

# SecureAuth IdP

## 2-Factor Authentication

### Secure and Flexible 2-Factor Authentication

SecureAuth provides the unique ability to allow a flexible workflow that not only protects your corporate resources, but does so in a way that is easy to manage and easy to use.

Our workflow integrates multi-factor authentication, including 2- and 3-Factor Authentication options that work with identity assertion to grant access into all facets of IT. This even includes mobile devices and native mobile applications.

Enterprises are given full control of their security configurations. They can designate access to individual users, groups, devices, or applications depending on their desired security levels and protocols. You can permit admittance with only a username and password, or you can require strong authentication with OTPs or even hard tokens.

### SecureAuth IdP 2FA Workflow is Part of the Single, Secure Solution

SecureAuth IdP is **one** integrated solution that does not require any hardware or installations, and all of our great features come built right into it.

2-Factor Authentication (2FA) works with data in your company's established directories and can be integrated with your existing VPNs, Web Servers, Cloud, and Mobile Applications. SecureAuth IdP pulls the necessary information from the enterprise data store that corresponds to the user's profile to validate the identity.

All of SecureAuth IdP functions are coded by us and enveloped into an integrated package. By simply modifying the parameters of the SecureAuth GUI console, an administrator can control the authentication workflow into the various corporate resources of Web, Network, Cloud, and Mobile.

### Identity Access Management and 2FA

SecureAuth's 2FA is easily deployed. Users self-enroll themselves for 2FA and can even reset their own passwords without any assistance from the help desk.

Admins can easily create restrictions and edit or revoke permissions from a Graphical User Interface (GUI). Dropdowns are enabled that make configuring the protection effortless.

Among the many options, admins can also design authentication due to various risk factors. You can enforce stronger authentication for users based on geography, IP, devices, and other factors. SecureAuth authentication can be required every time a user utilizes that device or for each application individually; or single sign-on (SSO) can be enabled, which would allow users access into all programs after accurately logging into one. You make all of the decisions.

### Various Authentication Methods

SecureAuth IdP makes authentication simple by providing multiple and integrated authentication options. Users already have most of them (or can quickly obtain one), so there is very little risk of not being able to authenticate due to missing the second factor.

SecureAuth offers phone calls, text messages, emails, static PINs, NFC, Mobile OATH tokens, PUSH Notifications, and more. You can even use hard tokens with our system if you so desire, but they are not required. They are all configurable from the admin console.



# Secure all of your corporate resources with SecureAuth IdP 2-Factor Authentication

## Flexible Workflow Integration

- Multi-Factor Authentication
- GUI Integration to:
  - Web, Network
  - Cloud, and Mobile

## Flexible Configuration Options

- ID + PW
- ID + 2FA + PW
- ID + 2FA + 3FA + PW
- ID + Device
- ID + Device + PW
- ID Token (SAML, OpenID, Kerberos)
- ID Token + 2FA
- ID Token + 2FA + PW

## Flexible Persistency:

- Device Fingerprinting
- Desktop
- Mobile
- Mobile/Desktop X.509 Certificates
- Java Certificates

## 2FA Based on Datastores

- AD, v3, LDAPs, SQL
- ODBC, REST APIs
- Web Services

2FA functions can be applied to any user, group, application, or device to ensure valid identities before granting access.

## Easy Identity Management (IdM)

### No Coding Required

- GUI Drop Downs
- No APIs

### Risk-based Authentication for

- Internal / External
- Registered / Unregistered Device
- Desktop / Mobile
- Group
- Country
- IP Address

## 2-Factor Authentication Includes:

- SMS OTP
- Telephony OTP
- E-mail OTP
- Static PIN
- KBA/KBQ
- Yubikey (USB)
- X.509 Native
- X.509 Java
- Kerberos (IWA)
- Password
- NFC Prox Card
- CAC/PIV Card
- Mobile OATH Token (TOTP)
- Browser OATH Token (TOTP)
- Windows Desktop OATH Token (TOTP)
- Third-Party OATH Token (TOTP)
- PUSH Notification
- Help Desk
- Social IDs (Facebook, Google, LinkedIn)
- Device Fingerprinting



2-Factor Access Control for the Mobile Enterprise

