Microsoft 365 Security Health Check

Lab case study: what a 3-day check finds, and what 30 minutes of fixes changes

Prepared by: **Cuong Do**, Microsoft 365 & Azure Security Engineer (AZ-500) | Date: November 2026 | Access used: Global Reader (read-only)

LAB BUILD. Every number and screenshot in this document comes from a Microsoft 365 Business Premium lab tenant I built and scanned myself. No customer data is shown.

1. At a glance

92	751	35 → 29	26 → 33	116 → 102	~30 min
CISA baseline controls checked (ScubaGear)	extra automated tests (Maester)	failed controls after 6 fixes	passed controls after 6 fixes	Maester failures after the same fixes	time to apply the 6 fixes

A brand-new Microsoft 365 tenant is **not secure by default**. Out of the box, this tenant failed 35 of the U.S. CISA "SCuBA" security baseline controls and 116 of Maester's tests, even though Business Premium already pays for most of the protection that was missing. The biggest gaps were in identity (who can sign in and how), app permissions, file sharing and email spoofing.

Six low-risk fixes, chosen because they take a few minutes each and do not disturb users, moved 6 controls from Fail to Pass and 1 from Warning to Pass, and cut Maester failures from 116 to 102. Every fix was checked again with the same tools, so the "after" numbers are measured, not estimated.

2. The scenario

Item	Lab tenant
Licence	Microsoft 365 Business Premium (includes Entra ID P1, Defender for Office 365 P1, Intune, Purview basics)
Users	7 users in 2 groups (Sales, IT), 1 Global Administrator, 1 Global Reader used for scanning
Starting point	Microsoft defaults. Security defaults replaced by Microsoft-managed Conditional Access policies (MFA for admins, MFA for all users, block legacy authentication).
Typical real client	20-300 staff company or MSP customer on Business Premium or E3/E5

3. How the check works

- **Read-only access.** I only need a Global Reader account plus a one-time admin consent for the Microsoft Graph read permissions. Nothing is changed during the check.
- **Two free, trusted tools. ScubaGear** is published by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and checks Entra ID, Exchange Online, Defender, SharePoint/OneDrive and Teams against its secure baseline. **Maester** is an open-source test framework that adds Microsoft's

Entra recommendations (EIDSCA), CIS Microsoft 365 Benchmark checks and the Office 365 Recommended Configuration Analyzer (ORCA).

- **Human review.** Every failed item is read, explained in plain English, checked against your licence and ranked by risk. Tool output alone is not the report.
- **Where tools stop.** Neither tool covers Intune device settings or Defender for Endpoint in depth. For clients using those, I add Microsoft Secure Score and a manual checklist.

4. What the first scan found

ScubaGear, run 1 (before any fix)

Product	Pass	Fail	Warning	Main issues
Entra ID (identity)	6	17	8	No phishing-resistant MFA, users can register apps and grant them access, weak MFA methods allowed, all admins are Global Admins
Exchange Online (email)	5	5	2	No DMARC, full calendar details shared with any domain, no [External] tag on outside mail
Defender / Purview	10	2	9	Audit log not recording, no DLP policy for card numbers
SharePoint / OneDrive	0	8	0	"Anyone" links allowed, default link too broad, links never expire
Teams	5	3	6	Anyone on Teams (including personal accounts) can message staff, email-to-channel open
Total	**26**	**35**	**25**	6 more items were not applicable

Highest-risk findings, in plain English

Risk	Finding	Why it matters
High	Audit log not recording	If an account is compromised, there is no record of what the attacker read, changed or deleted.
High	Any user can approve third-party apps and register new apps	"Consent phishing": one click on a fake app gives an attacker ongoing access to that user's mail and files, and MFA does not stop it.
High	Admins not required to use phishing-resistant MFA	Modern phishing kits steal the session even after the user approves MFA. One stolen admin session means full tenant takeover.
High	No DMARC on the email domain	Anyone can send email that looks like it comes from your company to your customers and suppliers.
High	Teams open to every external and personal account	Fake "IT helpdesk" chats on Teams are a common way in for ransomware groups.
Medium	SMS, voice call and email codes allowed for MFA	These codes can be intercepted (SIM swap) or phished more easily than app or passkey approval.
Medium	SharePoint/OneDrive "Anyone" links with no expiry	A link forwarded once stays open to anyone, forever.
Licence	Risk-based sign-in blocking, Privileged Identity Management	Need Entra ID P2 (E5). Listed separately so the client sees what an upgrade would buy, not as a failure.

