

FREE COMMUNITY ASSET

Microsoft 365 & Entra ID Security Defaults Checklist

Immediate baseline defense protocol to lock down all tenant accounts, block legacy protocols, and require MFA without licensing upgrades.

1.0 EXECUTIVE SUMMARY: ZERO-COST TENANT PROTECTION

Microsoft Security Defaults is a pre-configured security posture switch designed for organizations that want baseline identity protection without purchasing premium Entra ID P1 or P2 licenses. Enabling this single setting eliminates the primary entry vectors used in over 80% of business email compromise (BEC) incidents.

2.0 THE 5 MANDATORY POLICIES ENFORCED BY SECURITY DEFAULTS

- * **1. Tenant-Wide MFA Registration:** All users have 14 days to register for MFA via Microsoft Authenticator from their first sign-in.
- * **2. Mandatory Admin MFA:** Every account with administrator roles (Global Admin, Privileged Role Admin, Security Admin) MUST use MFA on EVERY sign-in.
- * **3. Challenging High-Risk Sign-ins:** Standard users are prompted for MFA whenever login anomalies, unfamiliar locations, or atypical devices are detected.
- * **4. Complete Block of Legacy Authentication:** Older mail clients using POP3, IMAP, SMTP, or legacy ActiveSync that cannot process modern MFA dialogs are strictly blocked.
- * **5. Protected Management Access:** Accessing the Azure Portal, Microsoft 365 Admin Center, Exchange Admin Center, or Azure PowerShell requires mandatory MFA.

LEGACY AUTHENTICATION WARNING

Legacy protocols (POP/IMAP) are the #1 attack vector for credential-stuffing botnets because they pass passwords in cleartext without supporting multi-factor handshakes. Blocking them closes an entire class of automated brute-force attacks.

3.0 IMPLEMENTATION CHECKLIST: 4 CLICKS TO DEPLOYMENT

- * **[] Step 1:** Sign in to the Microsoft Entra Admin Center (<https://entra.microsoft.com>) as a Global Administrator.
- * **[] Step 2:** Navigate to: Identity > Overview > Properties tab (or search 'Properties' in the top search bar).
- * **[] Step 3:** Scroll to the bottom of the Properties pane and select: Manage security defaults.
- * **[] Step 4:** Toggle 'Security defaults' to 'Enabled'. Select 'Save'.

PRE-ACTIVATION PREREQUISITE

If your organization has legacy Conditional Access policies enabled, Security Defaults cannot be turned on until they are disabled. For small teams, Security Defaults offers superior out-of-the-box coverage compared to poorly maintained custom rules.

4.0 POST-DEPLOYMENT VERIFICATION

- * **Test Admin Access:** Open a private browsing window (InPrivate/Incognito) and attempt to sign in to <https://admin.microsoft.com>. Confirm MFA challenge triggers.

- * **Inspect Sign-in Logs:** Navigate to Entra ID > Monitoring > Sign-in logs. Filter by 'Client App: Other / Legacy Protocols' to ensure legacy attempts are returned as 'Blocked'.
- * **User Communication:** Notify staff that upon next login they will receive a prompt to install Microsoft Authenticator.

5.0 DIRECT DOCUMENTATION LINKS

Entra Admin Center: <https://entra.microsoft.com>

Microsoft Security Defaults Docs: <https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>

Legacy Auth Remediation Guide: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/block-legacy-authentication>