Guardz.

Guide

Boosting The Security of Your M365 Identities

Introduction

Microsoft Azure, including the M365 cloud productivity platform, is a complex and broad product that can leverage different functions and methods for security and authentication based on licensing and business needs.

However, according to **security best practices**, there are readily available functionalities and default settings that don't get the attention they deserve. So this document is designed to bubble them up for broader education of the MSP community.

Enable Self-Service Password Reset (SSPR)

The Self-Service Password Reset [SSPR] is available in Microsoft Entra Free and onwards, but it's not enabled by default. The usage of SSPR in Microsoft Entra ID allows users to **securely reset their passwords** without contacting IT support.

This feature reduces helpdesk dependency while enhancing security through several key mechanisms. It requires users to validate their identity though multiple pre-configured authentication methods like the Microsoft Authenticator app, email/SMS verification or security questions.

Social engineering attacks to IT personnel with the request for reset passwords will less likely be successful, as users can simply be **redirected to the self-service portal**.

To enable SSPR, follow these steps:

1. Go to Microsoft Entra Admin Center → Protection > Password Reset.
2. Under Properties, enable SSPR for: Selected Groups / All Users **(Recommended)**
3. Under Authentication Methods:
   - Require 2 methods for reset **(Recommended)**
   - Allow: Authenticator App, Email, SMS, Security Questions (non-admins)
4. Enable Notifications:
   - Notify users on reset
   - Notify admins on suspicious activity
5. **Test it at aka.ms/sspr**

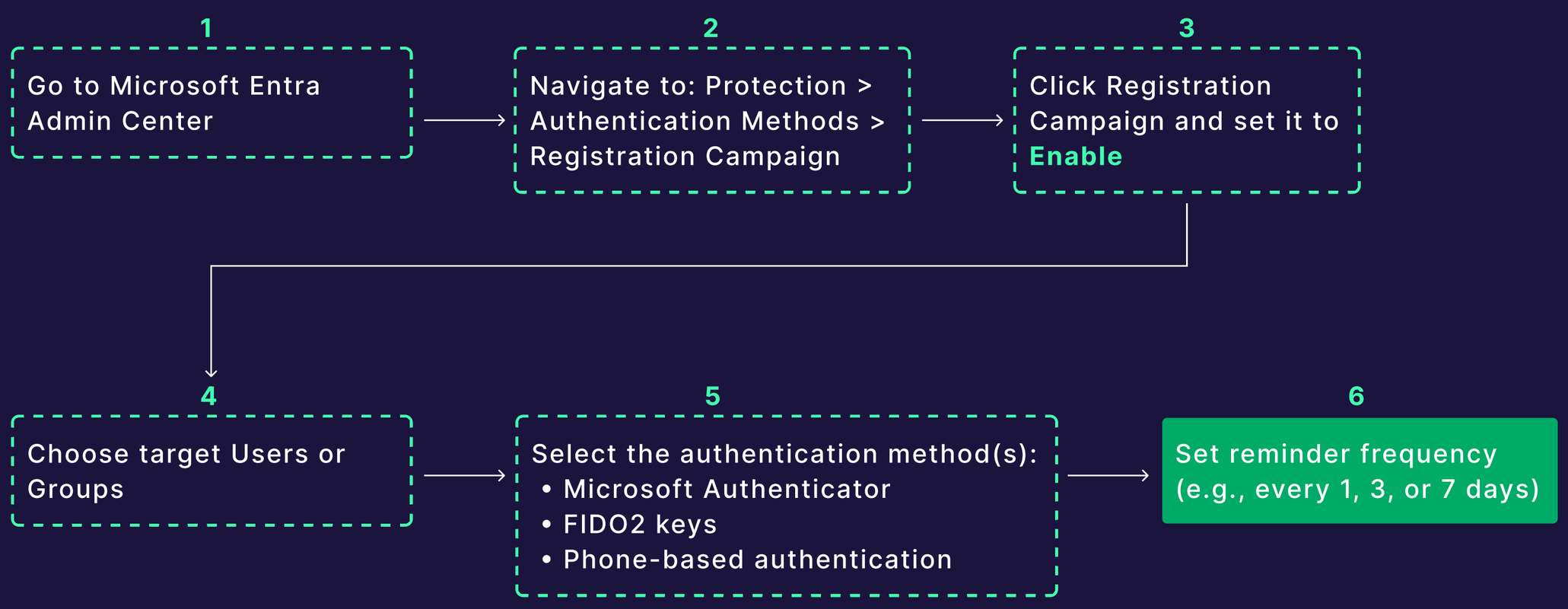
Review your Authentication Methods Registration Campaigns