Maester, run 1: a second opinion

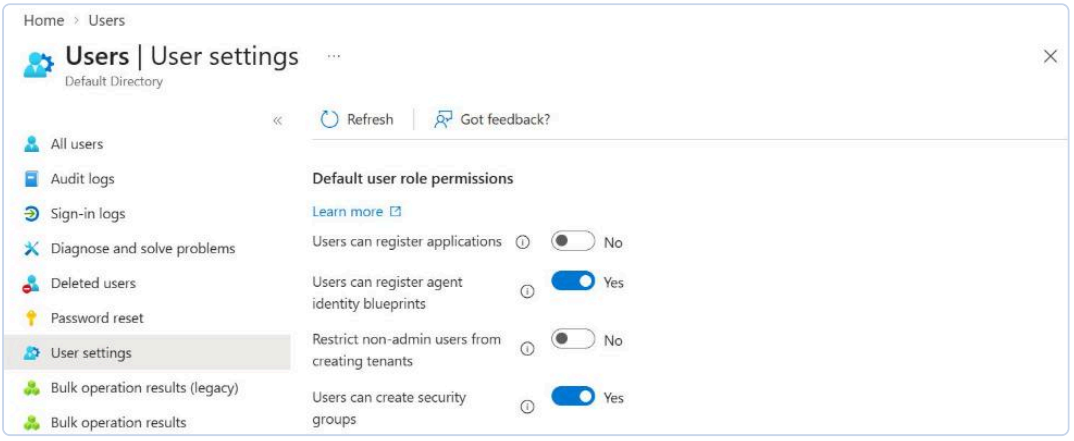
751 tests, 112 passed, 116 failed, the rest skipped or not applicable to this licence. The failures confirmed the ScubaGear picture and added detail: Entra configuration (23, EIDSCA), CIS Benchmark (13), CISA (15), email protection in Defender for Office 365 (21, ORCA) and Maester's own Conditional Access and tenant-hygiene tests (44). Using two tools means a finding is reported only when it is real, and the client gets the benchmark names auditors recognise.

5. Fixes applied (about 30 minutes)

For this case study I applied six fixes that are quick, reversible and safe to roll out without user training. Each one maps to a CISA control ID so the client can show it to an auditor.

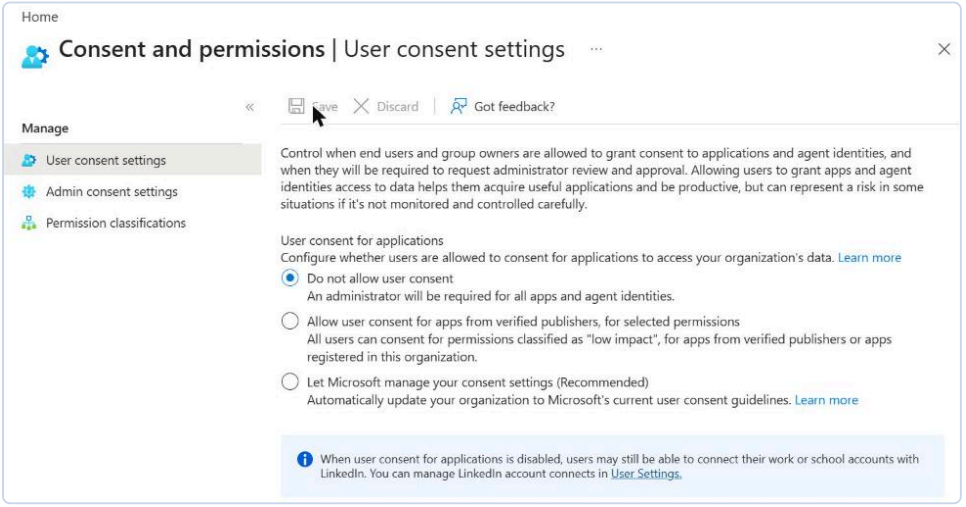
Fix 1. Only admins can register applications (MS.AAD.5.1)

Entra ID > Users > User settings > "Users can register applications" = No.



