

## Multifactor Authentication for Employees

### THE PROBLEM

On August 5, 2014 the New York Times reported that Russian hackers had amassed the largest known collection of stolen internet credentials, including 1.2 billion user name and password combinations. Compounded with the propensity of people to reuse passwords across sites and applications, a clear and present security threat is in play, and is getting worse. Without multi-factor authentication, security is a joke, so we have to enhance our existing and new applications to require it when appropriate.

### THE SOLUTION

As username and password exploits continue to dominate the headlines and threaten the security of even the strongest global companies and brands, security experts agree that adding multifactor authentication (MFA) to login flows can help mitigate this vulnerability and strengthen their security posture.

In a multifactor authentication scenario, in addition to username/password, users may be requested to provide additional credentials to verify their authenticity such as a fingerprint, retina scan, facial or voice recognition, a one-time password from a hardware or software token, an SMS texted code, an email delivered code, answers to secret questions, or their physical location – the list goes on and on.

Additional “something you know”, “something you have” or “something you are” factors can be requested at initial login to ensure the identity of the employee who wants to use a given application. Additionally, a technique known as contextual MFA is gaining in popularity, whereby requests for additional credential factors are based on the context of the user’s interaction such as a group they are in, access from a new device or location, the value of the resource being accessed or the time.

### THE BIG PICTURE

Auth0 can be used to enhance both existing applications, for which there may be no source code, and new applications, for which source code is available. For existing applications, the Identity Provider (IdP) configuration setting is changed from the existing IdP to Auth0. This allows Auth0 to operate as a broker, adding value through the authentication flow as MFA, contextual MFA, logging user activity, and more while it brokers requests to the existing employee IdP. New applications use the Auth0 APIs through convenient, platform-specific SDKs using the code samples and customized step-by-step guidance that developers highly value from Auth0.



*Auth0 adds MFA capability and more to both existing and new applications*

## MULTIFACTOR AUTHENTICATION OPTIONS

Once Auth0 has been introduced between the applications and the existing IdP or database that holds the employee identities, it can be used to easily add multifactor authentication and more to existing and new applications. Auth0 MFA features include:

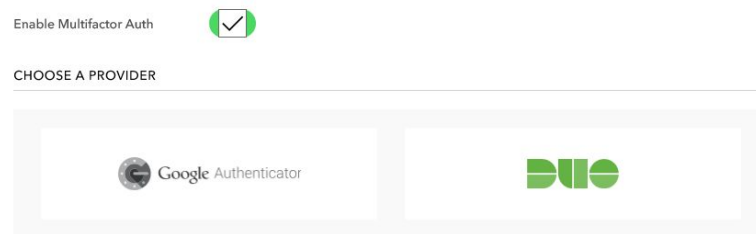
(i) Use practically any of the dozens of MFA solutions that exist today including SMS Text, email, biometric, password-less and more. Broad support for MFA service providers is enabled through powerful authentication flow “rules” with Auth0, which are described below. An example of rules being used to incorporate the YubiKey USB device can be found here (<https://auth0.com/docs/multifactor-authentication/yubikey>).

(ii) Add contextual MFA which allows you to define arbitrary conditions that will trigger additional authentication challenges to your users for increased security, for example, geographic location (geo-fencing), address or type of network used (IP filtering), time of day, day of the week or change in the location or device being used to log in – whatever you have access to, as described here (<https://auth0.com/docs/multifactor-authentication>).

```
1  function (user, context, callback) {  
2  
3      if( condition() && context.protocol !== 'redirect-callback' ){  
4          context.redirect = {  
5              url: 'https://your_custom_mfa'  
6          };  
7      }  
8  
9      if( context.protocol === 'redirect-callback'){  
10         //TODO: handle the result of the MFA step  
11     }  
12  
13     callback(null, user, context);  
14 }
```

Auth0 “rule” for using any MFA service that can be accessed via a URL

(iii) With the flip of a switch in the Auth0 dashboard, add or remove the popular Google Authenticator MFA experience ([https://en.wikipedia.org/wiki/Google\\_Authenticator](https://en.wikipedia.org/wiki/Google_Authenticator)) or the Duo Security MFA experience (<https://www.duosecurity.com/>) into the authentication flow. No rules are required to use these services, because Auth0 has already written them and made it as easy as flipping a switch.



*Enable MFA for any application with the flip of a switch*

## EXTENSIBILITY WITH RULES

Auth0 allows you to customize and extend the authentication flow through JavaScript functions called rules (<https://auth0.com/docs/rules>). Rules run after Auth0 or a federated IdP has authenticated the employee and before control is returned to the application that called Auth0.



*Rules are run after the user is authenticated and before control is returned to the application*

Many customers have found the Auth0 rules feature to be very helpful. Rules allow you to easily implement all kinds of customizations to the login process with just a little bit of code. Some of the most popular uses for rules include:

- Adding multi-factor authentication
- Contextual MFA (context-aware, risk-based authentication)
- Adding, removing or enriching user attributes drawn from several IdPs or databases
- Automate user enrollment and deletion
- Require consent & legal terms acceptance
- Redirect to a page where the user consents to certain claims being sent to the requestor
- Sending events to analytics tools like Mixpanel, Segment or KISSMetrics
- Enforce access control policies

Auth0 provides rule templates to speed the creation of new rules and a large number of useful rules have been contributed by the active community on GitHub (<https://github.com/auth0/rules>).

## WHAT ABOUT SINGLE SIGN-ON

Auth0 can be used to provide a full SSO capability that can span the enterprise and the Web, should an organization wish to implement SSO in addition to MFA. It can also federate with numerous corporate identity providers as well as social and commercial identity providers with the flip of a switch in the Auth0 Dashboard to support partners and customers in addition to employees, should the need arise.

## ADVANTAGES

Auth0 makes it easy to incorporate MFA and contextual MFA into the employee's experience for both existing and new applications, which is essential in today's world where username/password pairs offer little protection. Once it is being used for MFA, Auth0 provides the opportunity to add other capabilities such as keeping user activity logs, single sign-on, federated login with social or commercial identities and more. With Auth0, getting MFA implemented for all of the applications your employees use every day is easier than you think.