Microsoft 365 readiness check

Example Dental Group (sample)

As of November 2, 2026 · Prepared by Your company name

28 **Significant work needed**

Score out of 100

7 HIGH 3 MEDIUM 2 LOW

Microsoft deadlines

Date	What changes	Findings affected
Nov 7, 2026 (5 days)	Self-service password reset accepts only registered methods (profile phone numbers and emails stop working; rollout to mid-November)	**1**
Dec 31, 2026 (59 days)	SMTP AUTH with basic authentication turned off by default (final removal date to be announced, second half of 2027)	**2**
Feb 1, 2027 (91 days)	SMS and voice call MFA methods retired for users (no opt-out)	**2**
Apr 1, 2027 (150 days)	Exchange Web Services (EWS) permanently disabled in Exchange Online	**1**
Apr 7, 2027 (156 days)	Entra Connect Sync must be version 2.6.84.0 or later with application-based authentication, or directory sync stops	**1**
Jul 1, 2027 (241 days)	SMS and voice MFA retired for Global Administrators and external users	none

Identity

HIGH **Devices or apps still sign in with older mail protocols** Deadline Dec 31, 2026

Why it matters

These sign-ins (SMTP, IMAP, POP, ActiveSync and similar) are typically scanners, copiers, line-of-business apps or old phones. Several are being switched off, starting with SMTP AUTH basic authentication at the end of December 2026.

What to do For each line, find the device or app and move it to modern authentication (OAuth), Microsoft's High Volume Email or SMTP relay with a connector, or a supported mail client.

Evidence

- scanner@dental.example.com via Authenticated SMTP - 412 successful, last 2026-10-31
- billing@dental.example.com via Authenticated SMTP (Practice management system) - 96 successful, last 2026-11-01
- mchen@dental.example.com via IMAP4 - 38 successful, last 2026-10-30

▶ How to fix it (about 30-90 minutes per device or app)

HIGH **Users whose only MFA method is a text message or phone call** Deadline Feb 1, 2027

Why it matters Microsoft retires SMS and voice MFA on February 1, 2027 (July 1, 2027 for Global Administrators). With no other method registered, these people will be unable to complete sign-in.

What to do Have each person register the Microsoft Authenticator app or a passkey now (aka.ms/mysecurityinfo), then remove the phone method. A Temporary Access Pass helps anyone without a smartphone.

Evidence

- kdominguez@dental.example.com (Global Administrator)
- rsantos@dental.example.com
- jwhite@dental.example.com
- lnguyen@dental.example.com
- bharris@dental.example.com
- gflores@dental.example.com

▶ How to fix it (about 10 minutes per user, or one 20-minute group session)

HIGH **Entra Connect Sync still uses the old sign-in method; sync stops April 7, 2027** Deadline Apr 7, 2027

Why it matters Microsoft retires the old sync account sign-in on April 7, 2027. Servers that haven't moved to version 2.6.84.0 or later with application-based authentication stop syncing: new starters, leavers and password changes on-site no longer reach Microsoft 365.

What to do Upgrade each sync server to the latest Entra Connect Sync (download from the Entra admin center), then run the wizard and choose "Configure application-based authentication to Microsoft Entra ID".

Evidence
- DC01 - signs in with the old sync account Sync_DC01_4f2a9c81b7e0@exampledental.onmicrosoft.com

▶ How to fix it (about 45-90 minutes per sync server; plan a maintenance window)

HIGH **Admin accounts with no MFA method registered**

Why it matters: An admin role with only a password is the fastest way to lose the whole tenant. Emergency ("break glass") accounts are often left like this by accident.

What to do: Register a phishing-resistant method (a FIDO2 security key or passkey) on every admin account today; for emergency accounts store the key in a safe.

Evidence
- breakglass@dental.example.com

▶ How to fix it (about 15 minutes per account)

MEDIUM **Users who can't reset their own password after the November 7 change** Deadline Nov 7, 2026

Why it matters: From November 7, 2026, self-service password reset only accepts methods a person registered themselves. Phone numbers and email addresses typed into their user profile no longer count, so these people get stuck at the reset screen and call the helpdesk.

What to do: Turn on "Require users to register when signing in" for password reset and have each person register Microsoft Authenticator or a phone number at aka.ms/mysecurityinfo.

