MULTI-FACTOR AUTHENTICATION

What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) takes password security one level higher, requiring that in addition to providing a password, people in your organization will need to prove it's them by acknowledging a prompt on their pre-registered smartphone, or by entering a code sent to their email to approve the login. The "multi" in multi-factor means there is a minimum of one additional form of verification beyond just a password.

Why is Multi-Factor Authentication Necessary?

As organizations move toward cloud-based, accessible services for the convenience of conducting business at any time, from anywhere, protecting their people's online identity has become a critical responsibility. Even with good password practices (e.g. selecting strong, complex passwords or passphrases, never reusing passwords between different online services, etc.) their accounts are still at risk.

Bad actors regularly try to trick people into sharing their corporate password information. These tricks usually fail, but when they do succeed, and they compromise an employee's account, suddenly the organization's reputation, their clients, their vendors, their correspondence – is all at risk. Multi-factor authentication is a small price to pay to minimize the severe consequences of an account compromise.

Three Types of Authentication

Multi-Factor Authentication exponentially increases your level of security by requiring **at least two** of the following types of authentication:

1 Something You Know

Requires the person to present information only they should know.

Examples: Password, passphrase, pin number, security questions

2 Something You Have

A physical item that is unique to the person that can be used to validate their identity during a login attempt.

Examples: Pre-registered smartphone, smart card, token

3 Something You Are

Identity is validated by a unique physical attribute.

Examples: Fingerprint, retinal scan, face scan, voice

According to Microsoft, your account is **99.99% less likely** to get compromised if you're using MFA.[1]

References:

1. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984

Our Multi-Factor Authentication Solution

Aldridge's Multi-Factor Authentication service will add a Microsoft Azure Active Directory P1 or P2 subscription to your existing Microsoft 365 services.

P1 includes: Login Logging, Conditional Authentication, Self-Service Password Reset, and unlimited Single Sign On integrations

P2 includes: P1 features, plus Adaptive Authentication, permitting multi-factor challenges based on patterns of login behavior

We will directly assist a group of 3 to 5 people (that you designate as the multi-factor authentication pilot group) with setting up and using their Microsoft Authenticator application. Allowing the pilot group to test the experience and become comfortable with the application before being introduced to the rest of your organization. Additionally, we will provide written instructions on setting up and using the Microsoft Authenticator app which can be distributed to the rest of your employees.

Aldridge will activate and enforce multi-factor authentication for everyone in your organization (usually 3 to 5 business days after the pilot). We will engage in post-deployment assists for 1 to 2 business days after deployment to help users with any issues or exceptions. New hires will receive help configuring their multi-factor authentication as part of new user set up and onboarding.

Service Features

- Managed MFA Configuration & Deployment
- Advanced Baseline Security Features (Logging & Conditional Access)
- Rolled Into New User Onboarding Process
- Convenience Features (Password Reset & Single Sign On)
- MFA Self-Setup Guide

Enable Multi-Factor Authentication in Your Business Today

Businesses' increasing utilization of cloud-based software, coupled with the growing prevalence and sophistication of cyberattacks has made relying on one authentication type too risky. Multi-Factor authentication is no longer a recommendation, it's a requriement. Enabling MFA is a cheap and easy way to drastically improve your organization's security posture. Click the button below to contact an Aldridge representative and start securing your business today!

Contact Aldridge