

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

General educational guidance, not affiliated with or endorsed by the Center for Internet Security or Microsoft. Recommendation numbers refer to the CIS Microsoft 365 Foundations Benchmark v7.0.0 (20 May 2026). Published 2026-10-02.

12 steps, tenant to verification

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

80 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 80 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, sold for up to 300 users. 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 also has a limit: 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.

Which steps have to come first

Auditing comes first: Microsoft leaves it off on a new Business Premium tenant, and nothing done before it is on reaches the audit log, so Step 1 starts there. 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 accounts are the way back in. In email, SPF and DKIM must be publishing before DMARC moves to an enforcing policy, so Step 7 stages the records.

Apply the settings while the tenant is empty

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 reports your total as a percentage of the points available. 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, and says so where that action needs a license this plan does not include.

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 through alternate mitigation instead of leaving it open.

Some actions you cannot complete, and some you will not see

Secure Score shows every recommended action for a product you are licensed for, whatever edition you hold, so expect a list that includes actions needing E5. Those stay open, and EXCEPT is where you record why. Separately, a batch of its CIS-worded actions appears only once Microsoft Defender for Cloud Apps is connected, which Business Premium does not include. The settings behind those still apply and this guide still sets them; you just will not see them credited in the portal.

What score to aim for

Few organizations reach 100%, and on this plan some actions cannot be closed at all: the list includes actions that need a higher license, actions whose business cost you may decline, and new actions Microsoft adds over time. Work toward it anyway. The 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.

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 hardware security keys** for the emergency access accounts in Step 2, and the Microsoft Authenticator app on each admin's phone, for multifactor authentication (MFA: a second proof of identity at sign-in, beyond the password). Decide who will hold the emergency credentials.
- The **names of your admins**. Decide now who holds an admin account and which everyday account each of them keeps separate from it. Plan on one or two people holding Global Administrator: the two emergency access accounts in Step 2 count toward the benchmark's maximum of four.
- 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 the week or two Step 7 spends at **p=none** before DMARC moves to enforcement.

The twelve steps at a glance

Step 7 waits a week or two for DMARC reports, which spreads this work over more than one sitting for most people. 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 Turn on auditing, then create the admin accounts	purview.microsoft.com, admin.microsoft.com	none
02 Create two emergency access accounts	admin.microsoft.com, entra.microsoft.com	none
03 Move to Conditional Access	entra.microsoft.com	none on an empty tenant; a week in report-only on a tenant with users
04 Harden how people authenticate	entra.microsoft.com, admin.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, admin.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, PowerShell	none

STEP	WHERE	BUILT-IN WAIT
12 Verify with PowerShell, read the score	PowerShell, security.microsoft.com	judge the score after a week

01 Turn on auditing, then create the admin accounts

The first account in the tenant is a Global Administrator, the role that can change anything. Use it first to turn on the audit log, then set up the admin accounts the way the benchmark's opening section asks.

Turn on the audit log before anything else (CIS 3.1.1)

Microsoft leaves auditing off on a new Business Premium tenant. Open Microsoft Purview at purview.microsoft.com, go to the **Audit** solution, and select **Start recording user and admin activity**. Recording can take up to an hour to begin, and nothing done before then reaches the audit log; Entra's own sign-in and audit logs keep that period for 30 days. Step 11 confirms it is on.

Admin accounts are separate, and cloud-only (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 recommendation itself is that admin accounts are 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 administrator is a single point of failure, and every account past four is another account an attacker can take over. 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 narrower roles for routine work: Exchange Administrator and SharePoint Administrator each cover one service, and User Administrator covers accounts and groups.

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 never receives the phishing mail. Leave admin accounts unlicensed, or license each one only for Microsoft Entra ID P1, a separate purchase that carries no apps, and let the person's everyday account hold the Office apps. It also keeps admin account credentials out of any mailbox, so no inbox rule can forward them. Either choice meets the benchmark, whose recommended state is to leave a privileged account unlicensed or give it a license with no apps, such as Entra ID P1 or P2.

Secure Score's matching action, "Ensure Administrative accounts are separate, unassigned, and cloud-only", is one of those that need Defender for Cloud Apps, so it will not show on this plan. Related actions covering MFA for these accounts arrive with Step 3 and do show.

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](https://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.

- **Both accounts in one role-assignable security group** named `EmergencyAccess`, with no owners. Create it at `entra.microsoft.com` under **Entra ID > Groups > All groups > New group**, with **Microsoft Entra roles can be assigned to the group** set to Yes, a choice Entra offers only when the group is created. Only a Global Administrator or Privileged Role Administrator can then change its members. An ordinary group can be edited by several lesser admin roles, User Administrator among them, and anyone they add escapes every Conditional Access policy (CIS 1.1.2 warns about this).
- **Excluded from every Conditional Access policy** from Step 3 onward, through that group. Add the group to each new policy's exclusions as you create it; replacing an emergency account then means changing the group's members once.

These accounts need phishing-resistant MFA too

MICROSOFT'S MANDATORY MFA FOR ITS ADMIN PORTALS, ROLLED OUT FROM OCTOBER 2024 AND FEBRUARY 2025, HAS NO EXCEPTION FOR BREAK-GLASS ACCOUNTS

Both the benchmark and Microsoft say to register a passkey (FIDO2: a credential that signs you in without a password and resists phishing by design) or certificate-based authentication. Use a hardware security key for each account and store it in the safe with that account's password. A passkey in the Authenticator app sits on someone's phone and a synced one in a personal cloud account, and Microsoft says not to connect these accounts to any employee-supplied device. Microsoft also asks that they use a different method from your everyday admin accounts, and that the credential never expire or fall into a cleanup for lack of use.

A Temporary Access Pass lets you register the keys without registering a phone first. Turn on the Passkey (FIDO2) and Temporary Access Pass methods; both are rows in Step 4. Then, for each account, open **Entra ID > Users**, select the account, choose **Authentication methods > Add authentication method**, and add a Temporary Access Pass. Sign in with that pass at `mysignins.microsoft.com/security-info` and register the key. Registering it asks you to set a PIN on the key if it has none; store the PIN with that account's password, because signing in with the key asks for it.

