

PREPARED BY
Harbour IT

DATE
14 Oct 2026

DATA COLLECTED
14 Oct 2026, 04:00 UTC

MICROSOFT 365 TENANT
northwindtraders.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. Strongest method: 2 of 4 rows, Admins is 1. Sign-in methods by person: 36 of 36 rows, 1 column hidden. The headline figures cover every row.

Phishing-resistant

6 of 36

Passkey, security key, Windows Hello or certificate

Admins without phishing-resistant

2

Admin roles should need a passkey or security key

Phone is the only second factor

3

Text message or voice call

Passwordless ready

0 of 36

Can sign in without a password

No self-service reset

1

Can't reset a forgotten password themselves

Password never expires

0

Fine with MFA: expiry is no longer advised

Password over a year old

0

Matters most without MFA

Never signed in, old password

0

Probably still the first password

Strongest method 2 1 to review

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

By strength

Authenticator app or token



14

None



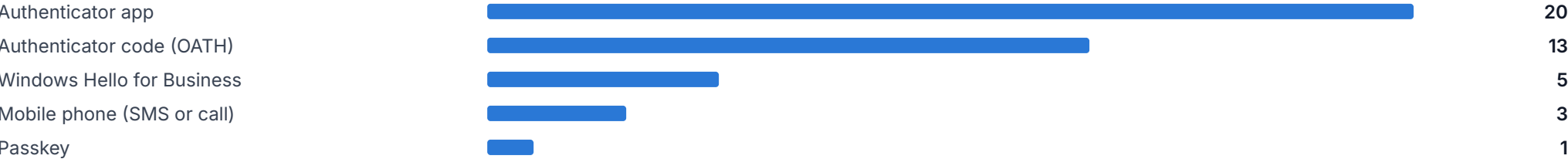
13

Flag	Strength	People	Admins	Share of members	What it means
	Authenticator app or token	14	1	39%	Strong, but a convincing fake sign-in page can relay a code or push approval.
● Medium	None	13	1	36%	No second factor: the password alone gets in.

Methods registered 5

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	5	0
	Passkey	Phishing-resistant	1	0
	Authenticator app	Authenticator app or token	20	1
	Authenticator code (OATH)	Authenticator app or token	13	0
● Low	Mobile phone (SMS or call)	Phone (SMS or voice call)	3	0

Sign-in methods by person 36 17 to review

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.

Flag	Account	Admin roles	Strongest method	Methods	Asked for first	Passwordless	Self-service reset	What to do
● High	breakglass@northwindtraders.example	Global Administrator	None	–	–	No	No	No second factor. Set up MFA first (see MFA coverage).
● Medium	ann.patel@northwindtraders.example	Global Administrator, Groups Administrator (limited scope)	Authenticator app or token	Authenticator app	Authenticator app	No	Yes	Admin without a phishing-resistant method: register a passkey or security key.
● Medium	alfie.roberts@northwindtraders.example	–	None	–	–	No	Unknown	No second factor. Set up MFA first (see MFA coverage).
● Medium	alfie.scott@northwindtraders.example	–	None	–	–	No	Unknown	No second factor. Set up MFA first (see MFA coverage).
● Medium	grace.wilson@northwindtraders.example	–	None	–	–	No	Unknown	No second factor. Set up MFA first (see MFA coverage).
● Medium	hannah.robinson@northwindtraders.example	–	None	–	–	No	Unknown	No second factor. Set up MFA first (see MFA coverage).
● Medium	leo.morris@northwindtraders.example	–	None	–	–	No	Unknown	No second factor. Set up MFA first (see MFA coverage).
● Medium	leo.wright@northwindtraders.example	–	None	–	–	No	Unknown	No second factor. Set up MFA first (see MFA coverage).

Flag	Account	Admin roles	Strongest method	Methods	Asked for first	Passwordless	Self-service reset	What to do
● Medium	maya.martin@northwindtraders.example	–	None	–	–	No	Unknown	No second factor. Set up MFA first (see MFA coverage).
● Medium	olivia.scott@northwindtraders.example	–	None	–	–	No	Unknown	No second factor. Set up MFA first (see MFA coverage).
● Medium	owen.taylor@northwindtraders.example	–	None	–	–	No	Unknown	No second factor. Set up MFA first (see MFA coverage).
● Medium	rhys.clark@northwindtraders.example	–	None	–	–	No	Unknown	No second factor. Set up MFA first (see MFA coverage).
● Medium	sophie.smith@northwindtraders.example	–	None	–	–	No	Unknown	No second factor. Set up MFA first (see MFA coverage).
● Medium	thomas.clarke@northwindtraders.example	–	None	–	–	No	Unknown	No second factor. Set up MFA first (see MFA coverage).
● Medium	arthur.evans@northwindtraders.example	–	Phone (SMS or voice call)	Mobile phone (SMS or call)	–	No	Unknown	Only a phone: set up the Authenticator app (or a passkey), then keep the phone as a backup at most.
● Medium	mia.hughes@northwindtraders.example	–	Phone (SMS or voice call)	Mobile phone (SMS or call)	–	No	Unknown	Only a phone: set up the Authenticator app (or a passkey), then keep the phone as a backup at most.
● Medium	zara.jackson@northwindtraders.example	–	Phone (SMS or voice call)	Mobile phone (SMS or call)	–	No	Unknown	Only a phone: set up the Authenticator app (or a passkey), then keep the phone as a backup at most.

Flag	Account	Admin roles	Strongest method	Methods	Asked for first	Passwordless	Self-service reset	What to do
	aaron.watson@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing
	amelia.watson@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing
	ella.baker@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing
	ethan.green@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing
	george.roberts@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing
	george.robinson@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing
	hannah.patel@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing
	harry.lee@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing
	imogen.edwards@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing
	megan.lee@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing

Flag	Account	Admin roles	Strongest method	Methods	Asked for first	Passwordless	Self-service reset	What to do
	olivia.smith@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing
	rhys.moore@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing
	ruby.taylor@northwindtraders.example	–	Authenticator app or token	Authenticator app, Authenticator code (OATH)	–	No	Unknown	Nothing
	grace.taylor@northwindtraders.example	–	Phishing-resistant	Passkey, Authenticator app	–	No	Unknown	Nothing
	isla.evans@northwindtraders.example	–	Phishing-resistant	Windows Hello for Business, Authenticator app	–	No	Unknown	Nothing
	jacob.hughes@northwindtraders.example	–	Phishing-resistant	Windows Hello for Business, Authenticator app	–	No	Unknown	Nothing
	leo.evans@northwindtraders.example	–	Phishing-resistant	Windows Hello for Business, Authenticator app	–	No	Unknown	Nothing
	owen.white@northwindtraders.example	–	Phishing-resistant	Windows Hello for Business, Authenticator app	–	No	Unknown	Nothing
	ruby.hill@northwindtraders.example	–	Phishing-resistant	Windows Hello for Business, Authenticator app	–	No	Unknown	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.
	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 36

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.

Account	Password last changed	Never expires	Synced from on-premises	Last sign-in	MFA set up	What it means
thomas.clarke@northwindtraders.example	Unknown	No	No	4 Jun 2026	No	–
hannah.robinson@northwindtraders.example	Unknown	No	No	9 Apr 2026	No	–
sophie.smith@northwindtraders.example	Unknown	No	No	24 Jan 2026	No	–
megan.lee@northwindtraders.example	Unknown	No	No	12 Oct 2026	Yes	–
grace.taylor@northwindtraders.example	Unknown	No	No	14 Oct 2026	Yes	–
owen.white@northwindtraders.example	Unknown	No	No	12 Oct 2026	Yes	–
ruby.taylor@northwindtraders.example	Unknown	No	No	1 Oct 2026	Yes	–
olivia.smith@northwindtraders.example	Unknown	No	No	10 Oct 2026	Yes	–
grace.wilson@northwindtraders.example	Unknown	No	No	13 Oct 2026	No	–
zara.jackson@northwindtraders.example	Unknown	No	No	12 Oct 2026	Yes	–
leo.evans@northwindtraders.example	Unknown	No	No	14 Oct 2026	Yes	–
amelia.watson@northwindtraders.example	Unknown	No	No	13 Oct 2026	Yes	–
george.robinson@northwindtraders.example	Unknown	No	No	13 Oct 2026	Yes	–
hannah.patel@northwindtraders.example	Unknown	No	No	7 Oct 2026	Yes	–

Account	Password last changed	Never expires	Synced from on-premises	Last sign-in	MFA set up	What it means
ethan.green@northwindtraders.example	Unknown	No	No	13 Oct 2026	Yes	–
ruby.hill@northwindtraders.example	Unknown	No	No	8 Oct 2026	Yes	–
mia.hughes@northwindtraders.example	Unknown	No	No	13 Oct 2026	Yes	–
rhys.moore@northwindtraders.example	Unknown	No	No	12 Oct 2026	Yes	–
leo.wright@northwindtraders.example	Unknown	No	No	1 Oct 2026	No	–
leo.morris@northwindtraders.example	Unknown	No	No	13 Oct 2026	No	–
isla.evans@northwindtraders.example	Unknown	No	No	7 Oct 2026	Yes	–
owen.taylor@northwindtraders.example	Unknown	No	No	13 Oct 2026	No	–
maya.martin@northwindtraders.example	Unknown	No	No	14 Oct 2026	No	–
arthur.evans@northwindtraders.example	Unknown	No	No	8 Oct 2026	Yes	–
harry.lee@northwindtraders.example	Unknown	No	No	13 Oct 2026	Yes	–
alfie.scott@northwindtraders.example	Unknown	No	No	7 Oct 2026	No	–
rhys.clark@northwindtraders.example	Unknown	No	No	13 Oct 2026	No	–
ella.baker@northwindtraders.example	Unknown	No	No	14 Oct 2026	Yes	–
alfie.roberts@northwindtraders.example	Unknown	No	No	2 Oct 2026	No	–
olivia.scott@northwindtraders.example	Unknown	No	No	11 Oct 2026	No	–
jacob.hughes@northwindtraders.example	Unknown	No	No	13 Oct 2026	Yes	–
george.roberts@northwindtraders.example	Unknown	No	No	1 Oct 2026	Yes	–
aaron.watson@northwindtraders.example	Unknown	No	No	12 Oct 2026	Yes	–
imogen.edwards@northwindtraders.example	Unknown	No	No	11 Oct 2026	Yes	–
ann.patel@northwindtraders.example	Unknown	No	No	30 Sep 2026	Yes	–
breakglass@northwindtraders.example	Unknown	No	No	2 Oct 2026	No	–

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
	northwindtraders.example	Microsoft Entra ID	Never	–	Never, with MFA required for everyone
	northwindtraders.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 14 Oct 2026, 04:00 UTC.