CICADA | RESOURCES

LESSON 02 OF 04 · 8 MIN · WORKING KNOWLEDGE

Microsoft 365 and Google Workspace

The handful of admin settings that matter most, and how to check them without becoming an IT department.

Five settings that carry most of the weight

01 **MFA for everyone**: enforced at the tenant level.

02 **Legacy authentication blocked**: so old protocols can't bypass MFA.

03 **Admin roles limited** to named people; no shared global admin.

04 **External sharing and forwarding** set deliberately, not left at the default.

05 **Alerts** for suspicious sign-ins, new inbox rules and admin changes.

Microsoft calls the baseline “Security Defaults” or Conditional Access; Google's equivalents are 2-Step Verification enforcement and admin role controls. Either way, the principle is the same.

Google Workspace equivalents

- Enforce 2-Step Verification for all users; require security keys for admins if possible.
- Limit super admin accounts and use narrower admin roles.
- Review external sharing in Drive, and guest access.
- Set up alert centre rules for suspicious logins and data exfiltration.
- Check DMARC and email authentication in the admin console.

Don't boil the ocean

You don't need every setting on day one. Do the five above, test that alerts arrive, and write down what you changed. If a provider manages this for you, ask them to show you the current state of each setting rather than accepting “it's all handled”.

Review again when someone joins or leaves, and after any major change to how the business works.

> **ASK FOR EVIDENCE**
>
> “MFA is on” is a claim. A screenshot of the policy, or a test sign-in from a new device, is evidence. Ask for the latter.

Key takeaways

- ✓ MFA, legacy auth blocking, admin limits, sharing defaults and alerts are the core.
- ✓ Google Workspace has direct equivalents for each.
- ✓ Test that alerts actually reach someone.
- ✓ Ask your provider for evidence, not reassurance.