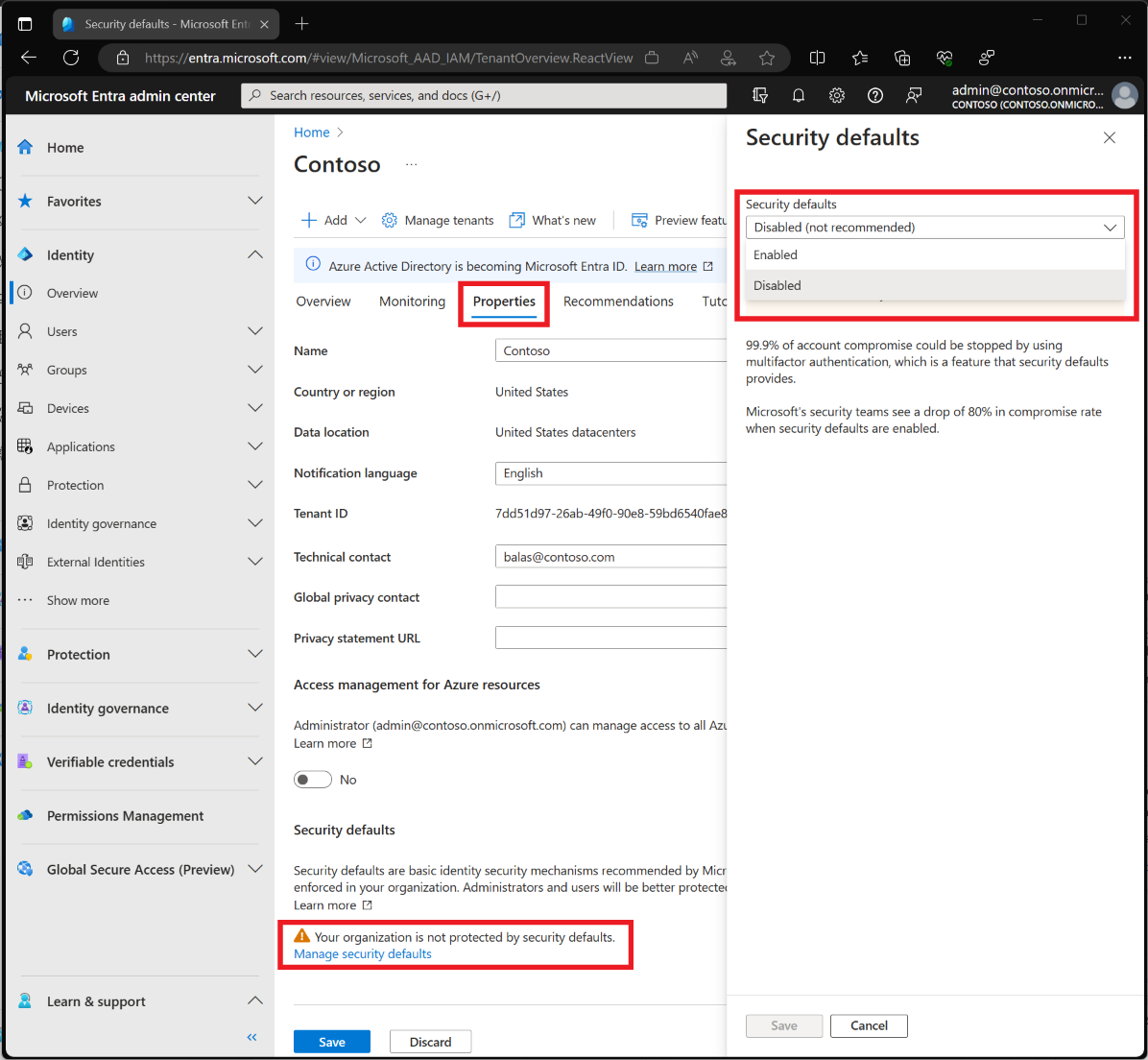
Security defaults make it easier to help protect your organization from identity-related attacks like password spray, replay, and phishing common in today's environments.

Microsoft is making these preconfigured security settings available to everyone

To enable the Security Defaults:

* Sign in to the Microsoft Entra admin center as least a Security Administrator.
* Browse to Identity > Overview > Properties.
* Select Manage security defaults.
* Set Security defaults to Enabled.
* Select Save.



