anoBytes | TECHNOLOGY SOLUTIONS

Set up and secure a new Microsoft 365 tenant

A security baseline for a small business on Microsoft 365 Business Premium. Covers admin accounts, multifactor authentication and Conditional Access, application consent, email protection, sharing defaults, and audit logging, with Microsoft Secure Score to track progress.

MICROSOFT 365 · CIS M365 FOUNDATIONS BENCHMARK v7.0.0 · MICROSOFT SECURE SCORE · HOW-TO GUIDE

Recommendation numbers refer to the CIS Microsoft 365 Foundations Benchmark v7.0.0 (20 May 2026). Published 2026-08-13.

12 steps, tenant to verification

identity first, then email, then sharing, then the audit trail

60 benchmark recommendations

of the 160 in CIS v7.0.0, the tenant-wide settings that fit this license

SCOPE

What this guide covers, and what it does not

The CIS Microsoft 365 Foundations Benchmark v7.0.0 holds 160 recommendations across nine sections, spanning the Microsoft 365 admin center, Defender, Purview, Intune, Entra, Exchange, SharePoint, Teams, and Fabric. This guide implements the 60 that form a tenant-wide security baseline you can set in a small number of sittings on a new tenant: admin accounts and roles, authentication, application consent, email protection, external sharing, and audit logging. Purview data loss prevention, Intune device management, and Fabric are their own projects and stay out of scope, apart from the two Intune settings in NEXT. Mail migration is out of scope too: the guide assumes mailboxes that start empty, and moving existing mail in from another provider is its own project.

The license this guide assumes

Microsoft 365 Business Premium, the plan most small businesses hold. It includes Microsoft Entra ID P1 (which provides Conditional Access), Microsoft Defender for Office 365 Plan 1 (Safe Links, Safe Attachments, and impersonation anti-phishing), and Microsoft Intune. It does bring a boundary: features that need Entra ID P2, Defender for Office 365 Plan 2, or E5 are listed in EXCEPT so you can record them as accepted gaps.

How the benchmark's profiles map to this license

Every recommendation carries a profile: E3 Level 1, E3 Level 2, E5 Level 1, or E5 Level 2, tracking the enterprise license tiers. Business Premium sits between them. Almost every E3 Level 1 item applies to it directly, and because the plan includes Defender for Office 365 Plan 1, the email controls the benchmark files under E5 (Safe Links 2.1.1, Safe Attachments 2.1.4, the anti-phishing policy 2.1.7) are reachable too. Where a step below includes a Level 2 item, it says so.

Why the step order matters

The emergency access accounts in Step 2 must exist before the Conditional Access policies in Step 3, because those policies can lock every admin out and the excluded emergency account is the way back in. In email, SPF and DKIM must be publishing before DMARC moves to an enforcing policy, which is why Step 7 stages the records.

A new tenant is the easy case

The benchmark is written as an audit of a live tenant. On an empty one, every setting below costs minutes and breaks nobody, because there are no users, devices, or mail flows to disrupt yet. The same settings applied a year in produce lockouts, dead printers, and confused guests; the HELP section lists what each one breaks so you can still apply this to a tenant with people in it.

SCORE Track progress with Microsoft Secure Score

Microsoft Secure Score lives in the Microsoft Defender portal at `security.microsoft.com/securescore`. It lists recommended actions for the Microsoft products you hold, awards each action up to 10 points, and expresses your posture as a percentage. Most actions score all-or-nothing; some score partially, in proportion to the users or devices covered. Open it before Step 1 and note the number, then watch it climb as the steps land.

The action names match the benchmark on purpose

Since 2023 Microsoft has been adding Secure Score actions whose names use the CIS benchmark's own wording: "Ensure that SPF records are published for all Exchange Domains", "Ensure Safe Links for Office Applications is enabled", "Ensure the admin consent workflow is enabled". Where a step below has a matching action, it names it, so you can watch the same control tick off in both frameworks with one change.

The score updates on its own schedule

Points for a change can take a day or more to appear. Microsoft Entra recommendation states refresh weekly and Microsoft Teams states refresh monthly, so finish the steps, then judge the score after a week rather than after an hour. If a control is handled by a tool outside Microsoft 365, mark the action resolved through a third party or alternative mitigation instead of leaving it open.

Some actions will never appear for you

Secure Score only shows actions for products the tenant is licensed for, and a batch of its CIS-worded actions surface only when Microsoft Defender for Cloud Apps is connected, which Business Premium does not include. The settings behind them still apply and this guide still sets them; you just will not see every one of them credited in the portal.

100% is the wrong target

The full action list includes items that need a higher license and items whose business cost you may decline. The realistic goal for a small business on this baseline is a score well above the "organizations like yours" comparison line, every reachable identity and email action closed, and a written reason for anything left open. The exception register template on our resources page holds those reasons.

PREP Before you start

- A **custom domain you control** and sign-in access to its **DNS host** (DNS is the internet's name directory; its records are where Step 7's email authentication lives).
- A **password manager**, already in use, for the admin and emergency account credentials this guide creates.

- **Two phones or hardware security keys** for multifactor authentication (MFA: a second proof of identity at sign-in, beyond the password), plus a plan for who holds the emergency credentials.
- The **names of your admins**. Decide now who the two to four administrators will be, and which everyday accounts they will keep separate from their admin accounts.
- A **role mailbox** such as `it@example.com` for security notifications, so alerts survive any one person leaving.
- About **three hours** for the portal work, plus a week of waiting built into Steps 3 and 7 before their enforcement switches flip.

MAP The twelve steps at a glance

The waits in Steps 3 and 7 spread this work over at least a week, so most people do it in more than one sitting. This map shows where each step happens and which steps hold a wait, so the next sitting can start where the last one stopped.

STEP	WHERE	BUILT-IN WAIT
01 Create the admin accounts properly	`admin.microsoft.com`	none
02 Create two emergency access accounts	`admin.microsoft.com`	none
03 Move to Conditional Access	`entra.microsoft.com`	a week in report-only before switching On
04 Harden how people authenticate	`entra.microsoft.com`	none
05 Turn on self-service password reset	`entra.microsoft.com`	none
06 Put app consent behind an admin	`entra.microsoft.com`, `admin.microsoft.com`	none
07 Publish SPF, DKIM, and DMARC	`your DNS host`, `security.microsoft.com`	a week or two at p=none before p=reject
08 Turn on the Defender email protections	`security.microsoft.com`	none
09 Harden Exchange Online mail flow	`security.microsoft.com`, `admin.exchange.microsoft.com`, `PowerShell`	none
10 Set the external sharing defaults	`SharePoint, Entra, and Teams admin centers`	none
11 Confirm the audit trail is recording	`purview.microsoft.com`	none
12 Verify with PowerShell, read the score	`PowerShell, security.microsoft.com`	judge the score after a week

01 Create the admin accounts properly

The first account in the tenant is a Global Administrator, the role that can change anything, and the shape of your admin accounts is the first thing the benchmark tests. Three rules from its opening section:

Admin accounts are separate accounts (CIS 1.1.1)

Each administrator gets a dedicated admin account used only for admin work, alongside the everyday account they read email with. The benchmark also wants admin accounts cloud-only: created in Microsoft 365, never synchronized from a local Active Directory, so a compromise on that side cannot reach the tenant's controls. With no on-premises directory, a new tenant passes this by default; keep it that way if you ever add synchronization.

Two to four Global Administrators (CIS 1.1.3)

One is a single point of failure; more than four is attack surface. Assign the role in the Microsoft 365 admin center at `admin.microsoft.com` under **Users > Active users**, through **Manage roles** on each account. The two emergency access accounts from Step 2 count toward the number, so a company of one still lands at three. Prefer lesser roles for everything routine: Exchange Administrator, SharePoint Administrator, and User Administrator each run their own service without holding the whole tenant.

Admin accounts carry as few licensed apps as possible (CIS 1.1.4)

An admin account with a mailbox can be phished; one without a mailbox cannot receive the lure. Leave admin accounts unlicensed, or license them only for Entra ID, and let the person's everyday account hold the Office apps. This also means admin account credentials never live in an inbox rule's reach.

Secure Score tracks the admin-account shape as "Ensure Administrative accounts are separate, unassigned, and cloud-only". Related actions covering MFA for these accounts arrive with Step 3.

02 Create two emergency access accounts

Before any policy exists that could lock administrators out, create the way back in (CIS 1.1.2). These are the accounts you will exclude from Conditional Access in Step 3, so they must exist first. In **Users > Active users** at `admin.microsoft.com`, create two accounts with these properties:

- **Named for the function** ("Emergency Access 1"), never for a person, so they survive any departure.
- **On the default `.onmicrosoft.com` domain**, so a problem with your custom domain or its DNS cannot take them down too.
- **No license assigned**, and the **Global Administrator** role assigned permanently.
- **A random password of at least 16 characters**, generated, printed or split, and stored offline in a safe or two, never in the everyday password manager alone.

These accounts need phishing-resistant MFA too

MICROSOFT'S MANDATORY MFA FOR ITS ADMIN PORTALS ROLLED OUT FROM OCTOBER 2024, WITH NO EXCEPTION FOR BREAK-GLASS ACCOUNTS

An emergency account that cannot complete MFA is not a way back in. The benchmark's guidance is to register a passkey (FIDO2: a hardware security key that signs you in and resists phishing by design) or certificate-based authentication for each emergency account, and to keep those keys locked away separately from the passwords. Test a full sign-in with each account twice a year, on a calendar, and review its sign-in log afterwards. A method that has quietly stopped working is otherwise found only when the account is needed. Any sign-in outside those tests is an incident, which is what the REVIEW table's monitoring row is for (CIS 2.2.1).

03 Move from security defaults to Conditional Access

A new tenant arrives with security defaults on: a fixed bundle that requires MFA registration for everyone, MFA for admins, blocks legacy authentication, and blocks device code sign-in. It is a good floor, and it allows no exclusions, so your emergency accounts would face the same enforcement as everyone else. Business Premium includes Conditional Access (CA: Entra's if-this-then-that sign-in policy engine), which enforces the same protections with the exclusions and session controls the benchmark asks for. Turn security defaults off under **Entra ID > Overview > Properties > Manage security defaults** at `entra.microsoft.com`, then immediately create these four policies under **Entra ID > Conditional Access > Policies**.

POLICY	SHAPE	CIS	SECURE SCORE ACTION
MFA for admin roles	Include the directory roles listed below; target all resources; grant access requiring multifactor authentication. Exclude one emergency account.	5.2.2.1	Require MFA for administrative roles
MFA for all users	Include all users; target all resources; grant access requiring multifactor authentication. Exclude one emergency account.	5.2.2.2	Ensure all users can complete multifactor authentication for secure access
Block legacy authentication	Include all users; target all resources; under Conditions > Client apps select Exchange ActiveSync clients and Other clients; block access. Exclude one emergency account.	5.2.2.3	Enable policy to block legacy authentication
Admin sessions expire	Include the same directory roles; target all resources; grant with MFA; under Session set Sign-in frequency to 4 hours or less and Persistent browser session to Never persistent. Exclude one emergency account.	5.2.2.4	Ensure Sign-in frequency is enabled and browser sessions aren't persistent for Administrative users

The benchmark's minimum role list for the two admin policies: Application, Authentication, Billing, Cloud application, Conditional Access, Exchange, Global, Helpdesk, Password, Privileged authentication, Privileged role, Security, SharePoint, and User administrator, plus Global reader.

Run each policy in report-only mode for a week first

THE BENCHMARK'S OWN ROLLOUT GUIDANCE, AND THE LOCKOUT INSURANCE

Report-only mode evaluates every sign-in against the policy and logs what would have happened, without enforcing. Create the two MFA policies and the session policy in report-only, read the sign-in logs after a week, then switch them to On. The legacy authentication block can go straight to On in an empty tenant, because there are no old clients yet to break. Never delete the excluded emergency account from a policy to tidy up. Without that exclusion, a policy that locks the admins out leaves a Microsoft support case as the only way back into your own tenant.

Security defaults also blocked device code sign-in, a flow made for keyboardless devices that phishers abuse. CA can block it too (CIS 5.2.2.12, under Conditions > Authentication flows); add that policy once the four above are stable.

04 Harden how people authenticate

Step 3 decided when MFA is demanded. This step decides what counts as MFA, in **Entra ID > Authentication methods** at `entra.microsoft.com`, plus two password rules.

SETTING	SET IT TO	CIS	WHY
Legacy per-user MFA	`Disabled for all accounts`	`5.1.2.1`	The pre-Conditional-Access MFA switch, under Users > All users > Per-user MFA. Left enabled it conflicts with CA and confuses sign-in prompts. Step 3's policies replace it entirely.
Microsoft Authenticator	`Show app name and geographic location: both Enabled, all users`	`5.2.3.1`	Under Policies > Microsoft Authenticator > Configure. A push prompt that names the app and the city makes a fraudulent prompt look wrong, which weakens MFA-fatigue attacks that spam approvals until someone taps yes.
System-preferred MFA	`Enabled, all users`	`5.2.3.6`	Under Settings. Sign-in offers the strongest method the person has registered instead of the one they registered first.
SMS and Voice call	`Off`	`5.2.3.5`	Under Policies. Phone-based codes fall to SIM swaps and phishing relays. Check who has only a phone registered before flipping this on a live tenant; see HELP.
Email OTP	`Off`	`5.2.3.7`	A one-time passcode (OTP) sent to email is only as strong as that mailbox. Level 2, and cheap to hold on a new tenant.
Custom banned password list	`Enforce custom list: Yes`	`5.2.3.2`	Under Password protection. Load it with your brand and product names, your town, and company shorthand: the words someone at your company would build a password from. Secure Score: "Ensure custom banned passwords lists are used".
Password expiration	`Set passwords to never expire`	`1.3.1`	At admin.microsoft.com under Settings > Org settings > Security & privacy. Forced rotation produces predictable increments; both CIS and Microsoft now recommend expiry off, with strength coming from MFA and the banned list.

05 Turn on self-service password reset

Self-service password reset (SSPR) lets people reset their own forgotten passwords after proving who they are, which removes the least verifiable helpdesk call a small business has: a voice on the phone asking for a reset. In **Entra ID > Password reset** at `entra.microsoft.com`:

- Under **Properties**, set **Self service password reset enabled** to **All** (CIS 5.2.4.1).
- Under **Authentication methods**, set the **number of methods required to reset** to **2**, so a reset takes two independent proofs (CIS 5.2.4.2, Level 2).
- Under **Notifications**, set both **Notify users on password resets** and **Notify all admins when other admins reset their password** to **Yes**. A reset the owner did not ask for becomes an alarm within minutes (CIS 5.2.4.4, 5.2.4.5).

People register their methods on the Security info page at `myprofile.microsoft.com`; the MFA methods from Step 4 double as reset methods, so for most users registration is one combined prompt at next sign-in.

06 Put application consent behind an admin

Attackers who cannot beat MFA ask the user to hand access over instead: a mail titled "shared document" leads to a real Microsoft consent screen for a malicious app, and one click grants it standing access to the mailbox with no password stolen at all. These six settings move every such grant through an admin.

SETTING	SET IT TO	CIS	WHERE
User consent for applications	`Do not allow user consent`	`5.1.5.1`	entra.microsoft.com > Entra ID > Enterprise apps > Security > Consent and permissions. Level 2, and the core of this step.
Admin consent workflow	`Enabled, with named reviewers who get email notifications`	`5.1.5.2`	Same blade, Admin consent settings. Users request, an admin decides; without this, blocked consent becomes shadow IT pressure. Secure Score: "Ensure the admin consent workflow is enabled".
Users can register applications	`No`	`5.1.2.2`	entra.microsoft.com > Entra ID > Users > User settings. App registrations become an admin task.
Restrict non-admin users from creating tenants	`Yes`	`5.1.2.3`	Same blade. A user-created side tenant is an unmanaged copy of your user directory.
User owned apps and services	`Both boxes cleared`	`1.3.4`	admin.microsoft.com > Settings > Org settings > User owned apps and services: no Office Store access, no self-started trials. Secure Score: "Ensure 'User owned apps and services' is restricted".
Microsoft Forms phishing protection	`Add internal phishing protection: checked`	`1.3.5`	Same Org settings list, Microsoft Forms. Scans forms your own users publish for credential-harvesting patterns.

07 Publish SPF, DKIM, and DMARC for every domain

Three DNS records let the world's mail servers verify mail claiming to be from your domain, and let yours reject imposters. SPF (a list of servers allowed to send as your domain), DKIM (a cryptographic signature on each message), and DMARC (the policy telling receivers what to do when both fail) are CIS 2.1.8, 2.1.9, and 2.1.10, all Level 1. Publish them at your DNS host in this order.

1. SPF, today

One TXT record on each sending domain: `v=spf1 include:spf.protection.outlook.com -all`. If a newsletter tool or website also sends as the domain, add its include before the `-all`. The `-all` ending tells receivers to fail anything else.

2. DKIM, today

In the Defender portal at `security.microsoft.com` under **Email & collaboration > Policies & rules > Threat policies > Email authentication settings > DKIM**, select the domain and create the DKIM keys. Microsoft hands you two CNAME records; publish them at your DNS host, return, and toggle signing to **Enabled**. The status line confirms when signatures are flowing.

3. DMARC, in monitor mode first

A TXT record at `_dmarc.example.com`: `v=DMARC1; p=none; rua=mailto:dmarc-reports@example.com; ruf=mailto:dmarc-reports@example.com`. The `p=none` policy changes no delivery yet; it makes receivers send you aggregate reports (the `rua` address) showing exactly who is sending as your domain, plus per-message failure samples (`ruf`) from the receivers that send them. After a week or two of clean reports, move to enforcement: `v=DMARC1; p=reject; pct=100; rua=mailto:dmarc-reports@example.com; ruf=mailto:dmarc-reports@example.com`.

4. The domains that send nothing

Parked domains and the default `.onmicrosoft.com` domain are spoofing targets precisely because nobody watches them. Give each a DMARC record of `v=DMARC1; p=reject;`, and give parked custom domains an SPF record of `v=spf1 -all`, which authorizes no sender at all. The .onmicrosoft.com domain already carries Microsoft's own SPF record; its DNS records are edited at admin.microsoft.com under Settings > Domains.

Secure Score: "Ensure that SPF records are published for all Exchange Domains". Verify from outside with any public DMARC checker, or `dig txt _dmarc.example.com`.

08 Turn on the Defender for Office 365 email protections

Business Premium includes Defender for Office 365 Plan 1: Safe Links (URLs checked at click time, after delivery), Safe Attachments (attachments detonated in a sandbox before delivery), and anti-phishing with impersonation protection (quarantining mail that poses as your own people or domains). The benchmark files these under its E5 profile, at Level 2, because plain E3 lacks them; on this plan they are yours to switch on.

The fast route: assign the Standard preset security policy

ONE WIZARD COVERS CIS 2.1.1, 2.1.4, AND 2.1.7

At `security.microsoft.com` under **Email & collaboration > Policies & rules > Threat policies > Preset security policies**, turn on **Standard protection** and apply it to all recipients. In the wizard, add your executives and finance staff to the impersonated-users list (it protects up to 350) and confirm your domains are flagged for impersonation. The preset creates Microsoft-maintained Safe Links, Safe Attachments, anti-phishing, anti-spam, and anti-malware policies, sets the phishing threshold to 3 (the level CIS 2.1.7 asks for), and Microsoft updates the settings as threats change. The trade-off is fixed settings: nothing inside a preset can be edited, which for a small business saves the upkeep of maintaining its own policies. If you need different values for some users later, scope those users out of the preset and build them custom threat policies from the benchmark's per-setting guidance, because a recipient covered by a preset always gets the preset's values regardless of custom policies.

Three settings sit outside the preset and need a minute each in the same Threat policies area:

- **Common attachment types filter** (CIS 2.1.2): in the default **Anti-malware** policy, confirm the filter is enabled so executable attachment types are stripped regardless of scan verdict.
- **Safe Attachments for SharePoint, OneDrive, and Teams** (CIS 2.1.5): under **Safe Attachments > Global settings**, enable it so a malicious file uploaded to a shared library is caught there too. The Safe Documents toggles on that pane need an E5-level license; record them in EXCEPT.
- **Outbound spam notifications** (CIS 2.1.6): in the default **Anti-spam outbound policy**, notify the role mailbox when a sender is blocked for outbound spam, and Bcc it a copy of suspicious outbound mail, which is how you learn one of your own accounts was compromised.

