Microsoft 365 Azure Active Directory Best Practices Checklist

By Alex Fields, ITProMentor.com

Updated July 15, 2019

	Checklist item	Description	End user impact	Where to change this	Importance
☐	Create emergency access global admin account	Cloud-only accounts configured with long password (e.g. 100 characters) and excluded from MFA / Conditonal access	None	Microsoft 365 Admin center > Users > Active users	Critical
☐	Configure multi-factor authentication settings	Disable app passwords (which bypass MFA), and enable MFA for all accounts	Users must register for and use the MFA service upon next sign-in via the web portal	Multi-Factor Authentication > service settings	Critical
☐	Setup Recommended Conditional Access policies	Refer to my Conditional access policy design and guide	Users must meet the conditions specified by policy in order to gain access to resources	Azure AD > Conditional Access blade	Critical
☐	Block users from consenting to apps requesting permissions	Users should not be able to grant permissions to apps or add-ins	If users want to configure add-ins they will require an admin's help	Enterprise Applications > User settings	Critical
☐	Configure the password expiration policy	Ensure that your password expiration is in alignment with corporate policy	Users will be required to change passwords according to the policy	Microsoft 365 Admin center > Settings > Security & Privacy	Recommended
☐	Configure Company branding for login	Corporate branding of the login page reduces likelihood of phishing via look-a-like pages	Users will see corporate background and logo displayed at login screen	Azure AD > Company branding	Recommended
☐	Restrict user access to the Azure AD admin portal	By default users can access and browse the admin portal (without the ability to changes)	Users will be unable to login to the Azure AD admin portal	Users > User settings	Recommended
☐	Enable Self-service password reset	Allow users to reset their own passwords using a second factor	Users must register for SSPR in order to reset passwords	Users > Password reset	Recommended
☐	Configure device settings for Azure AD joined devices	Require MFA in order to join new devices to Azure AD	Users who attempt to join new Windows 10 devices to Azure AD must perform MFA	Devices > Device settings	Recommended
☐	Configure external collaboration defaults	Consider disabling external users from being able to invite other guests to shared content	Users external to the organization will not be able to share or invite other users	Users > User settings > Manage external collaboration settings	Optional
☐	Enable combined registration (enhanced)	This feature is in preview, use preview features at your own risk	Users will only have to register once for both MFA and SSPR	Users > User settings > Access panel > Manage settings for access panel preview features	Optional
☐	Configure Enterprise apps	Azure AD can manage third-party apps as well as Microsoft apps	Users will have access to Enterprise apps via the apps portal or app launcher in 365	Azure AD admin center > Enterprise applications	Optional
☐	Configure optional settings for Office 365 Groups	Admins can configure expiration, naming policy and more	Group owners would receive email notification of renewal, adhere to policies, etc.	See settings under Groups blade in Azure AD	Optional