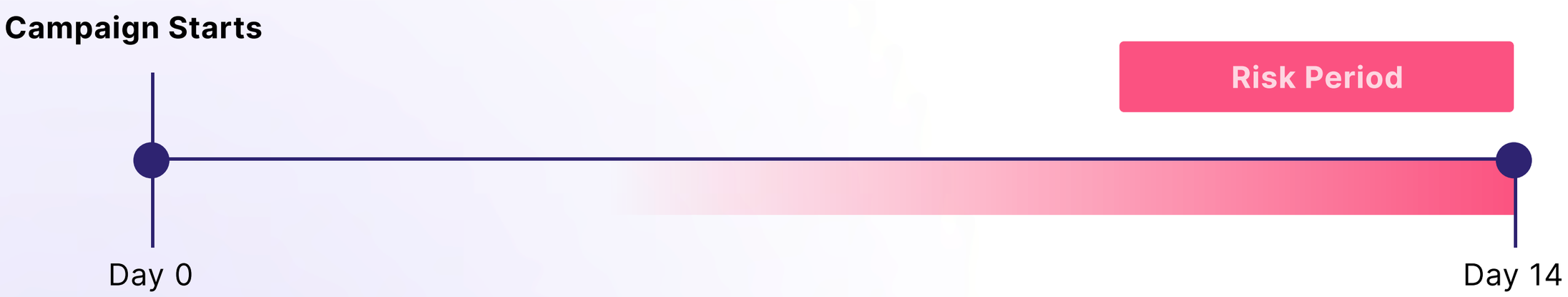
An Authentication Methods | Registration Campaign in Microsoft Entra ID is a feature that encourages users to register for Multi-Factor Authentication (MFA) and/or passwordless authentication methods before they are required to use them. This helps organizations increase adoption and improve security without disrupting users unexpectedly and encourages users to **set up secure authentication methods proactively**.

During the campaign it will provide the users with reminders until the setup is complete.
This is a great way to introduce a more safe way of authentication, but it might leave you with a gap of up to 14 days before MFA is enforced upon an account. During this period an account will pose a more significant risk. It's highly recommended to review this and narrow the period to a few days max.

To review or set up an Authentication Methods | Registration Campaign:

Enable Registration Campaign in Microsoft Entra:





Best Practice:

Shorten the registration period to **1–3 days** to reduce exposure and encourage quicker adoption.