Keep every allow list empty: no allowed sender domains in anti-spam policies (CIS 2.1.14) and no IP allow list in the connection filter (CIS 2.1.12). An allow list entry skips the filtering you just configured, and "add our own domain to the allow list" is a classic misconfiguration that turns self-spoofing into guaranteed delivery. Secure Score tracks this family as "Ensure Safe Links for Office Applications is enabled", "Ensure Safe Attachments policy is enabled", and "Ensure that an anti-phishing policy was created".

09 Harden Exchange Online mail flow

Seven settings spread across the Defender portal, the Exchange admin center at `admin.exchange.microsoft.com`, and Exchange Online PowerShell close the mail-flow gaps attackers use after compromising a mailbox, or instead of compromising one.

SETTING	SET IT TO	CIS	WHY
Automatic forwarding to external addresses	`Off`	`6.2.1`	In the Defender portal's default Anti-spam outbound policy, set Automatic forwarding rules to Off. A silent forward-everything inbox rule is the classic persistence move after a mailbox compromise: the attacker keeps reading long after the password changes. Secure Score: "Ensure all forms of mail forwarding are blocked and/or disabled".
SMTP AUTH	`Turned off for the organization`	`6.5.4`	Under Settings > Mail flow, check Turn off SMTP AUTH protocol for your organization. SMTP AUTH is the old mail submission protocol for apps and devices; modern mail clients no longer use it. The scanner or app that genuinely needs it gets a per-mailbox exception, which beats leaving the protocol open for every mailbox.
Direct Send	`Rejected`	`6.5.5`	One command in Exchange Online PowerShell: `Set-OrganizationConfig -RejectDirectSend $true`. Direct Send lets a device or service deliver mail straight to your mailboxes as your own domain with no sign-in at all, and attackers use it to send phishing that looks internal. Level 2. A printer that sends this way moves to the SMTP AUTH exception in HELP or a connector; mail a third party forwards back into your tenant without rewriting the sender is now rejected too.
External sender identification	`Enabled`	`6.2.3`	One command in Exchange Online PowerShell: `Set-ExternalInOutlook -Enabled $true`. Outlook tags mail from outside the organization, which defeats the display-name trick where "the CEO" writes from a free mailbox.
Modern authentication	`On`	`6.5.1`	On by default in new tenants; confirm at admin.microsoft.com under Settings > Org settings > Modern authentication. It is what lets Step 3's policies see Outlook sign-ins at all. Secure Score: "Ensure modern authentication for Exchange Online is enabled".
MailTips	`All tips on`	`6.5.2`	Turn all four switches on in Exchange Online PowerShell: `Set-OrganizationConfig -MailTipsAllTipsEnabled $true -MailTipsExternalRecipientsTipsEnabled $true -MailTipsGroupMetricsEnabled $true -MailTipsLargeAudienceThreshold 25`. The tip that flags external recipients stops misdirected mail, a quiet and common source of data incidents. Secure Score: "Ensure MailTips are enabled for end users".
Transport rules	`None that bypass filtering for a domain`	`6.2.2`	Under Mail flow > Rules, a new tenant has none; keep it that way. A rule setting spam confidence to -1 for a partner's domain reopens the allow-list hole from Step 8 under another name.

10 Set the external sharing and collaboration defaults

Sharing settings trade security against everyday convenience, so decide them deliberately while nothing is shared yet. The stance below keeps guest collaboration possible and makes every grant specific, signed-in, and expiring.

SETTING	SET IT TO	CIS	WHERE
SharePoint and OneDrive external sharing	New and existing guests	7.2.3	SharePoint admin center (admin.microsoft.com/sharepoint) > Policies > Sharing. Everyone outside must sign in as a guest; anonymous anyone-links are off tenant-wide. OneDrive follows SharePoint and can never be looser.
Default sharing link type	Specific people	7.2.7	Same page, File and folder links. The default link a user mints reaches only the people they name. Anyone can still choose a broader link where the sharing level allows it; the default is what most clicks ship with.
Default link permission	View	7.2.11	Same page. Granting edit rights becomes a deliberate step.
Guest access expiration	Expire automatically after 30 days	7.2.9	Same page, under More external sharing settings. Access granted for one project stops outliving the project; owners can renew what is still needed.
Entra guest permissions	Guest users have limited access to directory objects	5.1.6.2	entra.microsoft.com > Entra ID > External Identities > External collaboration settings. Guests collaborate on what they are invited to and cannot walk the directory.
Who can invite guests	Only users assigned to specific admin roles	5.1.6.3	Same blade. Guest creation becomes an admin decision, which is what makes the 30-day expiry reviewable. Level 2.
External calendar sharing	Off	1.3.3	admin.microsoft.com > Settings > Org settings > Calendar. A shared calendar leaks names, times, and travel; the cost is a little scheduling friction with outside contacts. Level 2.
Teams: chat with unmanaged Teams accounts	Off	8.2.2	Teams admin center (admin.teams.microsoft.com) > External collaboration > External access > Policies. Personal, consumer Teams accounts are a phishing lane with no organization behind them. Federation with real partner tenants stays available.
Teams meetings: anonymous join	Off	8.5.1	Teams admin center > Settings & policies, Global policy, Meetings. Unverified strangers stay out of meetings. Level 2; relax it deliberately if you host public webinars.
Teams meetings: lobby bypass	People in my org	8.5.3	Same pane. External participants wait in the lobby until admitted, so nobody joins a call unnoticed.

