HELP GUIDE

Workforce Authentication

Confirm the identities of your employees and contractors with seamless identity authentication.

AUTHENTICID

Whether your employees and contractors are in the office, working remotely, or a hybrid of the two, your organization must address several critical identity-related needs. These include quick access to business resources, confidence a user is who they say they are, and keeping sensitive information safe. Your business might require users to access various systems, company locations and equipment, and applications throughout their work day, requiring multiple points of access and logins. From hiring and onboarding to daily work, a workforce authentication solution using identity proofing simplifies the process for your organization and its users, all while securely confirming identities.

To prevent account compromise without sacrificing user experience, an agile, cutting-edge workforce authentication system should be implemented using the latest in biometric and document verification technologies.

What is Workforce Authentication?

Workforce Authentication verifies the identity of a user before granting that person access to company assets, whether physical or digital. Proper workforce authentication keeps unauthorized users out of organization resources. Workforce authentication is not one-size-fits-all and should be tailored to an organization's specific needs.

Workforce Authentication Top Security Risks

As bad actors and fraudsters improve their tactics, your workforce is more vulnerable to cybersecurity threats and identity fraud tactics, including:

Password Threats

Whether passwords are stolen or shared with other users, the threats could lead to unauthorized access to systems and/or data breaches.

Social Engineering

Whether through email, text, or social media, social engineering is growing more difficult to detect due to bad actors' use of new technology, which manipulates users into sharing confidential information or performing actions that compromise security.

Phishing Attacks

Passwords and other sensitive company and personal information can be handed over with the proliferation of increasingly sophisticated phishing attacks, the most prevalent form of social engineering.

Multiple Attack Surfaces

Users have multiple devices at home and/or in the office with numerous entry points for access and/or vulnerabilities.

Malware

Common in phishing and other email attacks, malware can lead to devastating loss of money and data for companies.

Unauthorized Access

Without strong access controls and/or reliance on passwords and poor password hygiene, systems are left vulnerable to attacks and login attempts from unauthorized users, whether by brute force attacks like credential stuffing or password spraying, and more.

Poor or Non-Centralized System Control

If employees or contractors are able to access sensitive data, download unsafe software, or security levels and remote monitoring are lacking, risks to data security are large.

Choosing a Workforce Authentication Method That Keeps Your Company and Users Secure

Keeping identity at the core of your workforce authentication can keep these threats at bay. A variety of authentication methods are available, and choosing the right one

Various Workforce Authentication methods can suffer from the same issues as many traditional methods of authentication: traditional use of passwords, one-time passwords, and even traditional multi-factor authentication can leave the door open for fraudsters, especially phishing attacks. These methods can also be clunky and time-consuming for users, leading to ineffective, inefficient workflows with poor security.

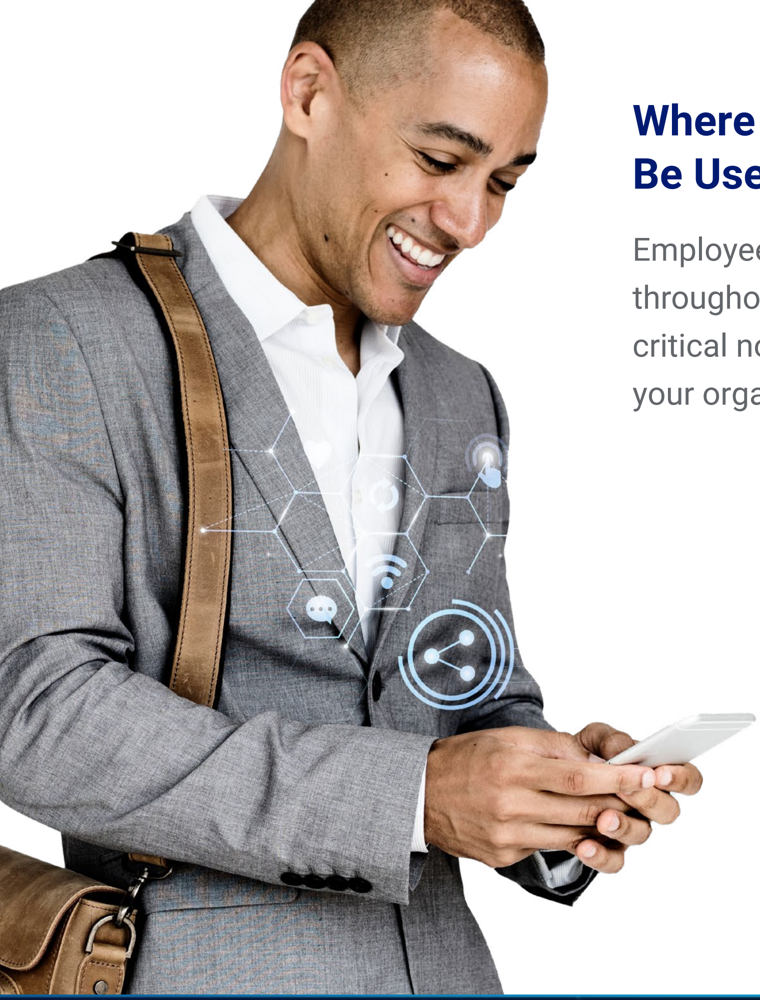
Password-based systems, while commonly used, are especially vulnerable. ***The downside:*** They are a nuisance for both the user and company's IT team. Forrester Research indicates the cost for an average password reset is $70.