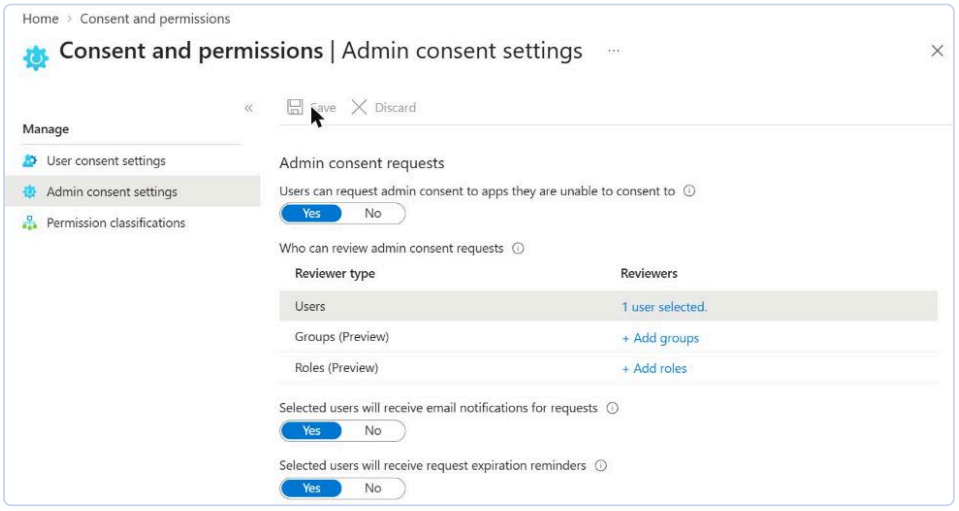
Fix 2. Users can no longer grant apps access to company data (MS.AAD.5.2)

Enterprise apps > Consent and permissions: changed from "Let Microsoft manage your consent settings" to "Do not allow user consent".



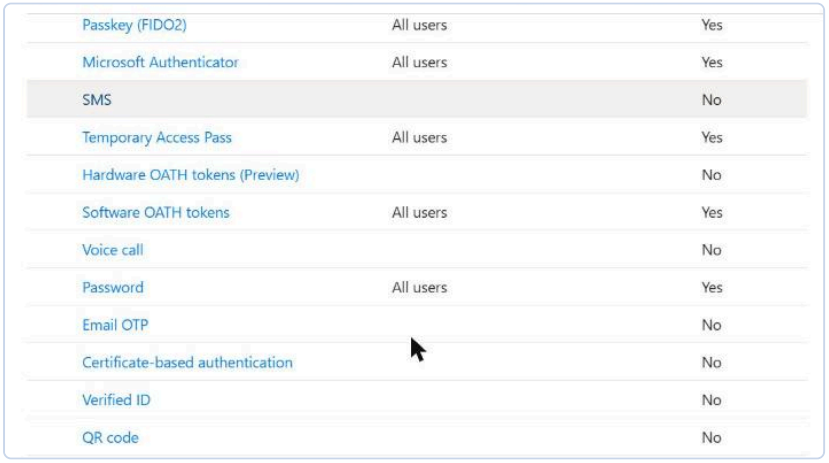
Fix 3. Admin approval workflow for app requests (MS.AAD.5.3)

So users are not blocked: they can request an app, and a named admin approves or rejects it, with email notifications and reminders.



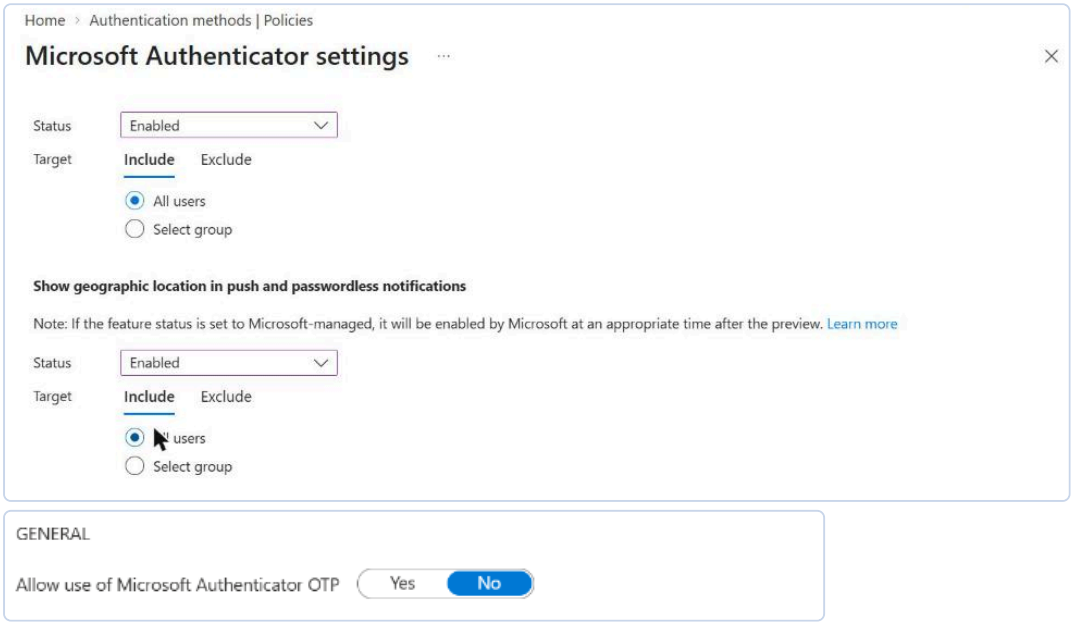
Fix 4. Weak MFA methods switched off (MS.AAD.3.5)