Sign in with both accounts before you leave this step

AND AGAIN EVERY QUARTER

Test each account before Step 3, while a failed sign-in still costs nothing: sign in with its key and open the Entra admin center. Repeat the test every quarter and whenever someone with access to the safe leaves. REVIEW's monthly log check treats any other sign-in as an incident (CIS 2.2.1).

03 Move from security defaults to Conditional Access

A new tenant arrives with security defaults on. That fixed bundle requires everyone to register for MFA, requires MFA for admins, prompts everyone else for MFA when Microsoft judges it necessary, requires MFA to reach the Azure portal and the other Azure Resource Manager tools, and blocks legacy authentication. On every tenant created since 1 July 2026 it also blocks device code sign-in. Microsoft holds that enforcement for the first 24 hours after a tenant is created, so you can provision it before MFA is required.

Those protections are sound, and they apply to every account you will have, with no exclusions available to you, so your emergency access 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 seven policies under **Entra ID > Conditional Access > Policies**. Between those two actions the only MFA the tenant enforces is Microsoft's mandatory MFA for its admin portals and Azure management tools, so do both in one sitting.

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 the EmergencyAccess group.	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 the EmergencyAccess group.	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 the EmergencyAccess group.	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 the EmergencyAccess group.	5.2.2.4	Ensure Sign-in frequency is enabled and browser sessions aren't persistent for Administrative users. Needs Defender for Cloud Apps, so it will not show on this plan.
Block device code flow	Include all users; target all resources; under Conditions > Authentication flows select Device code flow; block access. Exclude the EmergencyAccess group.	5.2.2.12	None. Security defaults was blocking this flow before you turned it off, so build the policy in the same sitting rather than later.
Block authentication transfer	Include all users; target all resources; under Conditions > Authentication flows select Authentication transfer; block access. Exclude the EmergencyAccess group.	5.2.2.17	None. Authentication transfer carries a signed-in state from one device to another, as when Outlook on the desktop shows a QR code that signs you in on your phone. Blocked, it stops a stolen device token being replayed elsewhere; people sign in to mobile apps the ordinary way instead.
Everyone reauthenticates	Include all users; target all resources; grant with MFA; under Session check Sign-in frequency and set Periodic reauthentication to 7 days or less. Exclude the EmergencyAccess group.	5.2.2.13	None. Without it Entra's default is a rolling 90-day window, so a session that keeps being used never has to sign in again, and neither does someone holding a stolen token. The admin policy above sets a tighter 4 hours for privileged roles.

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. The benchmark has one more policy for those same roles, at Level 2: require the Phishing-resistant MFA authentication strength rather than any second factor (CIS 5.2.2.5). Business Premium can enforce it, but build it as its own policy: Microsoft describes the similar Baseline security mode setting in Step 4 as protecting the Microsoft admin portals, and the benchmark asks for all resources. Take it once every admin

holds a passkey, including one stored in the Authenticator app, because it locks out any admin whose only method is an Authenticator approval or code.

On an empty tenant, switch all seven On now

REPORT-ONLY IS FOR A TENANT THAT ALREADY HAS PEOPLE IN IT

Report-only mode evaluates every sign-in against a policy and logs what would have happened, without enforcing. On the empty tenant this guide assumes it protects nobody, and every day the policies spend there is a day the tenant enforces less than security defaults did before you turned them off. So finish the Step 2 sign-in test, confirm the EmergencyAccess exclusion is on each policy, and create all seven On. Nobody is signed in yet, so nothing breaks. A tenant that already has people is the case report-only is for: there, 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. Either way, never remove the EmergencyAccess exclusion from a policy to tidy up. Without it, a policy that locks the admins out leaves a Microsoft support case as the only way back into your own tenant.

Microsoft adds policies of its own, and they do not exclude your emergency accounts

CHECK THE CONDITIONAL ACCESS LIST AGAIN A MONTH AFTER YOU TURN SECURITY DEFAULTS OFF

With security defaults off and Entra ID P1 in the plan, Microsoft creates its own Conditional Access policies in your tenant, in report-only, and turns each one on no less than 30 days after it appears unless you set it to Off. Microsoft emails you and posts to the message center two weeks before it turns one on, and says there and in the policy's details when one will come on sooner, so watch for those as well as the calendar check. They cover ground your seven policies already cover. Open **Entra ID > Conditional Access > Policies**, find every row whose **Created by** column reads Microsoft, and exclude the **EmergencyAccess** group from each one. You cannot rename or delete them, but you can set the state and the exclusions, and REVIEW puts that check on a monthly calendar.

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 the password rules that sit in the same blade and one that lives in the Microsoft 365 admin center.

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.
Passkey (FIDO2)	Enabled and targeted at all users, with Allow self-service set up: Yes	beyond CIS	Under Policies > Passkey (FIDO2). While it is off, nobody can register a passkey, the Step 2 accounts included. Since 1 September 2026 Microsoft has been turning it on automatically for people who can use SMS or voice codes, in a passkey profile that allows every type of passkey, synced ones included, so check its state and its profile first. With Allow self-service set up on No, people cannot register a passkey from their Security info page. Entra also wants MFA within the last five minutes before someone adds one; a Temporary Access Pass sign-in meets that. Opting into passkey profiles, where you choose device-bound passkeys only or synced ones as well, cannot be undone, and a device-bound-only profile is enforceable only with attestation turned on. With no profile and attestation off, synced passkeys are allowed.

SETTING	SET IT TO	CIS	WHY
Temporary Access Pass	Enabled, all users	beyond CIS	Under Policies. An admin issues a time-limited pass, an hour by default, that lets the person sign in and register a passkey. It is how the Step 2 accounts get their keys without a phone, and how anyone locked out of MFA gets back in (see HELP).
Microsoft Authenticator	Enabled for all users; Show app name and geographic location: both Enabled, all users	5.2.3.1	Under Policies > Microsoft Authenticator: switch the method on for all users on the Enable and target tab, then set both options on the Configure tab. 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.
Authenticator on companion applications	Disabled	5.2.3.10	Same Microsoft Authenticator pane, and on by default. The cut-down Authenticator built into Outlook mobile, which Microsoft calls Authenticator Lite, shows neither the app name nor the city whatever you set in the row above, so leaving it on undoes that protection for anyone who approves prompts there. On a tenant with people, check who has registered it before you switch it off: anyone whose only method is the cut-down version has to install the full app to sign in again.
System-preferred MFA	Microsoft managed, all users (the default)	5.2.3.6	Under Settings. Sign-in offers the strongest method the person has registered instead of the default they chose. Microsoft managed applies that at both sign-in steps, so someone with a passkey is offered it before the password; Enabled, the value the benchmark audits for, now applies it only at the second step. Keep the default and record 5.2.3.6 as a deliberate deviation.
SMS and Voice call	Off	5.2.3.5	Under Policies. Phone-based codes fall to SIM swaps and phishing relays, and Microsoft retires its own SMS and voice codes on 1 February 2027 (1 July 2027 for Global Administrators and external users). Check who has only a phone registered before flipping this on a live tenant; see HELP.
Email OTP	Off, after Allow external users to use email OTP: No	5.2.3.7	Under Policies > Email OTP. A one-time passcode (OTP) sent to email is only as strong as that mailbox. Level 2. Entra will not switch the method off while the Allow external users to use email OTP setting on its Configure tab is Yes, so set that to No first. That setting is what lets a guest sign in with a code sent to their address, so once it is off, a guest with no Microsoft or work account is asked to create a personal Microsoft account before they can accept your invitation. Decide before you flip it whether the people you will share with in Step 10 will do that.
Authentication methods migration	Migration Complete	beyond CIS	Under Policies > Manage migration, once the rows above are set, Microsoft Authenticator among them. After the switch Entra reads only this table, so a method switched on only in the legacy MFA or password reset policy stops working. Until then Entra also honors those legacy policies, which Microsoft no longer lets you edit, so a method switched off in this table can stay usable through them.

SETTING	SET IT TO	CIS	WHY
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. Already the default; confirm it. Forced rotation produces predictable increments; both CIS and Microsoft now recommend expiry off, with strength coming from MFA and the banned list.
Lockout threshold and duration	10 or less, and 60 seconds or more	5.2.3.8, 5.2.3.9	Same Password protection pane as the banned list above. The defaults, 10 and 60, already pass; confirm them. The threshold is how many failed sign-ins Entra allows before the first lockout, and the duration is how long that first lockout lasts; later lockouts run longer. Both defend against password spraying.

Baseline security mode, in the same Org settings pane

[MICROSOFT 365 ADMIN CENTER > SETTINGS > ORG SETTINGS > SECURITY & PRIVACY, ON EVERY PLAN](#)

Microsoft groups a set of recommended settings under **Baseline Security Mode**, in the same pane you just opened for password expiration. Several overlap with work you do by hand here: blocking legacy authentication, restricting which apps users may consent to, and requiring phishing-resistant sign-in for admins. Come back to this after Step 6, so you can see what you already covered and what it adds.

Two of the settings write Conditional Access policies, which show in your policy list with **Baseline security mode** in the Created by column and are turned on and off from this pane rather than from Entra. Open each one in Entra after you turn it on and check that the **EmergencyAccess** group is excluded. The phishing-resistant one locks out any admin whose only method is an Authenticator approval or code, so hold it until every admin has a passkey.

Microsoft's advice is to run each setting's impact report and turn on the ones reporting zero impact, but on an empty tenant every report reads zero, so judge each setting by what it does. Leave the consent setting off: it lets users consent to apps from your own tenant or Microsoft's certified list that ask only for low-risk permissions, which is looser than the Do not allow user consent you set in Step 6.

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 [mysignins.microsoft.com/security-info](#), where one combined prompt covers MFA and password reset. A passkey cannot reset a password: the methods that can are the Authenticator app, OATH tokens, security questions, and the SMS, voice, and email codes Step 4 turns off. With those three off, test a two-method reset on a spare account before you rely on it; if it cannot be met, set one method and record 5.2.4.2 as a deviation.

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 eleven settings move every such grant through an admin, close the neighbouring things a user can create without one, and put a life on the credentials an app holds.

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 the workflow, people blocked from consenting go looking for tools outside the tenant. Secure Score: "Ensure the admin consent workflow is enabled", another of the actions that needs Defender for Cloud Apps and will not show on this plan.
Restrict max password lifetime	On, 180 days or less, applied to all applications	5.1.5.4	Same Enterprise apps blade, under Security > Application policies. An app signs in with a client secret, and a secret created with no expiry is a password nobody rotates and nobody sees, still working years after it leaked into a build log. Off by default.
Block custom passwords	On, applied to all applications	5.1.5.5	Same Application policies list. Entra generates the secret instead of accepting a value someone typed, so an app credential cannot be a short or reused human password.
Restrict max certificate lifetime	On, 180 days or less, applied to all applications	5.1.5.6	Same list, the certificate half of the same rule. Set both or the limit covers only one kind of credential. All three bind credentials created from now on and leave existing ones alone, so a new tenant is the place to set them.
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. Otherwise any user can create a new tenant and become its Global Administrator, and the new tenant starts with none of this one's settings.
Restrict access to the Entra admin center	Yes	5.1.2.4	Same blade, under Administration center. It stops non-admins loading a set of frequently visited admin center pages, such as home, the tenant overview, and the users list; most other pages stay reachable by direct link. Microsoft says it is not a security measure: PowerShell and the Graph API still answer, so it only discourages casual browsing.
Users can create security groups	No	5.1.3.1	entra.microsoft.com > Entra ID > Groups > General, the setting Users can create security groups in Azure portals, API or PowerShell. A group anyone can create is a group anyone can use to grant access, and its creator owns it and decides who is in it.
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".

SETTING	SET IT TO	CIS	WHERE
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`, which tells receivers to fail anything else. Microsoft recommends that hard fail for Microsoft 365 domains, so DMARC can still act on mail that fails SPF and carries no DKIM signature. A receiver that checks SPF before DMARC can reject a hard-fail message during the SMTP conversation. RFC 9989 section 7.1 warns that this can reject a message that would otherwise pass DMARC on an aligned DKIM signature, which is how forwarded mail usually passes, and that a message rejected that early never reaches the DATA phase, so it never appears in your aggregate reports. If you would rather see every sender first, publish `~all` for the weeks you spend at `p=none` and change it to `-all` before you move to enforcement.