11 Confirm the audit trail is recording

Any investigation starts in the unified audit log, and its records only exist from the moment auditing is on. New tenants have it on by default; this step confirms that.

- **Unified audit log** (CIS 3.1.1): open Microsoft Purview at `purview.microsoft.com`, go to the **Audit** solution, and run any search. If the page instead offers a button to start recording user and admin activity, click it; that is the sign auditing

was off. Secure Score: "Ensure Microsoft 365 audit log search is enabled".

- **Exchange organization auditing** (CIS 6.1.1): in Step 12's PowerShell session, confirm `AuditDisabled` is `False` on `Get-OrganizationConfig`.
- **Mailbox audit actions** (CIS 6.1.2): mailbox auditing is on by default, and the benchmark asks for more actions than the default set, including `MailItemsAccessed` style visibility into reads, copies, and folder binds. Apply its extended admin, delegate, and owner action lists with `Set-Mailbox` and set `-AuditLogAgeLimit 180`; rerun it when new mailboxes are created, or quarterly. Secure Score: "Ensure mailbox auditing for all users is enabled".

Audit (Standard), which Business Premium includes, retains records for 180 days. Anything older exists only where you exported it, so the REVIEW table schedules a quarterly export of the admin-activity searches you care about; an incident found in month eight otherwise has no trail. The Defender portal's default alert policies (new inbox forwarding rules, admin role grants, malware campaigns) are already active; point their notifications at the role mailbox.

12 Verify with PowerShell and read the score

Read the settings back instead of trusting the screens you clicked through. The Exchange Online module covers the mail-flow half of this guide in one sitting:

```
Connect-ExchangeOnline

Get-OrganizationConfig | Format-List AuditDisabled, OAuth2ClientProfileEnabled,
  MailTipsAllTipsEnabled, MailTipsExternalRecipientsTipsEnabled,
  RejectDirectSend
Get-TransportConfig | Format-List SmtpClientAuthenticationDisabled
Get-HostedOutboundSpamFilterPolicy | Format-List Name, AutoForwardingMode,
  NotifyOutboundSpam, BccSuspiciousOutboundMail
Get-DkimSigningConfig | Format-List Domain, Enabled
Get-ExternalInOutlook | Format-List Enabled
Get-MalwareFilterPolicy | Format-List Name, EnableFileFilter
Get-HostedContentFilterPolicy | Format-List Name, AllowedSenderDomains
Get-TransportRule | Format-List Name, SetSCL, SenderDomainIs
```

The result you want: `AuditDisabled: False`, `SmtpClientAuthenticationDisabled: True`, `RejectDirectSend: True`, `AutoForwardingMode: Off`, both outbound-spam notify fields `True`, DKIM `Enabled: True` on every custom domain, the file filter on, empty allowed-domain lists, and no transport rules. Save the output with the date in the filename, and repeat the run quarterly; comparing two dated outputs is the drift check.

Then return to Secure Score at `security.microsoft.com/securescore` after a week. Confirm the actions named through this guide report complete, work the remaining reachable identity and email actions in its ranked order, and record a reason on anything you decline: mark it resolved through alternative mitigation where a real control exists elsewhere, or accept the risk in your exception register where it does not. Export or screenshot the score page with its date. That snapshot and the PowerShell readback, both dated from the week the tenant was built, are what an insurer or assessor will ask you for later.

NEXT When you enroll devices: two Intune settings to set first

Device management is its own project, and two tenant-wide Intune defaults are worth setting before the first device enrolls, at `intune.microsoft.com` (CIS section 4, both Level 1):

- **Devices with no compliance policy are marked not compliant** (CIS 4.1): under **Devices > Compliance > Compliance settings**. Otherwise an unpoliced device reports as compliant by default, and any future access rule keyed on compliance trusts it.
- **Personally owned device enrollment is blocked by default** (CIS 4.2): under **Devices > Enrollment > Device platform restriction**, set the Personally owned column to Block per platform. Bring-your-own-device then has to be set up deliberately, with mobile app management behind it.

Business Premium includes Intune and Defender for Business for the endpoint side. When you take that project on, our Remote Work & Mobile Device Policy template pairs with it.

SMALL A company of one or two

When to keep security defaults

If you do not want to build and maintain Conditional Access policies, keeping security defaults on is a defensible floor: Secure Score awards full points for its three headline actions (MFA for admins, MFA for all users, blocking legacy authentication) either way. The costs are real, though: no exclusions means your emergency accounts face the same enforcement with no carve-out, there are no session controls, and SMTP AUTH is force-disabled with no per-mailbox exception. This guide's CA route costs about an hour more, once.

The role count still works

CIS 1.1.3 asks for two to four Global Administrators, and a solo founder holds one working admin account plus the two emergency accounts from Step 2: three, inside the range, with no second human required. A solo founder has nobody else to notice that their account has been compromised, so the notification settings in Steps 5, 8, and 11 should all point at a mailbox they read.

Write the deviations down

Whatever you skip (calendar sharing stays on for a scheduling assistant, anonymous meeting join stays on for webinars), record it with the reason and a review date. An assessor reads a dated entry with a reason as a decision, and an undocumented gap as a finding. The exception register template on our resources page carries exactly those fields.

HELP What breaks, and the way back

- **A Conditional Access policy locked everyone out**

  Sign in with the excluded emergency access account from Step 2, go to **Entra ID > Conditional Access > Policies**, and switch the offending policy to report-only rather than deleting it, so its log survives the postmortem. This is why the exclusion exists, why the passkey for that account must work, and why the twice-yearly sign-in test is on the REVIEW calendar.

- **The printer or line-of-business app stopped emailing**

  That is Step 9's SMTP AUTH switch doing its job, and Step 3's legacy authentication block stops the same device too, because SMTP AUTH with a password is exactly the sign-in that policy blocks. Re-enable the protocol for that one sending mailbox with `Set-CASMailbox -Identity scanner@example.com -SmtpClientAuthenticationDisabled $false`, exclude the same account from the block-legacy-authentication policy, give the device a strong dedicated credential, and record the exception. The organization-wide switch stays off. One planning note: Microsoft's current timeline turns off username-and-password sign-in for SMTP AUTH by default at the end of December 2026, with the final removal date to be announced, so plan to move a device kept on this exception to OAuth or another sending method.

- **Someone's MFA stopped working after Step 4**

  They had only SMS registered when SMS was disabled. Before disabling weak methods on a tenant with users, read **Entra ID > Authentication methods > User registration details** and move the phone-only people to the Authenticator app first. For the one already locked out, an admin clears their methods under the user's Authentication methods pane and re-registers them.

- **A legitimate forward or share no longer works**
  Auto-forwarding to a personal mailbox and anyone-links are both off by design, for the reasons in Steps 9 and 10. The supported answers: shared mailboxes and delegation instead of forwarding rules, and Specific-people links instead of anyone-links. Grant the narrow version rather than reopening the broad setting.

- **A guest cannot open what you shared**
  Three settings in Step 10 gate them in order: sharing level (they must sign in as a guest), invite rights (an admin must have invited them), and the 30-day expiry (their access may have aged out). The Entra sign-in log shows whether the guest cleared sign-in at all; a denial after a successful sign-in points at the sharing settings.

- **Offboarding is more than deleting the account**
  Block sign-in first, then revoke sessions from the user's page in Entra so open tokens die, convert or export the mailbox and OneDrive, remove their admin roles, check for inbox rules and app passwords they created, and remove any guest accounts they sponsored. Removing the license alone does none of this.

REVIEW The checks that need a recurring look

These cannot be finished in the setup sitting. They are the recurring checks that keep the baseline accurate as the tenant fills up. Put them on a calendar now and name an owner for each.

WHAT TO REVIEW	WHERE	HOW OFTEN	CIS
Secure Score movement and new actions	security.microsoft.com/securescore	Monthly. Microsoft adds actions continually, so a falling percentage usually means the denominator grew.	beyond CIS
Emergency access account sign-ins	Entra sign-in logs, filtered to the two accounts	Monthly, plus the twice-yearly sign-in test. Any sign-in outside a test is an incident. The benchmark's automated version of this alert needs Defender for Cloud Apps; on this license the log review is the control.	2.2.1
Global Administrator count and role sprawl	admin.microsoft.com > Users > Active users, filtered to admins	Quarterly: still two to four, still separate accounts, still no licenses they do not need.	1.1.3
Guest inventory	Entra ID > Users, filtered to guests	Quarterly. The 30-day expiry handles files; this catches guests in Teams and groups that no active project explains.	5.1.6.3
DMARC aggregate reports	The rua mailbox from Step 7, or a report-digesting service	Weekly until the policy reaches p=reject, then monthly.	2.1.10
Consent requests and enterprise app inventory	Entra ID > Enterprise apps	Monthly: decide pending requests, and confirm each installed app still has a user and a reason.	5.1.5.2
Transport rules and anti-spam allow lists	The Step 12 readback	Quarterly: both still empty, or every entry explained.	6.2.2, 2.1.14
Audit log export	purview.microsoft.com > Audit, export to CSV	Quarterly, into your evidence store. Audit (Standard) keeps 180 days; your exports are the memory beyond that.	3.1.1

WHAT TO REVIEW	WHERE	HOW OFTEN	CIS
Quarantine and Defender email reports	security.microsoft.com > Email & collaboration	Weekly at first: false positives caught early keep users from asking for allow-list entries later.	beyond CIS
Configuration drift	The Step 12 readback, diffed against the baseline file	Quarterly. Step 12's commands are already written; the check is whether the new output still matches.	beyond CIS

EXCEPT Recommendations that need a higher license

These benchmark recommendations need licensing this plan does not include. Log them as accepted gaps with the license as the reason, and revisit if the tenant ever grows into E5 territory.