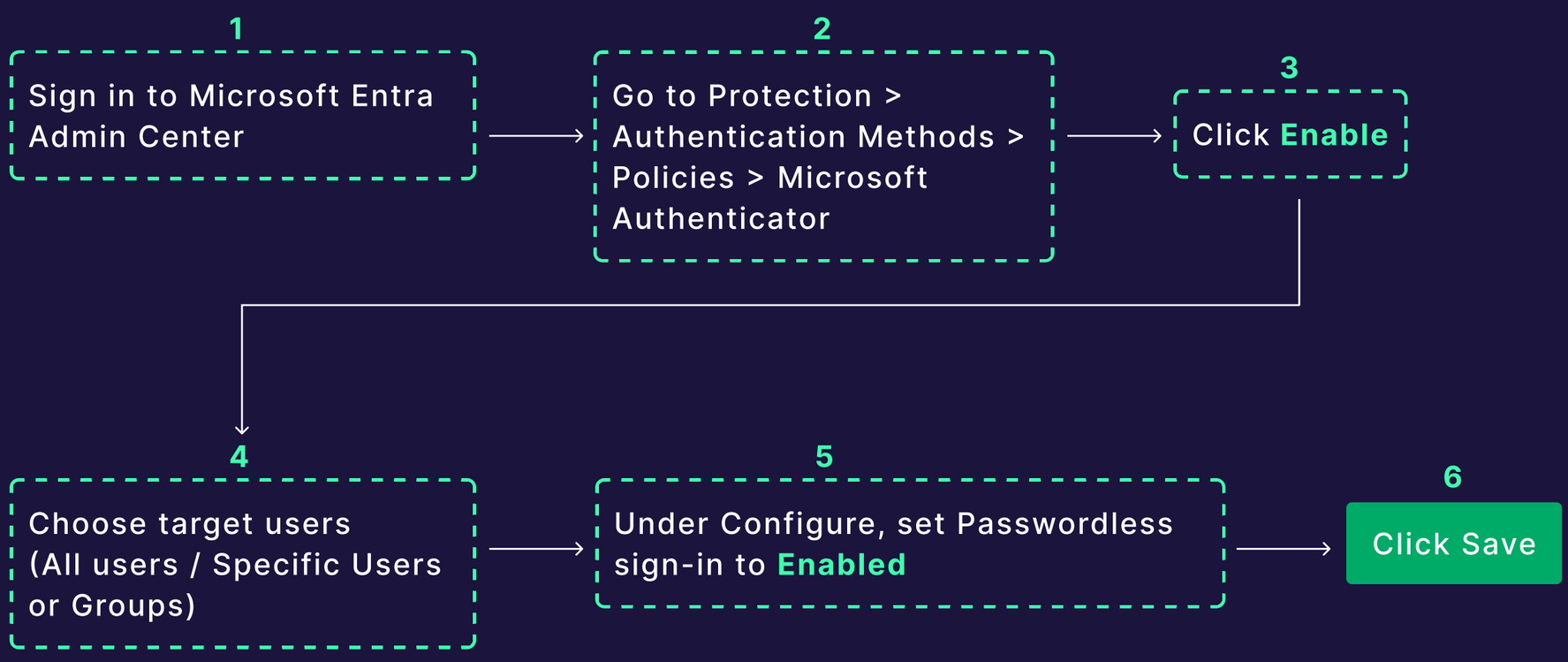
Passwordless Authentication

Traditional password-based authentication presents multiple security risks. This includes weak passwords, credential reuse, and vulnerability to phishing attacks. **Passwordless authentication eliminates these risks** by using stronger, more phishing-resistant methods like biometrics, security keys, and authenticator apps.

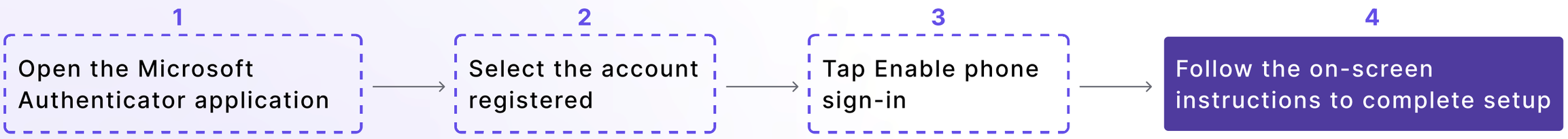
Microsoft's passwordless sign-in with the Microsoft Authenticator app enhances security by leveraging multi-factor authentication (MFA) in a single step. Instead of entering a password or passcode, users approve a sign-in request using biometric authentication (fingerprint or facial recognition) or a device PIN on their enrolled device.

This method is more secure because it **removes reliance on passwords**, which are commonly breached. It will also prevent phishing since there is no static password to steal. And finally, as it leverages device-based authentication it means access is tied to a user's trusted device.

Enable Microsoft Authenticator (Passwordless Sign-In):



Users need to configure the Authenticator app themselves to enable sign-in from a mobile device:



Now, when logging in, the user will simply be prompted for authentication and is not expected to provide a password. The combination of an enrolled device with its own biometric authentication is sufficient, **easier and safer.** Everyone wins.

Controlling App Consent

App Consent in Microsoft Entra ID (formerly Azure AD) is the process where users or admins grant applications permissions to access organizational data, APIs, or resources. This is critical for security and compliance, as **unmanaged app consent can introduce security risks**. Users can grant permissions to apps to run under their own available permissions, but this can still be a security risk.

By default, this is not restricted which allows unverified apps to run in the permissions boundaries of a regular user. Good news, it can be blocked or be restricted to only be allowed for verified publishers. It's also possible to require applications to be **explicitly approved by an an administrator** who wishes to remain in control.

Configure consent:

1. Go to Microsoft Entra Admin Center
2. Navigate to Applications > Enterprise Applications > Consent and Permissions
3. Choose a consent option:
   - ❌ Do not allow
   - ✅ Allow for verified publishers (recommended)
   - ⚠️ Allow for all apps
4. Click Save

Enable Admin Consent Workflow:

1. Go to Enterprise Applications > Consent and Permissions
2. Enable **Admin Consent Workflow**
3. Assign approvers (e.g., admins or security team)
4. Configure email notifications for approval requests

Conclusion

This guide outlines four key configuration changes chosen for their high security impact, ease of implementation, and ability to address common identity risks. Most can be set up within minutes, yet they significantly **strengthen your security posture**. While just a starting point, these controls make it harder for attackers to exploit identities. When paired with real-time security tools such as **Guardz**, strong configurations contribute to powerful, proactive protection against modern threats.