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`. 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. A clean report is one where every source sending as your domain passes SPF or DKIM. Where one fails and you recognize it, a newsletter tool or a booking system, there are two fixes: add that sender's include to your SPF record, or have them sign with a DKIM key you publish for them. Where you do not recognize it, that is the spoofing the record exists to stop, and it needs no fix. If the reports go to a service rather than a mailbox on your own domain, that service's domain has to publish an authorization record before any receiver will send them: a TXT record at `example.com._report._dmarc` in the service's zone, with the value `v=DMARC1;`. Without it the reports never arrive, and nothing tells you they are missing.

4. DMARC, moving to enforcement

Before you publish `p=reject`, decide whether your people might post to public mailing lists from the company domain. RFC 9989 section 7.4 says a domain hosting users who might post to a list should not publish `p=reject`. A list resends each message from its own server, so SPF fails, and DKIM fails too wherever the list edits the message. The subscriber's mail system then rejects it, and the list software reads the rejection as a dead address and unsubscribes them. A domain that publishes reject anyway should have a rule that those people do not post to lists, or tell them their list participation may be hindered. If they might post, stay at `p=quarantine`.

If such a domain still wants `p=reject`, the same section asks for at least a month at `p=none`, then the same period at `p=quarantine`, comparing the reports. For a domain whose people will not post to lists, how long to wait

depends on the tenant, because the reports can only show mail that is already being sent:

- On the empty tenant this guide assumes you wrote the sender list yourself, so a week or two of clean reports tells you what a month would, and going straight to `v=DMARC1; p=reject; rua=mailto:dmARC-reports@example.com` costs you nothing on the sender side.
- On a tenant that already sends mail, give it the same soak the RFC asks of list-posting domains: a month at `p=none`, then a month at `v=DMARC1; p=quarantine; rua=mailto:dmARC-reports@example.com`, reading the reports at each step.

Microsoft's examples still add `pct=100`; RFC 9989 replaced RFC 7489 in May 2026 and removed the `pct` tag, which always defaulted to 100, so leave it out. It added `t=y` as a partial replacement, which asks receivers to apply one level below what you publish, so `p=reject; t=y` is treated as quarantine while the reports keep arriving; a receiver still following RFC 7489 ignores the tag and applies reject. Microsoft's own rollout goes through `p=quarantine` on the way.

CIS 2.1.10 also asks for a `ruf=` address for per-message failure reports. Leave it out and record 2.1.10 as a deliberate deviation: few receivers send those reports, Microsoft 365 is not one of them, and the ones that do can include message headers and body.

5. The domains that send nothing

Parked domains and the default `.onmicrosoft.com` domain are spoofing targets because nobody watches the mail sent in their name. 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 SPF record, which you cannot change; add its DMARC record 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. Every mailbox already gets basic Safe Links and Safe Attachments through the Built-in protection preset, which Microsoft applies to all recipients by default. Standard protection replaces it for everyone it covers and sets the values the benchmark audits.

Assign the Standard preset security policy

ONE WIZARD COVERS CIS 2.1.1 AND 2.1.4, AND MOST OF 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, which holds up to 350. Your own domains get impersonation protection automatically, so the domains page is where you add a partner or supplier domain someone might be impersonated from, up to 50 of them.

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: none of the protection values can be edited, and the impersonation lists and the recipients it applies to are the only things the wizard lets you set. That saves a small business from maintaining its own. 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.

One setting falls short of the benchmark. CIS 2.1.7 asks for a message that mailbox intelligence flags as impersonation to be quarantined; Standard moves it to the Junk Email folder instead, and only Strict quarantines it. You have three ways out:

- Assign Strict rather than Standard and accept its heavier hand on bulk and spam.
- Build a custom anti-phishing policy from the benchmark's own values.
- Record 2.1.7 as partly met in your exception register with the Junk Email outcome as the reason.

The rest of 2.1.7 is covered either way.

Four settings the preset does not close for you:

- **Common attachment types filter** (CIS 2.1.2): the benchmark audits the **default Anti-malware policy** specifically, so open that one and confirm the filter is on, as it is by default. Any message carrying a listed file type, executables and installers among them, is rejected with a bounce to the sender and never gets a malware verdict, so the recipient never sees it. Keep Microsoft's default list.
- **Admin notification for internal senders** (CIS 2.1.3): in the same policy, turn on the admin notification for undelivered mail from internal senders and point it at the role mailbox, so a staff member whose machine is sending malware surfaces as an alert rather than as a confused phone call. It fires when Defender finds malware in an attachment; the filter above rejects without a malware verdict, so those rejections do not trigger it. The notification is off in the preset and cannot be turned on there, and the preset outranks the default policy for everyone it covers, so setting it on the default policy reaches the mail your staff send outside the organization and leaves mail between colleagues uncovered. Record that limit in your exception register.
- **Safe Attachments for SharePoint, OneDrive, and Teams** (CIS 2.1.5): under **Safe Attachments > Global settings**, confirm it is on, as it is by default. It does not scan every file; it scans in the background, prompted by sharing and guest activity, and blocks opening, moving, copying, and sharing a malicious file it finds. It still allows the download, so run `Set-SPOTenant -DisallowInfectedFileDownload $true` in SharePoint Online PowerShell to stop an infected file leaving that way too (CIS 7.3.1). Two gaps stay open either way: anyone can still delete a flagged file, and the Share option reappears under Manage access. The Safe Documents toggles on that pane need a license that includes Safe Documents, such as Microsoft 365 E5, and users on Microsoft 365 Apps for enterprise, where this plan includes Apps for business; 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; that copy is how you learn one of your own accounts was compromised. Microsoft is retiring the notify setting in favor of the **User restricted from sending email** alert policy, so add the role mailbox to that alert as well. While you are in the outbound policy, set the sending limits the benchmark asks for (CIS 2.1.15): 500 external recipients an hour, 1000 internal, 1000 a day, and restrict the user from sending mail once they pass one. A restricted user stays blocked until an admin removes them on the Restricted entities page in the Defender portal.