- **Risk-based Conditional Access** (5.2.2.6 through 5.2.2.8): Entra ID Protection's user-risk and sign-in-risk policies need Entra ID P2. Steps 3 and 4 are the compensating layer.
- **Just-in-time admin roles and access reviews** (5.3.1 through 5.3.5): Privileged Identity Management and automated access reviews need Entra ID P2. The quarterly role and guest reviews in REVIEW are the manual substitute.
- **Priority account protection and automated investigation** (2.4.1, 2.4.2, 2.4.5): Defender for Office 365 Plan 2. The Standard preset's impersonation lists in Step 8 cover the same people within Plan 1.
- **Safe Documents** (part of 2.1.5): the two Safe Documents toggles need an E5-level security license; the SharePoint, OneDrive, and Teams protection itself is on.
- **Customer lockbox** (1.3.6) and **audit retention beyond 180 days**: E5 and Audit (Premium) respectively. The quarterly export in REVIEW is the affordable answer to the second.

LIMITS What this setup does not protect against

- **A compromised endpoint.** Everything here governs the cloud side. A keylogged laptop signs in with valid MFA, which is why the device work in NEXT is the follow-on project.
- **A user who approves the wrong thing.** The consent workflow moves app grants to an admin, which makes that admin the target. Read consent requests as skeptically as you read invoices with changed bank details.
- **An insider with legitimate access.** The audit trail investigates them after the fact; the sharing defaults limit what can leave casually. Neither prevents deliberate exfiltration by someone doing their job's normal actions.
- **Data loss and retention.** Deleted mail and files follow recycle-bin rules, and the audit log records what happened without preserving the data itself. Retention policies, data loss prevention, and backup are the Purview and continuity projects; our BC/DR plan template holds that side.
- **Losing the tenant itself.** Billing lapses, a domain expiry, or the registrar account being compromised all sit outside Microsoft 365. Keep the registrar and DNS host on the vendor register with MFA of their own, and keep the emergency credentials where a fire at one site cannot take both copies.

DONE What you achieved

- A tenant where two to four cloud-only, minimally licensed admin accounts hold the privileged roles, two tested emergency access accounts stand behind them, and every sign-in faces MFA with legacy protocols and weak methods shut off.
- App access that flows through an admin: no user consent, no user app registrations, no store sprawl, no user-created tenants.
- Email that proves its origin (SPF, DKIM, DMARC on every domain including the parked ones), detonates attachments and rewrites links before users see them, quarantines impersonation, and cannot silently forward itself out or accept old-protocol sign-ins.

- Sharing that works through named, signed-in, expiring guests, with meeting lobbies and consumer-account chat closed.
- An audit trail confirmed to be recording with extended mailbox actions, alert policies pointed at a mailbox someone reads, and a dated PowerShell baseline plus a Secure Score snapshot filed as evidence.

Where that leaves you against the benchmark and the score

THE LINE TO PUT IN FRONT OF AN ASSESSOR OR INSURER

Sixty of the benchmark's 160 recommendations are addressed: the tenant-wide identity, email, sharing, and audit baseline, the Defender for Office 365 email controls its E5 profile carries, and the two Intune defaults in NEXT. The rest of the distance is scoped work this guide deliberately left out (Purview, Intune, Fabric, and the deeper per-workload hardening in each admin center) or licensing listed in EXCEPT. Three items stay conditional until you close them: DMARC is enforcing only after you move it past p=none, the mailbox audit action script needs rerunning as mailboxes appear, and the report-only CA policies count only once switched on. Write those, the EXCEPT list, and your deliberate deviations into the exception register, dated.

REF References

CIS Microsoft 365 Foundations Benchmark v7.0.0, 20 May 2026 · cisecurity.org/cis-benchmarks

Microsoft Secure Score, how scoring works, and what's new in its recommended actions · learn.microsoft.com/defender-xdr/microsoft-secure-score

Security defaults in Microsoft Entra ID · learn.microsoft.com/entra/fundamentals/security-defaults

Emergency access account recommendations · learn.microsoft.com/entra/identity/role-based-access-control/security-emergency-access

Conditional Access policies and templates · learn.microsoft.com/entra/identity/conditional-access

Defender for Office 365 Plan 1 and Plan 2 capabilities · learn.microsoft.com/defender-office-365/mdo-about

Preset security policies, their settings, and policy precedence · learn.microsoft.com/defender-office-365/preset-security-policies

Email authentication: SPF, DKIM, and DMARC in Microsoft 365 · learn.microsoft.com/defender-office-365/email-authentication-about

Enable or disable SMTP AUTH in Exchange Online · learn.microsoft.com/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission

Microsoft Purview auditing solutions and retention · learn.microsoft.com/purview/audit-solutions-overview

SharePoint and OneDrive external sharing settings · learn.microsoft.com/sharepoint/turn-external-sharing-on-or-off

Microsoft 365 Business Premium overview · learn.microsoft.com/microsoft-365/business-premium