in)	Microsoft managed, for All users, can be skipped for 1 day	On, or Microsoft managed	Moves people off text messages and calls.
Low	System-preferred MFA (asks for the strongest method a person has)	Off	On, or Microsoft managed	Otherwise people are asked for their own default, often a text message.
	People can report an MFA prompt they didn't expect	Microsoft managed	On	A reported prompt blocks the account's risky sign-ins and alerts admins.
	Methods managed in this policy (not the old MFA and SSPR settings)	Yes	Yes	Microsoft has retired the old per-user MFA and SSPR method settings.

Authentication strengths in Conditional Access 0

Conditional Access policies that require a particular strength of MFA rather than any MFA. Requiring Phishing-resistant MFA for admin roles is the usual first step.

No Conditional Access policy requires an authentication strength. Start with one requiring Phishing-resistant MFA for admin roles, once admins have a passkey.

Password age 20 1 to review

When each enabled member's password was last set. An old password matters most without MFA; an account that has never signed in may still have the password it was created with. Problems first, then oldest first.

Flag	Password last changed	Never expires	Synced from on-premises	Last sign-in	MFA set up	What it means
Medium	3 Apr 2024	Yes	No	Never	No	Never signed in, and the password was set over a month ago: it's probably still the one the account was created with. Block sign-in if it isn't needed, or reset the password.
	26 Sep 2025	Yes	No	29 Nov 2026	Yes	Unchanged for over a year; MFA protects it.
	25 Oct 2025	Yes	No	29 Nov 2026	Yes	Unchanged for over a year; MFA protects it.

Flag	Password last changed	Never expires	Synced from on-premises	Last sign-in	MFA set up	What it means
	23 Nov 2025	Yes	No	28 Nov 2026	Yes	Unchanged for over a year; MFA protects it.
	22 Dec 2025	Yes	No	28 Nov 2026	Yes	–
	20 Jan 2026	Yes	No	28 Nov 2026	Yes	–
	18 Feb 2026	Yes	No	27 Nov 2026	Yes	–
	19 Mar 2026	Yes	No	29 Nov 2026	Yes	–
	17 Apr 2026	Yes	No	28 Nov 2026	Yes	–
	16 May 2026	Yes	No	27 Nov 2026	No	–
	14 Jun 2026	Yes	No	28 Nov 2026	Yes	–
	10 Jul 2026	Yes	No	30 Jul 2026	No	–
	13 Jul 2026	Yes	No	23 Nov 2026	Yes	–
	22 Jul 2026	Yes	No	17 Nov 2026	Yes	–
	11 Aug 2026	Yes	No	28 Nov 2026	Yes	–
	31 Aug 2026	Yes	No	30 Sep 2026	Yes	–
	9 Sep 2026	Yes	No	23 Nov 2026	Yes	–
	8 Oct 2026	Yes	No	29 Nov 2026	Yes	–
	15 Nov 2026	Yes	No	29 Nov 2026	Yes	–
	24 Nov 2026	Yes	No	29 Nov 2026	Yes	–

Password expiry policy 3

How often cloud-only accounts on each domain must change their password. Microsoft and the NCSC now advise against regular expiry when everyone has MFA: forced changes lead to weaker, predictable passwords. Accounts synced from on-premises AD follow AD's policy instead.

Flag	Domain	Signs in with	Passwords expire after	Reminder before expiry	Recommended
	contoso.example	Microsoft Entra ID	Never	–	Never, with MFA required for everyone
	contoso.onmicrosoft.com	Microsoft Entra ID	Never	–	Never, with MFA required for everyone
Low	parked.example	Microsoft Entra ID	90 days	14 days	Never, with MFA required for everyone

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Read from Microsoft 365 with read-only access; nothing was changed. Data collected 29 Nov 2026, 18:57 UTC.