Keep every allow list empty: no allowed sender domains in anti-spam policies (CIS 2.1.14), and in the connection filter policy neither an IP allow list (CIS 2.1.12) nor the safe list (CIS 2.1.13). An entry lets that sender's mail skip spam filtering and the SPF, DKIM, and DMARC checks, and an allowed sender domain skips spoofing and phishing protection too; Microsoft still filters malware and high-confidence phishing. Since September 2022 an entry for one of your own domains applies only to mail that passes email authentication. The benchmark's expanded attachment list (CIS 2.1.11) is a Level 2 item on the same anti-malware pane, and you can take it later without redoing any of this. 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

Eight settings spread across the Defender portal, the Exchange admin center at `admin.exchange.microsoft.com`, the Microsoft 365 admin center, 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. An attacker who gets into a mailbox often sets up an inbox rule that forwards everything, and 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	In the Exchange admin center under Settings > Mail flow, confirm Turn off SMTP AUTH protocol for your organization is checked, as it is by default on tenants created since January 2020. 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 (see HELP), which beats leaving the protocol open for every mailbox.
Direct Send	Rejected	6.5.5	One command in Exchange Online PowerShell: <code>Set-OrganizationConfig -RejectDirectSend \$true</code> . 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: <code>Set-ExternalInOutlook -Enabled \$true</code> . 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. Classic Outlook for Windows needs it to connect at all, because Microsoft has switched basic authentication off. Secure Score: "Ensure modern authentication for Exchange Online is enabled".
MailTips	All tips on	6.5.2	Turn the three tips on and confirm the large-audience threshold, which is already 25 by default, in Exchange Online PowerShell: <code>Set-OrganizationConfig -MailTipsAllTipsEnabled \$true -MailTipsExternalRecipientsTipsEnabled \$true -MailTipsGroupMetricsEnabled \$true -MailTipsLargeAudienceThreshold 25</code> . The tip that flags external recipients warns people before a message goes to the wrong outside address, a common source of data incidents. Secure Score: "Ensure MailTips are enabled for end users".

SETTING	SET IT TO	CIS	WHY
Personal accounts in Outlook on the web	Off, both	6.3.2	One command in Exchange Online PowerShell: <code>\$p = Get-OwaMailboxPolicy Where-Object { \$_.IsDefault }; Set-OwaMailboxPolicy -Identity \$p.Identity -PersonalAccountsEnabled \$false -PersonalAccountCalendarsEnabled \$false</code> . Otherwise a person can pull a personal mailbox and calendar into the same window as the company one, where none of the filtering in Step 8 applies. It reaches the new Outlook for Windows and Outlook on the web. Classic Outlook for Windows, Outlook for Mac, and the Outlook mobile apps sit outside it, and so does opening a personal webmail site in a browser tab. The setting also only binds the default Outlook on the web policy, which is the only one a new tenant has.
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.

A new tenant has no shared mailboxes yet. When you create one, confirm its account shows **Sign-in blocked** in **Users > Active users**, as new shared mailboxes do by default (CIS 1.2.2). A shared mailbox is a real account with a password nobody manages, and blocking sign-in leaves it reachable only through the permissions you grant.

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. A new tenant defaults to Only people in your organization, which also passes; Specific people is the tighter of the two the benchmark accepts, and the link a user mints then reaches only the people they name. A user can still choose a broader link where the sharing level allows it; most links are created with the default.
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.

SETTING	SET IT TO	CIS	WHERE
Entra guest permissions	Guest users have limited access to properties and memberships of 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 list the directory's users, groups, and other objects. Already the default; confirm it. The tighter option, restricting guests to their own directory objects, also passes.
Who can invite guests	Only users assigned to specific admin roles	5.1.6.3	Same blade. Guest creation becomes an admin decision, and that 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 have no organization behind them, and phishers use them to reach your staff in chat. Federation with real partner tenants stays available.
Teams meetings: anonymous join	Off	8.5.1	Teams admin center > Meetings > Meeting policies > Global (Org-wide default), the toggle Anonymous users can join a meeting unverified, under Meeting join & lobby. Leave the separate org-wide Anonymous users can join a meeting switch On, as Microsoft recommends; it is retiring that switch. Unverified strangers stay out of meetings. Level 2.
Teams meetings: who can start one	Anonymous users and dial-in callers can start a meeting: Off	8.5.2	Same policy, under Meeting join & lobby. Already the default; confirm it. Microsoft applies it to a meeting whose lobby bypass is Everyone and to dial-in callers allowed to bypass the lobby. The next two rows keep both off by policy, but an organizer can change either for one meeting, and this setting then stops outsiders opening it before anyone from your side arrives.
Teams meetings: lobby bypass	People in my org	8.5.3	Same policy. External participants wait in the lobby until admitted, unless the organizer changes that meeting's options.
Teams meetings: dial-in lobby bypass	People dialing in can bypass the lobby: Off	8.5.4	Same policy, and the row above does not cover it: someone on the phone is a separate class from someone in the app. Already the default; confirm it. Organizers can change this one per meeting too.
Teams org-wide app settings	Let users install and use available apps by default: Off for third-party and for custom apps, and custom apps in preview Off	8.4.1	Teams admin center > Teams apps > Manage apps, then Actions > Org-wide app settings. Teams keeps its own app store, and third-party and custom apps are both allowed by default, so a user can install a third-party app there after Step 6 closed the same route in Entra. Allow named apps back through Manage apps as the business asks for them.

11 Confirm the audit trail is recording

Any investigation starts in the unified audit log, which holds records only from the moment auditing was turned on in Step 1. This step confirms it is recording and adds what the benchmark asks of mailbox auditing.

- **Unified audit log** (CIS 3.1.1): Step 12's readback should show `UnifiedAuditLogIngestionEnabled` as `True`, and a search in Purview's **Audit** solution covering the time since Step 1 should return the changes you made. Microsoft says new events can take several hours to become searchable, so search again later if it comes back empty. If the **Start recording user and admin activity** banner is still there, auditing is off: select it, and treat everything done so far as missing from the audit log. 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`.
- **No account bypassing the audit** (CIS 6.1.3): `AuditBypassEnabled` can be set on an account, and then nothing that account does in any mailbox is logged, however the settings above are configured. The property lives on the audit bypass association rather than on the mailbox, so `Get-Mailbox` never returns it and a check written that way passes on every tenant; Step 12's readback uses `Get-MailboxAuditBypassAssociation`, which is the cmdlet the benchmark audits with. A new tenant has none, and a written exception is the only reason to leave one.
- **Mailbox audit actions** (CIS 6.1.2): mailbox auditing is on by default and records most of what an investigation needs. The benchmark adds eight actions, and Microsoft's defaults now include one of them, the owner's `Create`, which leaves seven to add:
 - `Copy`, `FolderBind` and `Move` for admin actions.
 - `FolderBind` and `Move` for delegate actions.
 - `MailboxLogin` and `Move` for owner actions.

Add them in the `@{Add=...}` form below, because a plain list replaces Microsoft's defaults instead of adding to them. Either way, Microsoft stops managing the default actions for each sign-in type you change, so an action it adds later is not audited on those mailboxes; rerun the command for new mailboxes, and compare one mailbox against Microsoft's current default table each quarter. Microsoft's page on investigating compromised accounts lists `MailItemsAccessed`, the action that shows the messages a compromised account read, as on by default for E3 and E5 licenses, which Business Premium is not, so check that it appears in the lists and add it the same way if it does not.

```
Get-EXOMailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited |  
  Set-Mailbox -AuditAdmin @{Add="Copy","FolderBind","Move"} `  
    -AuditDelegate @{Add="FolderBind","Move"} -AuditOwner @{Add="MailboxLogin","Move"}  
Get-Mailbox user@example.com | Format-List AuditAdmin, AuditDelegate, AuditOwner
```

The benchmark also sets `-AuditLogAgeLimit 180`. Microsoft's mailbox auditing page now says that property no longer manages how long mailbox audit records are kept and that Purview manages retention instead, so it adds nothing to the 180 days Audit (Standard) already gives you. Secure Score: "Ensure mailbox auditing for all users is enabled".

- **Mailboxes that ignore the organization default** (CIS 6.1.2): Resource mailboxes, public folder mailboxes, and the DiscoverySearch mailbox ignore the organization default, so each of those needs `AuditEnabled` set to `True` on the mailbox itself; a room or equipment mailbox is the one a small business meets first. Microsoft's own table of supported mailbox types now lists resource and public folder mailboxes as not supporting mailbox auditing, so set what the benchmark asks for and then check that records appear before you count on them.

