CICADA | RESOURCES

IDENTITY | 120 MIN | WORKING KNOWLEDGE | UPDATED NOVEMBER 2026

Lock down Microsoft 365 in an afternoon

The admin settings that matter most in Microsoft 365, and the Google Workspace equivalents.

The short version

- ✓ Enforce MFA for everyone and block legacy authentication.
- ✓ Limit Global Admins to two named accounts.
- ✓ Review external sharing, forwarding and guest access.
- ✓ Turn on alerting for suspicious sign-ins and mailbox rules.

Start with identity

- **Enforce MFA** for all users (Security Defaults, or Conditional Access if you have the licences).
- **Block legacy authentication**: old protocols that bypass MFA.
- **Limit Global Admins** to two, named, with MFA and no everyday mailbox use.
- **Turn on number matching** to stop prompt fatigue.
- **Review break-glass access**: one emergency account, long unique password, offline recovery codes, monitored.

Google Workspace equivalents: 2-Step Verification enforcement, super admin limits, security keys for admins, and less privileged admin roles.

Then email and sharing

- **External forwarding:** disable automatic forwarding to external addresses, or restrict it.

- **Mailbox rules:** alert on rules that delete or move mail; a classic sign of compromise.
- **External sharing:** decide whether files can be shared with anyone outside, or only named domains.
- **Guest access:** review who is a guest; remove stale accounts.
- **DMARC:** publish SPF and DKIM, then move DMARC to quarantine or reject.

Turn on the alarms

Enable alerts for: impossible travel, multiple failed sign-ins, new admin roles, new inbox rules, mass file downloads and MFA changes. Send them to a mailbox someone actually reads, not just the admin who set it up.

> TEST IT
>
> Sign in from a new location or device and confirm the alert arrives. An alert nobody sees is not a control.

If you're not sure

Ask your IT provider to walk through these five settings and show you the current state. If you don't have a provider, Microsoft's own security assessment and the built-in Secure Score are a reasonable starting point. Don't accept 'it's all handled' without evidence.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.

Action checklist

- [ ] MFA enforced; legacy auth blocked
- [ ] Global admins limited to two named accounts
- [ ] External forwarding restricted
- [ ] Guest and external sharing reviewed
- [ ] SPF, DKIM and DMARC published
- [ ] Alerts for suspicious sign-ins and inbox rules

0 of 6 done