

# All clients

PREPARED BY

Harbour IT

DATE

14 Oct 2026

DATA COLLECTED

 14 Oct 2026, 04:00  
UTC

MICROSOFT 365 TENANT

3 clients

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 policy: 36 of 36 rows, 1 column hidden. The headline figures cover every row.

## Sign-in methods policy 36

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.                            |
|       |                                                                        |                                                            |                                              |                                                                      |

| Flag  | Setting                                                                | Current                                                    | Recommended                                  | Why                                                                      |
|-------|------------------------------------------------------------------------|------------------------------------------------------------|----------------------------------------------|--------------------------------------------------------------------------|
| ● 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.     |
|       | 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.     |

| 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.     |

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.