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 are on from the start and email Global Administrators, whose accounts here have no mailbox, so 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-AdminAuditLogConfig | Format-List UnifiedAuditLogIngestionEnabled
Get-OrganizationConfig | Format-List AuditDisabled, OAuth2ClientProfileEnabled,
    MailTipsAllTipsEnabled, MailTipsExternalRecipientsTipsEnabled,
    MailTipsGroupMetricsEnabled, MailTipsLargeAudienceThreshold,
    RejectDirectSend
Get-TransportConfig | Format-List SmtpClientAuthenticationDisabled
Get-HostedOutboundSpamFilterPolicy | Format-List Name, AutoForwardingMode,
    NotifyOutboundSpam, NotifyOutboundSpamRecipients, BccSuspiciousOutboundMail,
    BccSuspiciousOutboundAdditionalRecipients, RecipientLimitExternalPerHour,
    RecipientLimitInternalPerHour, RecipientLimitPerDay, ActionWhenThresholdReached
Get-DkimSigningConfig | Format-List Domain, Enabled
Get-ExternalInOutlook | Format-List Enabled
Get-EOPProtectionPolicyRule -Identity "Standard Preset Security Policy" |
    Format-List Name, State, SentTo, SentToMemberOf, RecipientDomainIs,
    ExceptIfSentTo, ExceptIfSentToMemberOf, ExceptIfRecipientDomainIs
Get-ATPPProtectionPolicyRule -Identity "Standard Preset Security Policy" |
    Format-List Name, State, SentTo, SentToMemberOf, RecipientDomainIs,
    ExceptIfSentTo, ExceptIfSentToMemberOf, ExceptIfRecipientDomainIs
Get-MalwareFilterPolicy | Format-List Name, EnableFileFilter,
    EnableInternalSenderAdminNotifications, InternalSenderAdminAddress
Get-AtpPolicyForO365 | Format-List EnableATPForSPOTeamsODB
Get-HostedContentFilterPolicy | Format-List Name, AllowedSenderDomains
Get-HostedConnectionFilterPolicy | Format-List Name, IPAllowList, EnableSafeList
Get-OwaMailboxPolicy | Format-List Name, PersonalAccountsEnabled, PersonalAccountCalendarsEnabled
Get-TransportRule | Format-List Name, SetSCL, SenderDomainIs, RedirectMessageTo
Get-MailboxAuditBypassAssociation -ResultSize unlimited |
    Where-Object { $_.AuditBypassEnabled } | Format-List Name, AuditBypassEnabled
```

The result you want:

- `UnifiedAuditLogIngestionEnabled: True` and `AuditDisabled: False`.
- `OAuth2ClientProfileEnabled: True`, `SmtpClientAuthenticationDisabled: True`, and `RejectDirectSend: True`.
- The three MailTips fields `True`, with the threshold at 25.
- `AutoForwardingMode: Off`; both outbound-spam switches `True`, with the role mailbox in `NotifyOutboundSpamRecipients` and in `BccSuspiciousOutboundAdditionalRecipients`; and the sending limits at the Step 8 values, with `ActionWhenThresholdReached: BlockUser`.
- Every custom domain listed with `Enabled: True`. A domain missing from the list has no DKIM keys yet.
- External sender tagging `Enabled: True`.
- Both preset rules `State: Enabled`, with every recipient and exception field empty, which Microsoft documents as a rule with no conditions or exceptions, covering everyone.
- The file filter on, and on the Default row the internal-sender notification on, with the role mailbox in `InternalSenderAdminAddress`.
- `EnableATPForSPOTeamsODB: True`.
- Empty allowed-domain and IP allow lists, and `EnableSafeList: False`.
- Both personal-account fields `False`.
- No transport rule setting an SCL, naming a sender domain, or redirecting mail to an outside address, and nothing returned by the last command.

`NotifyOutboundSpam` can read `True` while `NotifyOutboundSpamRecipients` is empty, and then that setting notifies nobody, so read the recipient fields rather than the switches beside them. `Get-MalwareFilterPolicy` returns the preset's policy beside the default one, so expect two rows: the notification fields you set show on Default and stay blank on the Standard Preset Security Policy row, whose name carries a 13-digit suffix, and which Microsoft says not to edit. 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, and work the remaining reachable identity and email actions in its ranked order. Record a reason on anything you decline: mark it resolved through alternate 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. The readback covers the mail-flow half of this guide; for the identity and sharing half, the Secure Score export and screenshots of the Conditional Access policy list and the SharePoint sharing page do the same job.

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 > Device onboarding > Enrollment > Device platform restriction**, set the Personally owned column to Block per platform. Register company devices first: with the block on, Intune also blocks enrollment of a Windows laptop that joins Entra during setup unless it is registered in Windows Autopilot, and treats an iPhone, iPad, or Mac as personal unless it is registered by serial number (an iPhone or iPad also by IMEI) or enrolled through Apple's Automated Device Enrollment. 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 choice: Secure Score awards full points for its three headline actions (MFA for admins, MFA for all users, blocking legacy authentication) either way. What you give up:

- No exclusions, so your emergency accounts face the same enforcement as everyone else.
- No session controls.
- SMTP AUTH force-disabled with no per-mailbox exception.

This guide's CA route costs about an hour more, once. Going back may not be available at all. Microsoft's wording is that creating Conditional Access policies prevents you from enabling security defaults, and the policies Microsoft adds can only be set to Off, never deleted. Whether switching every policy off is enough, or whether Entra counts a policy that merely exists, is not documented, so test it on your own tenant before you rely on it. Choose the route you mean to stay on.

The role count still works

A solo founder holds one working admin account plus the two emergency accounts from Step 2, which is three and inside the range CIS 1.1.3 asks for, with no second human required. What a solo founder does not have is anyone 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 every day.

Write the deviations down

Whatever you skip, such as keeping calendar sharing on for a scheduling assistant, record it in the exception register with the reason and a review date, so an assessor can see it was a decision.

HELP Troubleshooting and offboarding

• A Conditional Access policy locked everyone out

Sign in with either 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. If its **Created by** column reads Baseline security mode, turn that setting off in the Microsoft 365 admin center instead. If neither emergency account can sign in, the only way back in is a support case with Microsoft.

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

Step 9's SMTP AUTH switch blocks it, and so do Step 3's policies: SMTP AUTH with a password is the sign-in the legacy authentication block stops, and it cannot complete the MFA the other policies require.

1. Re-enable the protocol for that one sending mailbox with `Set-CASMailbox -Identity scanner@example.com -SmtpClientAuthenticationDisabled $false`.
2. Exclude the same account from every Conditional Access policy that blocks legacy authentication or requires MFA. In Step 3's set those are the legacy block, MFA for all users, and the reauthentication policy; check the **Created by** column for others.
3. Give the device a strong dedicated credential.
4. 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, and Microsoft has said it will announce the final removal date in the second half of 2027. On a tenant that already existed by then, an admin can still re-enable it, so an exception survives that date. That is a separate switch from the per-mailbox one above, so check Microsoft's current SMTP AUTH article when the date arrives. Microsoft says that on a tenant created after December 2026, basic authentication for SMTP AUTH is unavailable by default and OAuth is the supported method, so if you are building a tenant from that point on, plan the device onto OAuth or a connector rather than onto an exception.

• Mail we send started bouncing after p=reject

A sender you did not find in the Step 7 reports is failing both SPF and DKIM, and receivers now reject it during the SMTP conversation, so the sender sees a bounce and you see nothing in your own tenant. Drop the record back to `p=quarantine` while you fix it, then either add that sender's include to your SPF record or have them sign with a DKIM key you publish for them. The aggregate reports at the `rua` address are where you find who it was.

- **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 anyone already locked out, an admin opens the user's Authentication methods pane, issues a Temporary Access Pass, and has them register the Authenticator app with it.

- **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). Step 4 adds a fourth: with email OTP off for guests, someone with no Microsoft or work account is asked to create a personal Microsoft account, and until they do, they cannot sign in. The Entra sign-in log tells the two apart. A denial after a successful sign-in points at the sharing settings; no sign-in at all points at the method.

- **Offboarding checklist**

1. Block sign-in first.
2. Revoke sessions from the user's page in Entra, so their refresh tokens stop working.
3. Convert or export the mailbox and OneDrive.
4. Remove their admin roles.
5. Check for inbox rules they created.
6. Remove any guest accounts they sponsored.

Removing the license alone does none of this.

REVIEW Recurring checks

