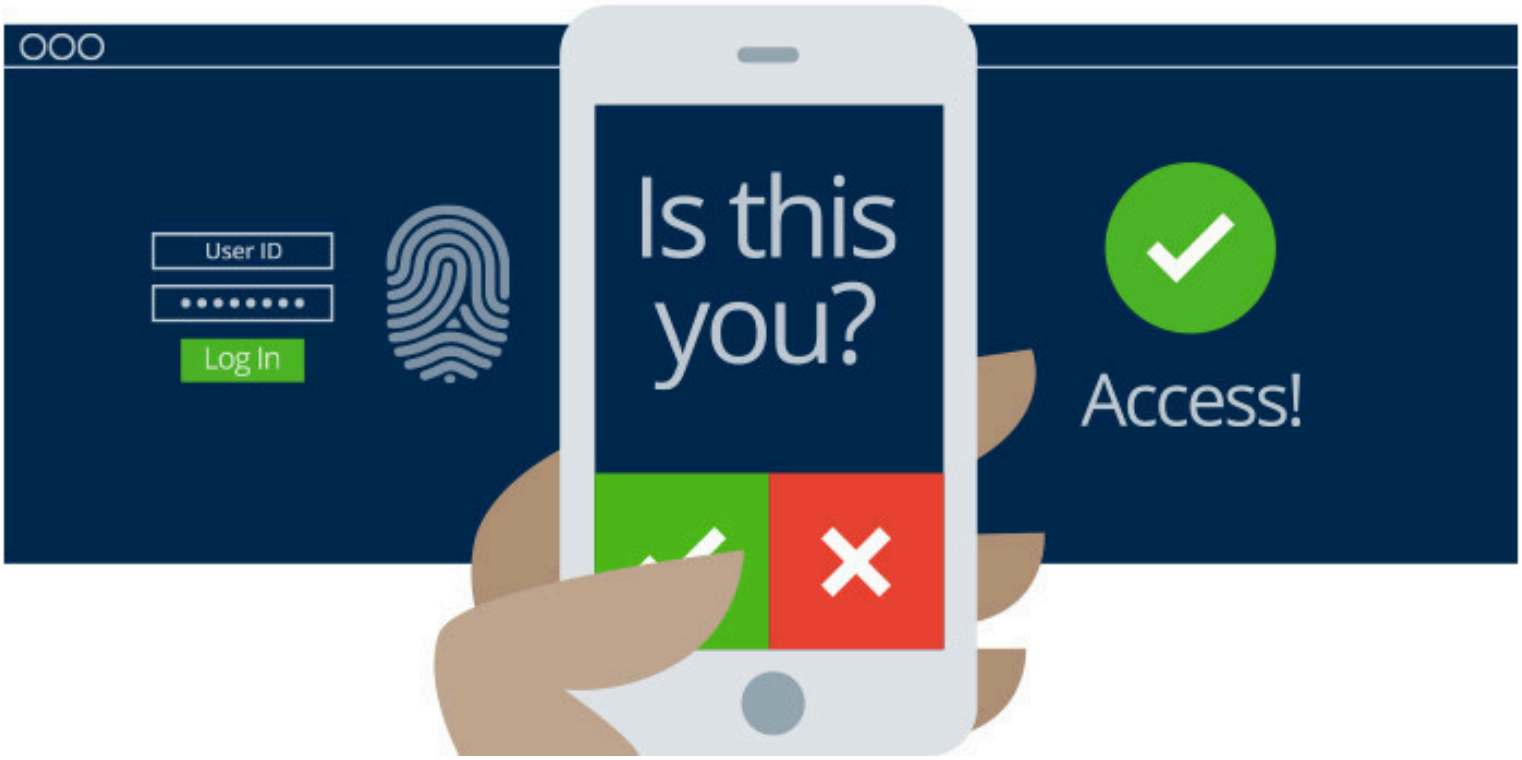
Quicklaunch™
identity & integration



MULTI-FACTOR AUTHENTICATION

Overview

Multi-factor authentication (MFA) is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database.

Why should organizations be interested in MFA?

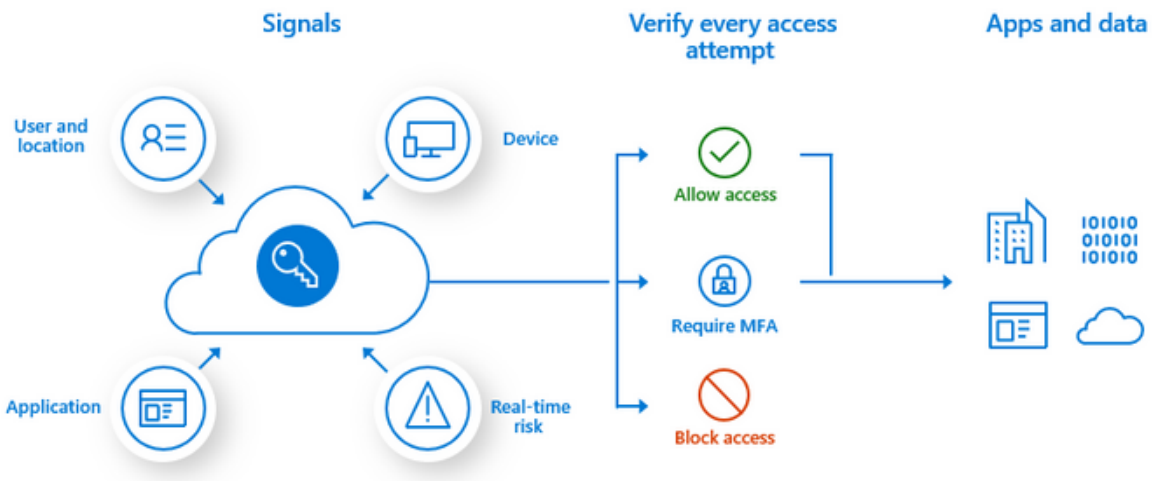
Implementing MFA makes it more difficult for an intruder to gain access to secure databases, applications, and other infrastructure assets. MFA can help prevent adversaries from gaining access to your organization's assets even if passwords are compromised through phishing attacks or other means.

Increasingly, a user ID and password combination alone does not provide enough protection against unauthorized login. One of the major drawbacks of using an ID and password system alone is the requirement to maintain a password database. Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. These factors reduce the security of password-protected systems and resources more each day.

How does MFA work?

MFA requires a system or network users to present two or more credentials at login to verify their identity before they are granted access. Each additional authentication factor added to the login process increases security. A typical MFA login would require the user to present some combination of the following:

- Something you know - Password
- Something you have - Email OTP/SMS OTP/Challenge Questions/Yubikey
- Something you are - Biometrics like a fingerprint or face scan.



Key Features

Password Manager Integration
Enable a secure password reset mechanism through multi-factor authentication.

Role-based Authentication
Establish role-based authentication through several modes like SMS, email, mobile app.

Challenge Questions
Verify your users through challenge questions & make sure the right person logs in.

YubiKey Integration
Yubikey will act as a hard-token authenticator enabling users to login to their apps anytime, anywhere using touch ID

SMS OTP
Users get a verification code on their phones which helps verify their identity.

Google Authentication
Protect your user accounts and company data with Google Authenticator.

Diverse Detection Criteria
Trigger authentication based on user's location, network, device, browser etc.