CYBER WARDEN

PRACTICAL CYBER RISK MANAGEMENT

# Enable Microsoft Entra Security Defaults

This document is a summary of https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults

## What are security defaults, and why do I need this?

In Microsoft's words:
*"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, because we know managing security can be difficult. Based on our learnings more than 99.9% of those common identity-related attacks are stopped by using multifactor authentication and blocking legacy authentication. Our goal is to ensure that all organizations have at least a basic level of security enabled at no extra cost."*

The key statement here is "more than 99.9% of those common identity-related attacks are stopped by using multifactor authentication and blocking legacy authentication."
This describes perfectly how to stop over 99% of attacks on your business in their tracks. This includes Business Email Compromise, when bolstered with a strong DMARC policy (reject or quarantine).

When Phishing Resistant authentication (such as FIDO2 based security keys or passkeys), then risk is reduced even further.

## Prepare

**Create** two separate Global Admin accounts for "break glass" scenarios. Keep the credentials and authentication in an envelope, locked in a safe. We recomment using FIDO2 physical keys (e.g. Yubikey) for this purpose. You can register each key for both accounts for redundancy.
Test the "break glass" accounts BEFORE you enforce security defaults. See emergency access account recommendations for more information.

If your **administrator(s)** are using a priviliged account for their day-to-day work, then they should have separate administrator accounts created for this purpose that don't have mailboxes, and aren't used for general web browsing, and their day-to-day account should be relegated to a regular user account. When admin privileges are needed, they can use a an incognito/private browser session and authenticate accordingly for ease of use. We

recommend that all admin accounts use phishing resistant authentication via passkeys or FIDO2 keys. This also removes the need to remember passwords. Register and test these before enabling security defaults.

**Notify** your users of the upcoming change, and allow them to prepare before it by installing Microsoft Authenticator on their mobile device, and pre-registering at https://myprofile.microsoft.com and selecting the Security Info link.
Microsoft provide communication templates and user documentation to prepare your users for the rollout if you wish.

## Enabling security defaults

All users have 14 days to register using the Microsoft Authenticator app. After the 14 days pass, the user can't sign in until registration is completed. A user's 14-day period begins after their first successful interactive sign-in after enabling security defaults.
When users sign in and are prompted to perform multifactor authentication, they see a screen providing them with a number to enter in the Microsoft Authenticator app. This measure helps prevent users from falling for MFA fatigue attacks.

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