

Multifactor Authentication for Customers

THE PROBLEM

Unfortunately, people create very weak passwords, and what's worse is that they reuse their passwords across social and commercial Web sites. Should any of those Web sites be penetrated, one day an impostor who has your customer's username and password may login to your Web site. The only feasible defense is to implement multifactor authentication (MFA). But any MFA solution has to work for both older applications, for which there is no source code and new applications for which there is source. It has to be able work in a scenario where the customer's identity is held elsewhere such as at Google, Microsoft, Facebook or Amazon, and it has to be easy to implement.

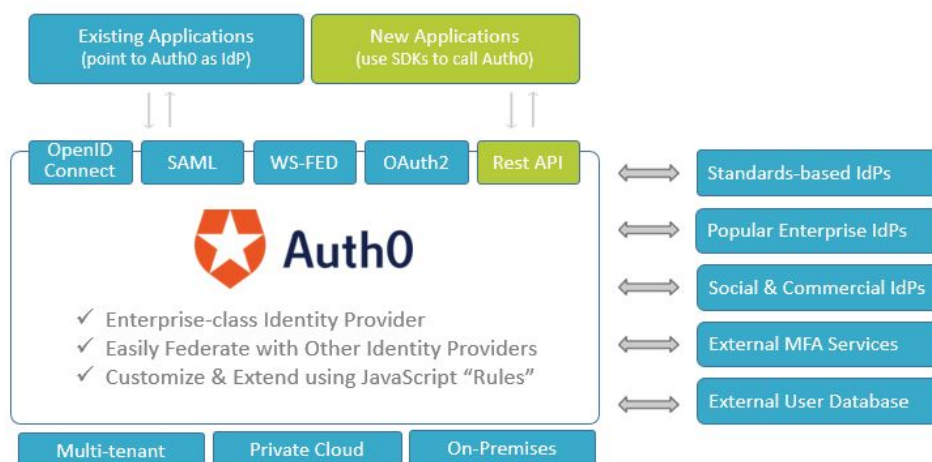
THE SOLUTION

In a multifactor authentication scenario, additional "something you know", "something you have" or "something you are" factors are requested by the application in addition to username/password. Popular methods include a fingerprint with Apple TouchID, retina scan, facial or voice recognition, a one-time password from a hardware or software token, an SMS texted code, an email delivered code, answering secret questions, or being in some physical location – the list goes on and on.

MFA can be requested at initial login to ensure the identity of the customer 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 customer's interaction such as a group they are in, access from a new device or location, the resource being accessed or the time.

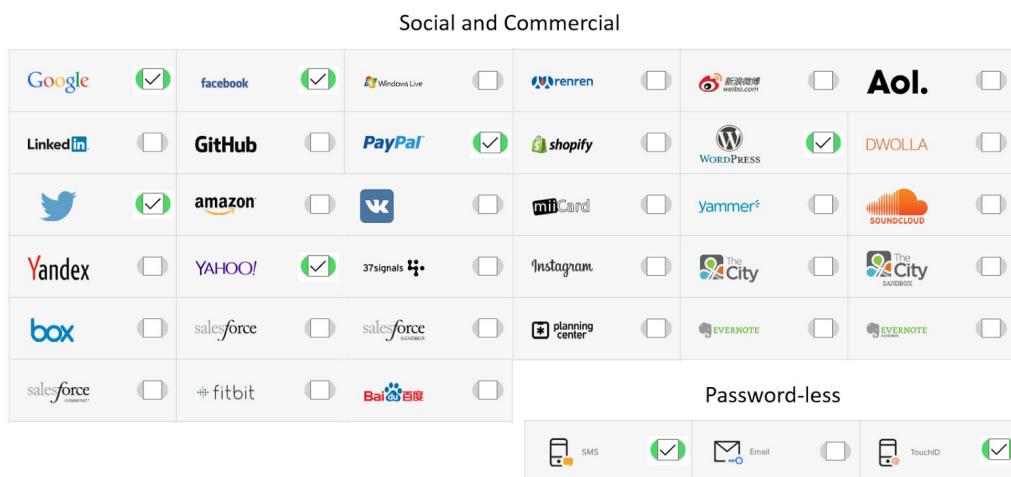
THE BIG PICTURE

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, change the setting that is used to get to the Identity Provider (IdP) for the customers from the existing identity provider to Auth0. This allows Auth0 to operate as a broker between the application and the original customer IdP or external user database. New applications will use the Auth0 APIs through the convenient SDKs that are specific to each device or application framework, along with the renowned Auth0 code samples and customized step-by-step guidance for each specific scenario that developers rave about.



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

Once the applications are using Auth0 as their IdP, Auth0 enables you to service existing customers without them having to change their passwords or take any action whatsoever. Customers can be given the choice to log in with any of the standards-based or popular social and commercial IdPs such as Windows Live, Google, Facebook, Amazon, Salesforce, as a few examples.



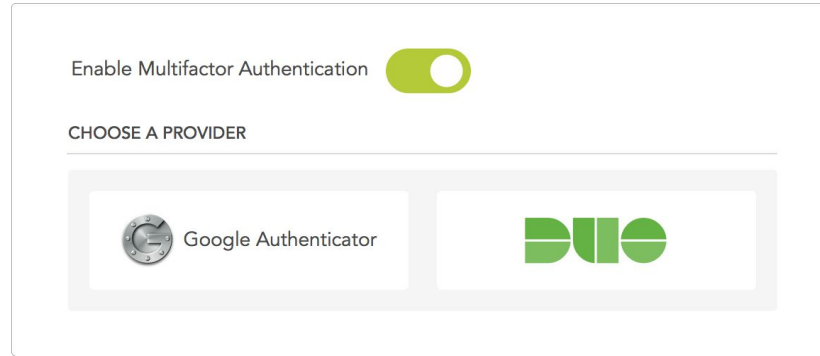
Auth0 federates with any OpenID Connect, OAuth or popular IdP

Once in place, Auth0 provides the solid foundation required to add additional capabilities uniformly across all applications running on mobile devices or on the Web such as providing SSO, password-less authentication, multi-factor authentication, contextual MFA, logging user activity, and more.

MULTIFACTOR AUTHENTICATION OPTIONS

It is easy to add contextual multi-factor authentication where and when it is appropriate, on a per-application basis, for each user or group of users. Auth0 MFA features include:

- (i) Use any of the dozens of MFA solutions that exist today including SMS Text, email, biometric, password-less and more, and be ready to add any new ones easily as they become available or necessary. Auth0 provides support for all MFA service providers through powerful authentication flow “rules”, which are described below.
- (ii) Add contextual MFA which allows you to define arbitrary conditions that will trigger additional authentication challenges to your customers 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 as described here (<https://auth0.com/docs/multifactor-authentication>).
- (iii) With the flip of a switch in the Auth0 dashboard, add the popular Google Authenticator MFA experience (https://en.wikipedia.org/wiki/Google_Authenticator) or the Duo Security MFA experience (<https://www.duosecurity.com/>) into the authentication flow for any applications.



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>), which run in a secure sandbox and allow Auth0 to be extended easily. Rules run after the existing IdP has authenticated the customer 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 of our 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 JavaScript 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
- User enrollment
- Consent & legal terms acceptance
- Redirect to a page to consent to user 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>).

ADVANTAGES

Auth0 makes it easy to incorporate MFA and contextual MFA into the customer's experience for both existing and new applications and provides the opportunity to add other capabilities such as password-less authentication, keeping user activity logs, single sign-on, login with social or commercial identities and more. With Auth0, getting MFA implemented for all of the applications your customers use is easier than you think.