Basic Security Setup

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Configuration** | **Comments** | **How to do - Link** | **Check** |
| Multi-Factor Authentication | * Enable a Conditional Access Policy for Multi-Factor for Administrator Accounts * Enable a Conditional Access Policy for Multi-Factor for all User Accounts | * <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa#create-a-conditional-access-policy> * <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa#create-a-conditional-access-policy> |  |
| Sign Out Inactive Users Automatically | implement Idle Session Sign-out. | implement Idle Session Sign-out. |  |
| Block Legacy Authentication |  | <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication> |  |
| Set User Passwords to Never Expire | It is now recommended by the National Institute of Standards and Technology (NIST) to disable password expiration. The guidance is only to force a change or update a password if an account is confirmed as compromised.   * Set the password expiration policy for your organization * Set an individual user's password to never expire | * <https://learn.microsoft.com/en-us/microsoft-365/admin/manage/set-password-expiration-policy> * <https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/set-password-to-never-expire> |  |
| Banned Password List | Microsoft Entra ID includes a global banned password list, that protects all Microsoft 365 services. Microsoft Entra ID also provides organizations the ability to add a list of banned passwords. | <https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection> |  |
| External Sharing | Microsoft 365 provides external sharing settings at the tenant and application levels. The decision to modify these settings should be business-related. Setting this to Only people in your organization, limits external sharing capabilities. | <https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off> |  |
| Account Lockout Threshold | Microsoft Entra Smart lockout uses cloud intelligence to lock out malicious actors trying to guess end-users passwords. The intelligence platform recognizes sign-ins from valid users and treats those differently from those that attackers and other unknown sources. The smart lockout can lock out the attackers yet still allow users to continue to access their accounts. | <https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout> |  |
| Mobile Application Management Policy | These policies can include rules that block the user's attempt to access or move corporate data or are a set of prohibited or monitored actions users can perform when in the app.  The core benefits of Mobile application management (MAM) policies are:   1. Protect organizational data at the app level 2. End-user productivity isn't affected 3. Policies don't apply when app use is in a personal context 4. App protection policies make sure that app protections are in place | <https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policies> |  |
| Block Client Forwarding Rules | Client Rules Forwarding Block lets you manage email auto-forwarding in your organization. Using client-side forwarding rules to exfiltrate data to external recipients is becoming an increasingly used vector for attackers. | <https://support.microsoft.com/office/stop-auto-forwarding-emails-in-microsoft-365-f9d693ba-5c78-47c0-b156-8e461e062aa7> |  |
| Do not allow users to grant consent to un-managed applications | Before an application can access organizational data, a end-user must grant the application permissions. By default, all users can consent to applications for permissions that don't require administrator consent. By allowing users to give apps access to data, users can easily acquire useful applications and be productive   * Configure how end-users consent to applications * Configure the admin consent workflow | <https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent>  <https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow#enable-the-admin-consent-workflow> |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Reference:

* <https://learn.microsoft.com/en-us/microsoft-365/community/basic-security-set-up-for-microsoft-365#security-within-microsoft-365>
* <https://www.microsoft.com/en-ca/microsoft-365/enterprise/microsoft365-plans-and-pricing>

Microsoft 365 Apps for business, provides basic productivity tools but lacks several advanced features and services. Some of the key features not included are:

* Advanced Threat Protection (ATP): The free version does not include ATP, which provides enhanced protection against sophisticated threats such as phishing, malware, and ransomware. ATP helps to safeguard email, files, and collaboration tools like SharePoint and OneDrive.
* Data Loss Prevention (DLP): DLP capabilities, which help prevent the unauthorized sharing of sensitive information and enforce compliance policies, are not included in the free version.
* Identity and Access Management: Advanced identity and access management features such as Azure Active Directory Premium, which includes features like Conditional Access and Identity Protection, are not included in the free version. These features help secure user identities and access to resources.
* Information Protection: Advanced information protection features such as Azure Information Protection, which allows organizations to classify, label, and protect sensitive data, are not included in the free version.
* Security Configuration Policies: The free version does not provide access to security configuration policies, which allow organizations to enforce security settings across devices and applications, ensuring compliance with security standards and best practices.
* Advanced Security Reporting and Analytics: The free version lacks advanced security reporting and analytics capabilities that provide insights into security threats, compliance posture, and user behavior.
* Mobile Device Management (MDM): MDM capabilities for managing and securing mobile devices, such as enforcing device encryption, remote wipe, and app management, are not included in the free version.

Things suited from excel checklist for us:

* Inventory and Control of Software Assets
* Data Protection
* \*\* Account Management
* Access Control Management
* Email and Web Browser Protections
* Security Awareness and Skills Training
* Data Recovery
* Malware Defenses - Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets. Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.
* Continuous Vulnerability Management