SMS and voice call were already off. Email one-time passcode was switched off. Passkeys and Microsoft Authenticator stay on. Checked first that the admin account signs in with a passkey, so nobody is locked out.



Fix 5. Authenticator shows the app name and sign-in location, OTP codes off (MS.AAD.3.3)

Changed from "Microsoft managed" to Enabled, so a user who gets an unexpected approval request sees where it comes from. The first re-scan still failed this control: the CISA rule also requires the Authenticator one-time code option to be off, because a six-digit code can be phished while a number-matching push cannot. Switched it off; the second re-scan passed. A good example of why every result is checked by a person, not just by the tool.



Fix 6. Unified audit log turned on (MS.SECURITYSUITE.5.1)

Without it, there is no record of what an attacker read, changed or deleted after a break-in. The Purview portal button kept looping on this brand-new tenant, so it was turned on with one PowerShell command (`Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true`). Exchange refused the command on day one while Microsoft was still provisioning the tenant, and accepted it the next morning; the setting showed True about an hour later. On an established client tenant this is a one-minute change.

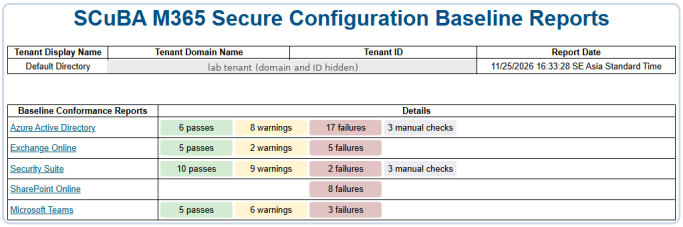
6. Before and after

Product	Pass before	Pass after	Fail before	Fail after
Entra ID	6	11	17	12
Defender / Purview	10	12	2	1
Exchange Online	5	5	5	5
SharePoint / OneDrive	0	0	8	8
Teams	5	5	3	3
Total	**26**	**33**	**35**	**29**

Moved from Fail to Pass: MS.AAD.3.3 (Authenticator context), MS.AAD.3.5 (weak MFA methods), MS.AAD.5.1 (app registration), MS.AAD.5.2 (user consent), MS.AAD.5.3 (admin consent workflow), MS.SECURITYSUITE.5.1 (audit log). **Moved from Warning to Pass:** MS.SECURITYSUITE.1.4.

Maester, run 2 (with Teams connected this time): 139 passed, **102 failed**, against 112 / 116 before the fixes. The two tools agree on what changed, which is the point of running both.

ScubaGear, before (25 Nov, 16:33)

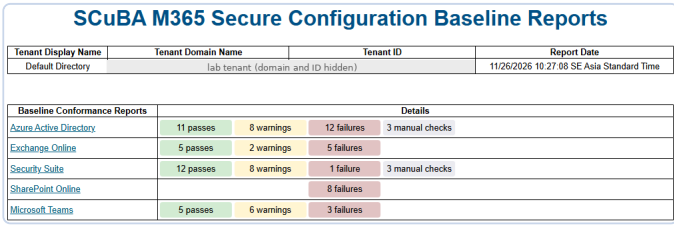


SCuBA M365 Secure Configuration Baseline Reports

Tenant Display Name	Tenant Domain Name	Tenant ID	Report Date
Default Directory	lab tenant (domain and ID hidden)		11/25/2026 16:33:28 SE Asia Standard Time

Baseline Conformance Reports	Details			
Azure Active Directory	6 passes	8 warnings	17 failures	3 manual checks
Exchange Online	5 passes	2 warnings	5 failures	
Security Suite	10 passes	9 warnings	2 failures	3 manual checks
SharePoint Online			8 failures	
Microsoft Teams	5 passes	6 warnings	3 failures	

ScubaGear, after (26 Nov, 10:27)

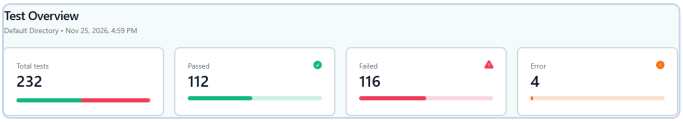


SCuBA M365 Secure Configuration Baseline Reports

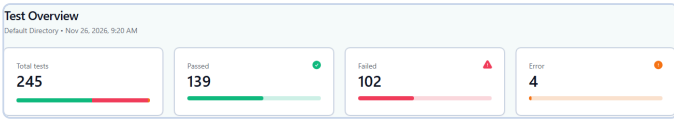
Tenant Display Name	Tenant Domain Name	Tenant ID	Report Date
Default Directory	lab tenant (domain and ID hidden)		11/26/2026 10:27:08 SE Asia Standard Time

Baseline Conformance Reports	Details			
Azure Active Directory	11 passes	8 warnings	12 failures	3 manual checks
Exchange Online	5 passes	2 warnings	5 failures	
Security Suite	12 passes	8 warnings	1 failure	3 manual checks
SharePoint Online			8 failures	
Microsoft Teams	5 passes	6 warnings	3 failures	

Maester, before (25 Nov)



Maester, after (26 Nov)



Exchange, SharePoint and Teams did not change because they were not part of this first round. The SharePoint (8 controls) and Teams (3 controls) fixes are each made on a single settings page, so a second short round would remove roughly a third of the remaining failures.

7. What is still open, and why

- **Conditional Access and device compliance.** Most of the remaining Entra ID failures need a proper set of Conditional Access policies (break-glass exclusions, legacy and device-code flows blocked, sign-in frequency) and, for device checks, Intune. These are planned with the client, piloted in report-only mode for a week, then switched on.
- **Licence-limited items.** Risk-based policies and Privileged Identity Management need Entra ID P2. Reported as an upgrade option, not as a failure.
- **DMARC.** The lab only has the default onmicrosoft.com domain. On a real company domain this is a DNS change and one of the highest-value fixes.

8. Lessons that save clients time

- **"Microsoft managed" is not "on".** Several settings default to "Microsoft managed", which the baseline does not accept. They must be set explicitly.
- **Security defaults and Conditional Access cannot run together.** Moving to Conditional Access needs a plan so there is no gap in MFA coverage.
- **Break-glass accounts must be declared.** Microsoft's own managed policies exclude some accounts, which the baseline flags. The check records which exclusions are intentional.
- **Check sign-in methods before switching any off.** Done here first, so no account was locked out.

9. What a client receives

Package	What is included
Security Health Check 3 days, fixed price	Read-only scan with ScubaGear and Maester, Secure Score review, PDF report with findings ranked by risk in plain English, a 30-day fix plan, and a 30-minute call to walk through it. Access needed: one Global Reader account.
Fix round (optional)	I apply the agreed quick fixes, starting in report-only mode where users could be affected, then re-scan and give you the before/after numbers, like section 6.
Identity hardening	Conditional Access set, phishing-resistant MFA for admins, break-glass accounts, PIM where licensed, handover document.

About me. Microsoft 365 and Azure security engineer, AZ-500 certified. Hands-on with Microsoft Sentinel, Defender XDR, Entra ID Conditional Access, Purview DLP and labels, for MSSP and financial-services environments.

Contact: linkedin.com/in/cuongdohung | upwork.com/freelancers/cdsecuritylab

---

Lab build. Tools: CISA ScubaGear 2.0 (Windows PowerShell 5.1) and Maester 2.3 (PowerShell 7), run 25 and 26 November 2026 with a Global Reader account (fixes applied with a separate Global Administrator account). Control IDs refer to the CISA Secure Cloud Business Applications (SCuBA) baselines.