CLOUDSWITCHED

FREE RESOURCE — SETUP GUIDE

Microsoft 365 Admin Setup Guide

A step-by-step configuration guide for the Microsoft 365 admin centre — tenant & domain setup, MFA and Conditional Access, email security, device management, and monitoring. Use it to harden a brand-new M365 tenant on day one or to remediate an existing tenant before rolling out to users.

5	35+	Day 1	2026
SETUP SECTIONS	CONFIG CHECKS	SECURE FROM THE START	BEST PRACTICE

ENTRA ID · CONDITIONAL ACCESS · DEFENDER FOR 365 · INTUNE

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive Setup Guide

01

Tenant & Domain Setup

This guide is for IT administrators setting up a new Microsoft 365 tenant or hardening an existing one. **Follow the sections in order** — security settings should be configured before rolling out to users. Each item is an interactive checkbox you can tick directly in any modern PDF viewer.

Section 01 covers the foundational settings of your Microsoft 365 tenant: organisation profile, domain verification, DNS records, password policy, self-service password reset, and sign-in page branding.

1.1 FOUNDATIONAL TENANT CONFIGURATION

- ☐ **Organisation profile:** set company name, address, and contact details in *Settings > Org settings*.
- ☐ **Domain verification:** add and verify all company domains; set the primary domain used for email addresses.
- ☐ **DNS records:** configure MX, Autodiscover, SPF, DKIM, and DMARC for every mail-flow domain.
- ☐ **Password policy:** Microsoft now recommends *no expiration with MFA enforced*, or 90–365 days without — pick one and document it.
- ☐ **Self-service password reset (SSPR):** enable SSPR to reduce helpdesk tickets and improve user experience.
- ☐ **Company branding:** add logo and colours to the sign-in page — helps users spot phishing pages that don't match.

DEDICATED ADMIN ACCOUNTS — DO THIS FIRST

Create separate admin accounts (e.g. admin@yourdomain.com) for administrative tasks. Admin accounts must have **MFA enforced**, must **never be used for daily email or browsing**, and should be **cloud-only** — not synced from on-premises Active Directory.

02

Security Configuration

The essential identity-and-access controls every Microsoft 365 tenant should have in place before users log in. Multi-Factor Authentication is the single most effective control — Conditional Access adds the contextual rules around it.

2.1 MULTI-FACTOR AUTHENTICATION (MFA)

- Enable **Security Defaults** as a minimum — free with all plans, enforces MFA for every user.
- On Premium plans, **disable Security Defaults** and use **Conditional Access** for granular MFA control instead.
- Require MFA for **all admin accounts** with no exceptions — Global, Exchange, SharePoint, Security, and Compliance admins.
- Block **legacy authentication** protocols that cannot support MFA *(POP, IMAP, SMTP basic auth, MAPI/HTTP, Exchange ActiveSync basic).*

2.2 CONDITIONAL ACCESS (ENTRA ID P1 / P2 REQUIRED)

- **Require MFA** for all users when signing in from untrusted locations.
- **Block sign-ins** from countries where you have no employees or business operations.
- **Require compliant devices** for access to sensitive applications — needs Intune integration.
- **Block risky sign-ins** using Entra ID Identity Protection risk scoring *(P2).*
- Create a **break-glass account** excluded from Conditional Access for emergency admin access.

BREAK-GLASS ACCOUNT — LAST-RESORT ACCESS

Create **one** emergency admin account with a very strong password stored in a **physical safe**. It must be **excluded from every Conditional Access policy and MFA requirement** so you can recover if the tenant is locked out. Monitor its usage with sign-in alerts to security@yourdomain.com — any login is an incident.

03

Email & Communication Settings

Configure Defender for Office 365, Teams, and SharePoint so external collaboration is safe by default. The settings below assume you have Microsoft Defender for Office 365 (included in Business Premium and most enterprise plans).

3.1 EMAIL SECURITY (DEFENDER FOR OFFICE 365)

- **Anti-phishing policies:** enable mailbox intelligence, impersonation protection for executives, and on-message safety tips.
- **Safe Attachments:** enable *Dynamic Delivery* so attachments are scanned without delaying email.
- **Safe Links:** enable URL rewriting and time-of-click scanning for all users across Outlook, Teams, and Office apps.
- **External email tagging:** enable the [External] tag in subject lines or banners for emails from outside the tenant.

3.2 TEAMS & SHAREPOINT / ONEDRIVE SHARING

- **Teams external access:** restrict external access to specific trusted domains; disable anonymous meeting join.
- **SharePoint sharing:** set the default sharing scope to *"People in your organisation"* — never *"Anyone with the link"*.
- **OneDrive sharing:** align sharing settings with SharePoint; block external sharing by default and require authentication for guest links.

> **EXTERNAL TAG — SMALL CHANGE, BIG IMPACT**
>
> Adding the [External] banner to inbound mail is one of the cheapest, most effective phishing-resistance controls. Pair it with brief user training so people learn to slow down whenever they see the tag — this is where invoice fraud and CEO-impersonation attempts are caught.

04

User & Device Management

How you structure groups, assign licences, and enrol devices determines how quickly the tenant scales and how cleanly leavers can be off-boarded. Get this right at the start and you avoid years of accumulated technical debt.

4.1 GROUPS, NAMING, AND LICENSING

- **Groups strategy:** use *Microsoft 365 Groups* for Teams channels, *Security Groups* for access control, and *Distribution Lists* for email lists — don't mix them.
- **Naming conventions:** establish a group naming policy *(e.g. DEPT-Marketing, SG-Finance-Read)* to prevent group proliferation.
- **Licence assignment:** use *group-based licensing* to automatically assign licences based on department or role — never assign per user.

4.2 DEVICE MANAGEMENT (INTUNE)

- **Intune enrolment:** on Premium plans, configure device enrolment for company-owned and BYOD devices with separate enrolment profiles.
- **App protection policies:** require PIN or biometric to access corporate data on mobile devices; block copy-paste to personal apps.
- **Windows Autopilot:** configure for zero-touch device deployment for new starters — ship the laptop direct from the vendor.

WHY GROUP-BASED LICENSING MATTERS

When licences follow group membership, a new starter added to DEPT-Sales automatically gets E3, Defender, and Intune. A leaver removed from the group automatically releases those licences. Manually assigning licences leaves orphaned licences and missing capabilities for years — it is the #1 source of M365 cost waste in SMEs.

05

Monitoring & Reporting

You cannot manage what you cannot see. The final section sets up the visibility you need to keep the tenant healthy: audit logging, alert policies, Secure Score, usage reports, and service-health subscriptions.

5.1 VISIBILITY & AUDIT

- **Audit logging:** verify the *Unified Audit Log* is enabled (on by default for new tenants — but verify, especially for tenants created before 2023).
- **Alert policies:** configure alerts for suspicious sign-in activity, mass file deletion, eDiscovery activity, and malware detections.
- **Microsoft Secure Score:** review weekly and work through the highest-impact recommendations first.
- **Usage reports:** review monthly to identify adoption gaps and unused or under-utilised licences.
- **Service health:** subscribe to service-health notifications for early warning of Microsoft outages and advisories.

Configuration notes

PREPARED BY

DATE

APPROVED BY

CLOUDSWITCHED

MICROSOFT 365 & CLOUD PRODUCTIVITY FOR UK SMES

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom