Microsoft 365 Admin Setup Guide

Configuring the Microsoft 365 admin centre, security policies, conditional access, and organisational settings. Get your M365 tenant properly secured from day one.

5	Day 1	Best	Free
SETUP AREAS	SECURITY FROM THE START	PRACTICE CONFIGURATION	ADMIN GUIDE

Who This Guide Is For

This guide is for IT administrators setting up a new Microsoft 365 tenant or hardening an existing one. Follow these steps in order — security settings should be configured before rolling out to users.

1 Tenant & Domain Setup

Configure the foundational settings of your Microsoft 365 tenant.

- → **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 for email addresses.
- → **DNS records:** Configure all required DNS records: MX, Autodiscover, SPF, DKIM, DMARC
- → **Password expiration:** Set password policy — Microsoft now recommends no expiration with MFA, or 90–365 days without
- → **Self-service password reset:** Enable SSPR to reduce helpdesk tickets for password resets
- → **Company branding:** Add your logo and colours to the sign-in page for a professional appearance and phishing awareness

Dedicated Admin Accounts

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

2 Security Configuration

Configure the essential security settings to protect your organisation.

Multi-Factor Authentication

- Enable **Security Defaults** as a minimum (free with all plans) — enforces MFA for all users
- For Premium plans: disable Security Defaults and use **Conditional Access** for granular MFA control
- Require MFA for **all admin accounts** with no exceptions
- Block **legacy authentication** protocols that cannot support MFA (POP, IMAP, SMTP basic auth)

Conditional Access (Premium Only)

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

Break-Glass Account

Create one emergency admin account with a very strong password stored in a physical safe. This account must be excluded from all Conditional Access policies and MFA requirements. It is your last resort if all admin accounts are locked out. Monitor its usage with alerts.

3 Email & Communication Settings

Configure email security, Teams, and SharePoint for your organisation.

- → **Anti-phishing policies:** Enable mailbox intelligence, impersonation protection for executives, and safety tips
- → **Safe Attachments:** Enable Dynamic Delivery to scan attachments without delaying email
- → **Safe Links:** Enable URL rewriting and time-of-click scanning for all users
- → **External email tagging:** Enable the '[External]' tag in subject lines or banners for emails from outside
- → **Teams external access:** Restrict external access to specific trusted domains, disable anonymous meeting join
- → **SharePoint sharing:** Set default sharing to 'People in your organisation', not 'Anyone with the link'
- → **OneDrive sharing:** Align sharing settings with SharePoint. Block external sharing by default.

4 User & Device Management

Set up user provisioning, group management, and device policies.

- → **Groups strategy:** Use Microsoft 365 Groups for Teams channels, Security Groups for access control, Distribution Groups for email lists
- → **Naming conventions:** Establish a group naming policy to prevent proliferation of poorly named groups
- → **Licence assignment:** Use group-based licensing to automatically assign licences based on department or role
- → **Intune enrolment:** For Premium plans, configure device enrolment for company and BYOD devices
- → **App protection policies:** Require PIN/biometric to access corporate data on mobile devices
- → **Windows Autopilot:** Configure for zero-touch device deployment for new starters

5 Monitoring & Reporting

Set up monitoring to maintain visibility over your Microsoft 365 environment.

- → **Audit logging:** Verify Unified Audit Log is enabled (it is on by default but verify)
- → **Alert policies:** Configure alerts for suspicious sign-in activity, mass file deletion, and malware detection
- → **Secure Score:** Review Microsoft Secure Score weekly and work through recommendations
- → **Usage reports:** Review monthly usage reports to identify adoption gaps and unused licences
- → **Service health:** Subscribe to service health notifications for early warning of Microsoft outages

Notes

Prepared by: Date: Approved by: