Let’s face it, passwords alone are no longer enough to protect your critical resources and data, you have to step things up to maintain security in today’s environment. With two-factor authentication from SecureAuth IdP you can take something a user knows – username and password – and combine it with something that the user has – phone, email, token, etc. – to ensure that access is granted securely and appropriately.

SecureAuth IdP’s 20+ authentication methods range from SMS, telephony, and email one-time passwords (OTPs) to push notifications and USB keys, just to name a few. With our flexible and scalable two-factor authentication workflows, users can be directed to additional methods of authentication to step up access control security on any device - mobile or desktop. Custom workflows can easily be configured by your in-house administrator without requiring coding or third-party tools.

**Features:**
+ 20+ authentication methods
+ Adaptive authentication techniques
+ Unlimited, custom-built authentication workflows
+ User self-enrollment
+ Standards based with no vendor lock-in

**Benefits**
+ Meets your unique access control needs
+ Reduces user friction
+ Integrates easily into existing infrastructures
+ Leverages existing tokens and data stores

**20+ Authentication Methods**
- SMS OTP
- Telephony OTP
- Email OTP
- Static PIN
- KBA/KBQ
- X.509 Native
- X.509 Java
- CAC
- PIV Card
- Push Notification
- Mobile OATH Token
- Browser OATH Token
- Windows Desktop OATH Token
- Third-party OATH Token
- Device Fingerprinting
- Yubikey (USB)
- Password
- Social IDs
- Federated IDs
- Kerberos
- Help Desk
Meet your unique needs with secure and configurable authentication

SecureAuth IdP is an identity provider that obtains identity credentials, verifies the identity against the known data store and then serves up the identity details to service providers or applications in an agreed upon format. Regardless of the application platform, an IdP puts control of the identity verification process in your hands. By employing an identity provider you can easily enforce security standards and deliver low-friction user access at the same time.

This unique architecture provides the ability to configure unlimited flexible authentication workflows that not only protect your corporate resources exactly as needed, but in a way that is easy to manage and easy to use. Different user populations and resources need different security. To meet this varying need, IdP enables full control of authentication workflow configuration, combining over 20 methods with adaptive context and risk based factors, such as live threat intelligence from the Norse DarkMatter network.

With IdP you create workflows that can grant access to individual users, groups, devices, or applications depending on security levels or organizational policy. IdP delivers the flexibility to permit authentication with only a username and password or require multi-factor authentication with risk analysis employing OTPs or hard tokens. It’s up to you!

Plays well with others

Chances are, you already have some form of access control in place, but you’re looking for more. That’s no problem, because at SecureAuth we love standards. We build our solutions using industry leading and standard technologies to ensure that they complement your current security solutions and deploy quickly, layering strong authentication on top of your existing security infrastructure.

SecureAuth IdP installs right into your environment, tying to your enterprise directories, authentication protocols, web servers, and VPNs and utilizing the same IDs, profile information and policies you use today. There is never a need to remake, duplicate, or migrate your data stores, we’ll leverage what’s already in place. Got hard tokens? We work with them too. Yes we can all just get along!

Easily configure authentication to virtually any application

SecureAuth IdP’s two-factor authentication is easily configured and deployed. With IdP, users can self-enroll their devices and even reset their own passwords without any assistance from the help desk, ensuring less friction in the user experience and a lower cost of ownership.

Admins can easily create restrictions and edit or revoke permissions right in the admin interface and dropdowns make configuring the protection effortless.

The SecurePath to Strong Access Control

SecureAuth IdP delivers more than a two-factor solution, it delivers complete access control to meet today’s advanced threats. Going beyond 20+ standard two-factor methods, IdP also provides the latest in adaptive authentication techniques including inspection of IP address, geo-velocity, device fingerprints and more as well as live threat analysis from the Norse DarkMatter network. And once IdP verifies and authenticates identities it can then provide secure single-sign on access to on-premise, cloud, mobile, web and VPN resources. SecureAuth IdP is a single solution that puts you on the SecurePath to strong access control.

SecureAuth IdP analyzes data before and during the authentication process.