Evidence
- kdominguez@dental.example.com (admin)
- rsantos@dental.example.com
- jwhite@dental.example.com
- lnguyen@dental.example.com
- bharris@dental.example.com
- gflores@dental.example.com

▶ How to fix it (about 5 minutes per user, or one 15-minute group session)

MEDIUM **Licensed users with no MFA method registered**

Why it matters: No MFA method is registered yet. Security defaults or Conditional Access will force registration at the next sign-in, but until then the account is

password-only, and an attacker who has the password can register their own method.

What to do Get each user registered with Microsoft Authenticator or a passkey this week. For accounts that aren't people (shared mailboxes, scanners), block sign-in instead.

Evidence

- cmorales@dental.example.com
- hlopez@dental.example.com
- scanner@dental.example.com
- oldlab@dental.example.com

▶ How to fix it (about 5-10 minutes per user)

LOW **Users who still have a phone method as a backup** Deadline Feb 1, 2027

Why it matters They have a stronger method already, so sign-in keeps working, but the phone method will stop working and helpdesk calls follow when people try it.

What to do Remove the phone methods, or disable SMS and voice in the Authentication methods policy once everyone has a replacement.

Evidence

- tbaker@dental.example.com
- sortiz@dental.example.com
- pwalker@dental.example.com

▶ How to fix it (about 2 minutes per user)

Mail

HIGH **Mailboxes allow SMTP AUTH (usually a copier, scanner or app sending mail)** Deadline Dec 31, 2026

Why it matters SMTP AUTH with basic authentication is turned off by default at the end of December 2026. Scan-to-email and app notifications that use these mailboxes stop sending, usually without anyone noticing until a customer asks.

What to do Find what sends through each mailbox, then move it to OAuth, Microsoft's High Volume Email, or an SMTP relay through a connector. Switch SMTP AUTH off on the mailbox afterwards.

Evidence

- billing@dental.example.com - SMTP AUTH switched on for this mailbox

- scanner@dental.example.com - SMTP AUTH switched on for this mailbox

▶ How to fix it (about 30-90 minutes per device)

HIGH **Apps use Exchange Web Services (EWS), which stops working April 1, 2027** Deadline Apr 1, 2027

Why it matters	Typical EWS users: backup tools, CRM and email-archiving add-ons, room booking, older Mac mail apps and in-house scripts. Microsoft disables EWS permanently and they stop syncing.
What to do	Ask each vendor for their Microsoft Graph version and its release date, upgrade before April 2027, then remove the EWS permission.
Evidence	• Mailbox backup service - Application permission (full mailbox access via EWS) • frontdesk@dental.example.com signed in via EWS (Mailbox backup service)

▶ How to fix it (depends on the vendor)

HIGH **Mailboxes are set to forward mail outside the company**

Why it matters	Forwarding to personal addresses leaks client data and is a classic sign of a compromised mailbox. External forwarding is allowed by the outbound policy, so this mail is leaving the company now.
What to do	Confirm each one with the person and their manager. Remove forwarding that isn't approved, and if any is unexplained, treat the account as compromised (reset password, revoke sessions, review inbox rules).
Evidence	• apatel@dental.example.com forwards to anita.personal@example.net (keeps a copy)

▶ How to fix it (about 15 minutes per mailbox; 1-2 hours if compromise is suspected)

Admin and licensing

MEDIUM **Disabled accounts still hold paid licences**

Why it matters	Usually leavers. Each one is a monthly licence being paid for nobody.
What to do	Convert the mailbox to a shared mailbox if the mail is needed (no licence required under 50 GB), then remove the licence.

Evidence
- jmurphy@dental.example.com
- avega@dental.example.com

▶ How to fix it (about 5 minutes per account)

LOW **Licensed users with no sign-in in 90 days**

Why it matters: Unused accounts cost licences and are easy targets because nobody notices activity on them.

What to do: Confirm with the business, then block sign-in, convert to shared mailboxes or remove the licence.

Evidence
- oldlab@dental.example.com

▶ How to fix it (about 5 minutes per account)

What was read

Area	Result
Tenant	Read
Security defaults	Read
Conditional Access	Read
Licences	Read
Users and last sign-in	Read
MFA registration report	Read
MFA methods per user	Read
Admin roles	Read
Apps using Exchange Web Services	Read
Legacy and EWS sign-ins	Read
Exchange organization settings	Read
Mailboxes	Read

Read-only check of Microsoft Entra ID and Exchange Online. Sign-in history covers the last 30 days. Attestry 0.2.0.