No sitting finishes these; they keep the baseline accurate as the tenant fills up with people, guests, and mail. 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 the total possible points can rise and drop your percentage even when nothing in the tenant changed.	beyond CIS
Emergency access account sign-ins	Entra sign-in logs, filtered to the two accounts	Monthly, plus the quarterly sign-in test from Step 2 and one after any change in who holds the credentials. 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

WHAT TO REVIEW	WHERE	HOW OFTEN	CIS
Global Administrator count and role sprawl	admin.microsoft.com > Users > Active users, filtered to admins, then Settings > Partner Relationships	Quarterly: still two to four, still separate accounts, still no licenses they do not need. Check Partner Relationships in the same pass. If you bought the subscription through a reseller, they hold admin access that never appears in Active users, and it should still be there for a reason.	1.1.3
Conditional Access policies Microsoft added	Entra ID > Conditional Access > Policies, Created by column	Monthly. Exclude the EmergencyAccess group from each of Microsoft's managed policies as it appears (Step 3).	beyond CIS
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 (Step 11).	3.1.1
Mailbox audit actions	Get-Mailbox on one mailbox, against Microsoft's default table	Quarterly, and rerun the Step 11 command whenever mailboxes are added.	6.1.2
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 you move to E5 or add one of Microsoft's add-on suites for Business Premium, which bring Entra ID P2 or Audit (Premium).

- **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, 2.4.5): 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 a license that includes them, such as Microsoft 365 E5, and Microsoft 365 Apps for enterprise, where this plan includes Apps for business; the SharePoint, OneDrive, and Teams protection itself is on.
- **Defender for Cloud Apps** (2.4.3): not in this plan.
- **Data loss prevention for Teams** (3.2.2): E5. Purview is out of scope for this guide anyway, so this belongs with the rest of that project.
- **Customer lockbox** (1.3.6) and **audit retention beyond 180 days**: E5 and Audit (Premium) respectively.

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, so 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.** Microsoft 365 keeps short recovery windows rather than a backup you control: recycle bins, deleted-item retention in Exchange, a 30-day restore in OneDrive, and SharePoint backups kept for 14 days that Microsoft support can restore a whole site from. Anything older is gone unless a retention policy or a copy of your own keeps it, and the audit log records what happened without preserving what was lost. Retention policies, data loss prevention, and a backup you control, such as Microsoft's paid Microsoft 365 Backup, are the Purview and continuity projects; our BC/DR plan template holds that side.
- **Losing the tenant itself.** A subscription that ends is disabled, with only admins able to reach its data, and then deleted; since February 2026, one bought directly from Microsoft under a Microsoft Customer Agreement no longer gets the expired stage that used to keep users working first. Keep recurring billing on, and add the role mailbox as an additional recipient for billing notifications, which otherwise go to admin accounts that have no mailbox here. A domain expiry or a compromised registrar account sits 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 with two to four Global Administrators, two of them the emergency access accounts you have signed into, and every admin account cloud-only and minimally licensed. Once the Step 3 policies are On, every other account faces MFA, passkeys are ready to register, and legacy protocols, device code sign-in, authentication transfer, the cut-down Authenticator, and weak methods are shut off.
- App access that flows through an admin: no user consent, no user app registrations, no Office Store or Teams app installs without an admin, no user-created tenants, and an expiry date on every credential an app is given.
- 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 recording since Step 1, with the benchmark's mailbox audit actions applied, no account bypassing the log, alert policies pointed at a mailbox someone reads, and a dated PowerShell baseline plus a Secure Score snapshot filed as evidence.

Benchmark and score coverage after these steps

WHAT TO SAY WHEN AN ASSESSOR OR INSURER ASKS

Eighty 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. Of the remaining 80:

- Thirteen need a license above this plan and are listed in EXCEPT.
- Thirty are Level 2 items whose business cost you may decide against.
- Thirty-seven are Level 1. Twenty-one of those are the scoped work this guide leaves out: Purview, Fabric, the Entra device settings, and the access rules that need Intune enrollment behind them. Two apply only to a tenant synchronized from a local Active Directory, so a cloud-only tenant records them as out of scope. That leaves fourteen Level 1 settings on panes these steps open: Bookings, group membership requests, MFA capability reporting, password-reset re-confirmation, Teams message reporting, zero-hour auto purge (ZAP) for Teams, the Strict preset for priority accounts, and the SharePoint and Teams panes. Several already hold the value the benchmark asks for, so a second pass through the benchmark's sections 1, 2, 5, 7 and 8 confirms some and changes the others.

Four of the 80 are partly met, and the guide says so where each one appears:

- 2.1.3: the internal-sender malware alert covers only mail leaving the organization.
- 2.1.5: Safe Documents needs a license above this plan.
- 2.1.7: the mailbox-intelligence action needs the Strict preset or a custom anti-phishing policy.
- 2.2.1: the alert is a Defender for Cloud Apps policy, so the monthly sign-in log review in REVIEW stands in for it.

Two are deliberate deviations: 2.1.10 leaves out the failure-report address, and 5.2.3.6 keeps system-preferred MFA at Microsoft managed. A third, 5.2.4.2, joins them if your Step 5 test forces one reset method. Three more stay conditional until you close them: DMARC is enforcing only after you move it past p=none, the mailbox audit additions need rerunning as mailboxes appear, and any CA policy left in report-only counts only once switched on. Write those, the EXCEPT list, and your deliberate deviations into the exception register, dated.

References

CIS Microsoft 365 Foundations Benchmark v7.0.0, 20 May 2026 · cisecurity.org/benchmark/microsoft_365

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

Plan a Conditional Access deployment, and why it does not combine with security defaults · learn.microsoft.com/entra/identity/conditional-access/plan-conditional-access

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

Role-assignable groups · learn.microsoft.com/entra/identity/role-based-access-control/groups-concept

Mandatory multifactor authentication for Azure and Microsoft admin portals · learn.microsoft.com/entra/identity/authentication/concept-mandatory-multifactor-authentication

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

Microsoft-managed Conditional Access policies, and when Microsoft turns them on · learn.microsoft.com/entra/identity/conditional-access/managed-policies

Enable passkeys (FIDO2) in Microsoft Entra ID · learn.microsoft.com/entra/identity/authentication/how-to-authentication-passkeys-fido2

Temporary Access Pass for registering passwordless methods · learn.microsoft.com/entra/identity/authentication/howto-authentication-temporary-access-pass

Moving from the legacy MFA and password reset policies to the Authentication methods policy · learn.microsoft.com/entra/identity/authentication/concept-authentication-methods-manage

System-preferred authentication and its Microsoft managed state · learn.microsoft.com/entra/identity/authentication/concept-system-preferred-authentication

Retiring SMS and voice codes · learn.microsoft.com/entra/identity/authentication/concept-sms-voice-retirement

Baseline security mode settings in the Microsoft 365 admin center · learn.microsoft.com/microsoft-365/baseline-security-mode/baseline-security-mode-settings

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

Safe Attachments for SharePoint, OneDrive, and Teams, and blocking the download of a detected file · learn.microsoft.com/defender-office-365/safe-attachments-for-spo-odfb-teams-configure

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

RFC 9989, the current DMARC specification, which replaced RFC 7489 in May 2026 · rfc-editor.org/rfc/rfc9989.html

Deprecation of Basic authentication in Exchange Online · learn.microsoft.com/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online

Updated Exchange Online SMTP AUTH Basic Authentication Deprecation Timeline · techcommunity.microsoft.com/blog/exchange/updated-exchange-online-smtp-auth-basic-authentication-deprecation-timeline/4489835

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

Turning auditing on, and its Business Premium default · learn.microsoft.com/purview/audit-log-enable-disable

Manage mailbox auditing, including the audit bypass association · learn.microsoft.com/purview/audit-mailboxes

Investigating compromised accounts with MailItemsAccessed · learn.microsoft.com/purview/audit-log-investigate-accounts

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