Knowledge-based Authentication (KBA) is easy to implement. ***The downside***: This method often becomes a target for attackers due the ease of acquiring personal data.

Two-Factor Authentication Time-Based Pins & Keys, which rely on multiple pieces of information held by a user (whether a password with a text, or security key), add an additional layer of security to make it more difficult for unauthorized users to access your system.
The downside: This method requires a charged device in hand, and often requests get timed out by multi-tasking workers.

Hardware tokens and/or access cards
The downside: They can be lost or stolen and are often inconvenient for users. With a growing remote workforce, this method has become less optimal.

Biometric Authentication
The upside: This method can not only create a passwordless experience for users, but through its reliance on unique biological identifiers can provide both high assurance a person is who they say they are while being extremely difficult to spoof or steal when paired with liveness detection, even when bad actors use the latest in AI technology.



Where Can Workforce Authentication Methods Be Used?

Employees need access to a variety of systems multiple times throughout the day to do their job. Consequently, this process is critical not for just identity and security, but the daily function of your organization.

- New Applicant Screening & Hiring
- Onboarding
- Access to Daily Use Systems
- Access to Sensitive Company Data
- Restrict Access to Certain Workforce Types: Vendors and Contractor Levels
- Privilege Content Access
- Step-Up Authentication Triggers

Employee Enrollment

Verify the identities of applicants as well as new hires during onboarding.

Physical Access

On-site verification of vendors and employees to ensure secure access for legitimate users.

System and App Access

Prevent unauthorized access to organizational systems and apps with step-up enablement for your security needs.

Remote Access

Verify identities with confidence for workers in any location while maintaining user experience.

Legacy Password Self-service

With the cost for an average password reset at $70, save time, resources, and money by eliminating reliance on passwords.

AUTHENTICID

Meeting the needs of your Remote and In-Office Employees and Vendors

How Can Workforce Authentication with Identity Proofing Protect Your Business?

Focus on identity proofing for a robust, seamless process that offers the ability to enroll, authenticate, and re-authenticate your vendors and employees to speed up your hiring and onboarding processes while getting confidence that you truly know your employees and vendors. Biometric solutions with liveness detection can triangulate an identity claim when paired with verification of a government-issued document and eliminates reliance on passwords and other ineffective authentication methods.

Pairing these methods with multi-factor authentication and step-up authentication for access to more sensitive documents, data, or equipment safeguards company resources.

A leading workforce authentication solution can reduce friction and manual checks, while offering the ability to reauthenticate users throughout their workdays with ease.

The Benefits of Workforce Authentication with Identity Proofing

Boost Efficiency with Self-Service Employee Onboarding

Enables new employees or contractors to verify a broad range of ID documents in seconds, plus provides the ability to extract data on the ID for automatic form fill.

Secure Remote Workforce Access

Allow secure access for your remote workforce and protects PII data by removing the need for emailing or faxing hard copies of identity documents.

Ongoing Passwordless Logins and Reauthentication

Enroll a user's facial biometrics to enable passwordless MFA for the ultimate convenience and security.

Reduce Friction

With the ability to verify via a selfie and powerful identity document data extraction, user experience is improved while accuracy and security are at the forefront.

Stay Compliant

Stay compliant with KYC and AML regulations in the employee screening process as well as HIPAA, GDPR, or CCPA.

Saves Company Time, Money, and Resources

Streamlining workforce authentication processes helps save time and money while reducing security risks.

Scalable

No matter the size of your team, cutting-edge workforce authentication can scale to meet your organization's needs and help your business manage identity and access requirements.

How AuthenticID Identity Proofing Technology Can Help

AuthenticID's document verification and biometric authentication technology provide a streamlined way to safely and securely authenticate and onboard users with the access levels you control.

AuthenticID's identity proofing solution is future-proofed and features:

- A layered approach to identity proofing with document verification, selfie verification, and Fraud Shield technology for comprehensive coverage
- 100% automated ID verification with a confident yes/no decision in seconds – no manual review
- Fraud detection and bad actor watchlists powered by AI and Machine learning technology
- Biometric authentication with liveness detection to detect spoofing and deepfakes
- Workflow enablement for step-up and multi-factor authentication
- Platform can eliminate vulnerable passwords

Powerful Identity Verification Solutions, Made Simple

ID Verification

Verify government-issued IDs in seconds with 99%+ accuracy. Detects fraudulent documents with more than 2,000 unique computer vision data models.

Biometric Authentication

Confirm a person's true identity with just a selfie. Our facial recognition software leverages proprietary AI and Machine Learning to verify an identity and FaceMatch the selfie to another photo.

Fraud Shield

Block fraudsters indefinitely. Fraud Shield allows you to identify, flag and add users to the Bad Actor Watchlist using biometric and biographic data.

Liveness Detection

Ensure the person taking a selfie to verify their identity is actually present. Liveness detection stops the most sophisticated spoofing including face masks and deep fakes.

To learn more about Workforce Authentication and other next-gen authentication tools, visit AuthenticID.com or schedule a demo.