

Web Authentication for the Enterprise



How SecureAuth is different from alternative solutions:

Easier on the end user

- Same username and password
- Strong authentication happens invisibly in the background
- No tokens to carry or manage
- 100% mobile – user not tied to single client

Simple, less expensive to deploy and administer

- A fraction of the cost of hard tokens (RSA SecurID, Vasco, etc.)
- No modification to application required
- No hardware tokens or client software to manage
- No additional, proprietary user data to store and sync
- Requires no provisioning

More Secure

- Bi-directional scheme authenticates both user and protected resource
- Digital certificates prevent phishing, MITM vulnerability

How Does SecureAuth Work?

SecureAuth is able to work web applications' native ability to redirect an unauthenticated user. SecureAuth is able to accept an unauthenticated user as a redirect, process a configurable 2-Factor, tokenless authentication and then return the user to the application.

MultiFactor SecureAuth for Web Authentication

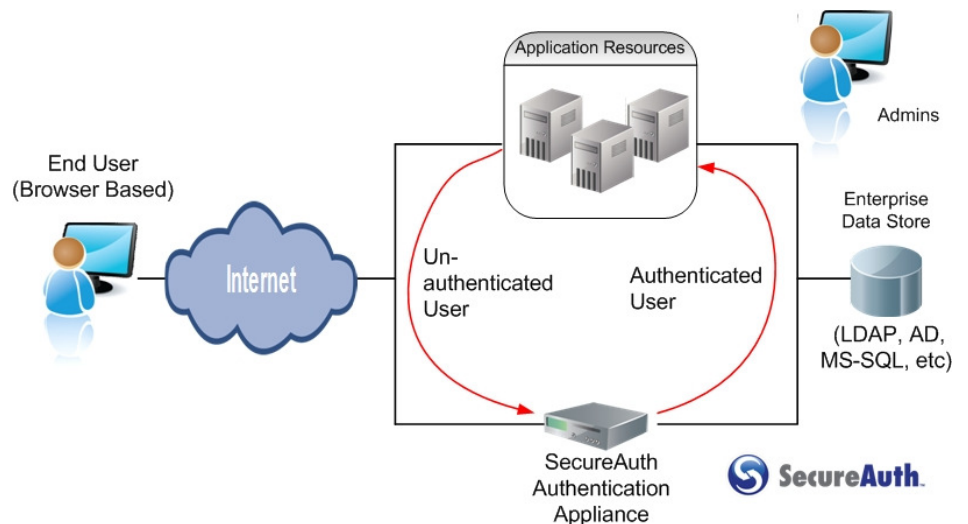


Image #1: SecureAuth authenticates the user and then returns either a valid session or authentication message to the application.

MultiFactor SecureAuth steps to Sign on:

1. Via browser, user attempts to access web resource
2. User is redirected to SecureAuth URL
3. SecureAuth conducts bi-lateral authentication
4. Upon Successful Authentication, SecureAuth redirects user back to target application
5. User is granted access either via a common session ticket or an authentication message such as SAML or datastore GUID.

SecureAuth utilizes native integration into most enterprise and web application environments including:

