Activity
Applications
Authentication
Organizations NEW
User Management
Branding
Security
Attack Protection
Multi-factor Auth
Monitoring
Actions
Auth Pipeline
Monitoring
Marketplace
Extensions
Authorization
Settings

Multi-factor Authentication

Multi-factor Authentication works by requiring additional factors during the login process to prevent unauthorized access.

Use of the Phone Message, Email, WebAuthn, and Push via Auth0 Guardian factors require the purchase of an Enterprise MFA add-on to your Auth0 subscription. Please contact us to get started.

1 Factors

Utilize push, SMS, email, one-time password, or a combination of different methods and easily enable them across all users and applications.

WebAuthn with FIDO Security Keys
Use WebAuthn-compliant security keys
Disabled

WebAuthn with FIDO Device Biometrics
Use WebAuthn-compliant device biometrics
Disabled

One-time Password
Provide a one-time password using Google Authenticator or similar.
Enabled

Push via Auth0 Guardian
Provide secure access with a push notification using Guardian.
Enabled

Phone Message
Users will receive a text message or voice call containing a verification code.
Enabled

Email
Users will receive an email message containing a verification code.
Enabled

Recovery Code
Provide a unique code that allows users to regain access to their account.
Disabled

DUO Security
Use your DUO account for Multi-factor Authentication.
Disabled

2 Define policies

Policies determine when a user will be prompted to complete additional steps to prove they own a particular account. Use policies to define your level of acceptable risk. You can achieve more refined multi-factor configurations (ex. per application, per user, etc.) by using Rules. Learn More

Require Multi-factor Auth

Define when users will be able to authenticate using an additional factor for all Applications

- **Never** — Users are not required to use an additional factor to login.
- **Use Adaptive MFA** ADD-ON — Users are required to have an additional factor if the login appears to be a high risk. Contact Sales.
- **Always** — Users are always required to use an additional factor to log in.

MFA Risk Assessors

Enable Adaptive MFA Risk Assessment ADD-ON

Risk will be assessed and recorded for all login transactions in your tenant logs. Adaptive MFA Risk Assessment is required for enabling the Adaptive MFA policy, but can also be used to implement custom MFA policies using Rules.

Save Cancel

Get support
Give feedback