Multi-Factor Authentication
Datasheet

Challenges

Password compromises are estimated to be the root cause of an estimated 98% of successful breaches. Yet, the burden of managing passwords, especially for hybrid workforces distributed across on-premises, remote offices, and at-home environments is increasingly onerous. In fact, password-related issues already take up an estimated 40% of IT's time.

Some forms of Multi-Factor Authentication (MFA) still rely on passwords for one authentication factor. This approach has benefits but still incurs the downsides of passwords, particularly for hacker-led attacks.

A passwordless Multi-Factor Authentication approach is needed not only for security but also to maximize IT efficiencies.

Passwords Challenges

98% Of breaches could be prevented by the right kind of MFA

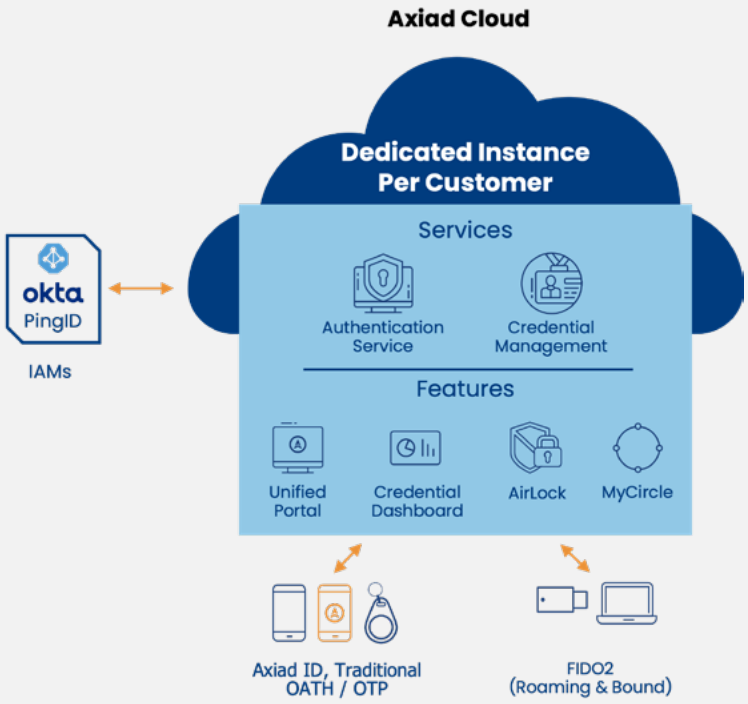
89% Use 3 or more authentication methods

52% Of employees find workarounds to overly complex security

Product Overview

Leveraging the power of the Axiad Cloud, Axiad Multi-Factor Authentication (MFA) provides consolidated, consistent, and efficient passwordless and phishing-resistant MFA for end users. With support for a variety of tokens and FIDO2, Axiad MFA delivers enterprise-grade phishing-resistant authentication at scale and everywhere it's needed. Axiad MFA helps organizations efficiently address end user security and compliance requirements, particularly for remote and/or hybrid workers.

Enterprise-grade Multi-Factor Authentication



How Axiad MFA is unique

- **Consolidated:** A single approach serves all end user needs, everywhere across the environment
- **End-to-end Security:** All entities are secured without passwords or shared secrets
- **Unified view of all credentials:** Unified portal provides a single pane of glass for managing all end user credentials
- **Broad token support:** A wide range of tokens are supported as well as physical / virtual token consolidation
- **Secure Design:** Architected for best-practices security including isolation by customer, encrypted communications, and key storage in specialized hardware

Key Features

Consolidated: Serves all authentication needs, everywhere across the environment

- **End-to-end Security:** All entities are secured without using passwords or shared secrets so the authentication process is secure from end-to-end
- **Passwordless Multi-Factor Authentication (MFA):** Utilizes multiple types of authentication methods without a password or push notification that can be intercepted or phished
- **Phishing-Resistant Authentication:** Delivers a broad range of phishing resistant authentication based on FIDO2 and WebAuthn with multiple enterprise-grade Authenticators

Consistent: Ensures consistent authentication across OSs, applications, services, and more

- **Broad OS support:** Secures Microsoft Windows, Apple OSs, Linux, and more
- **Windows-friendly:** Provides authentication across Windows ecosystem including Azure, Windows Hello for Business, Windows OS, and more
- **Token Side-by-Side support:** Leverages a wide array of physical and virtual tokens side-by-side
- **Integrated:** Supports wide range of protocols, connectors, and standards for interoperation across the Identity ecosystem out of the box

Efficient: Increases IT and end user efficiencies at scale with automated, streamlined workflows

- **Unified view of all MFA credentials:** Manages all MFA credentials, including Azure AD's issued credentials such as WHFB and Microsoft Authenticator
- **Unified Portal:** Streamlines work and automates tasks for both IT and End Users across the organization
  - » **Single Pane of Glass:** Delivers all functionality including custom workflows for both IT and End Users
  - » **Airlock:** Provides help desk automation by eliminating temporary passwords, automating administration, and enabling self-service credential management
  - » **MyCircle:** Empowers self-service by enabling the workforce to issue department-level credential resets, thereby avoiding temporary passwords and increasing efficiency for IT and end users
  - » **Certificate Workflows:** Supports a range of certificate request and delivery workflows

Platform Capabilities: Leverages Axiad Cloud Platform capabilities including secure design, convenient implementation, and more.

Benefits

Move Beyond Passwords

Deliver better enterprise-wide security controls that go beyond passwords that are relatively simple to compromise

Automate MFA

Automate processes and checklists (e.g., completing security training and self-serving smart card setup) required for setup and edits

Protect the Hybrid Workforce

Ensure authentication is completed uniformly across all types of workers by requiring two or more verification factors

axiad

About Axiad

Axiad delivers organization-wide passwordless orchestration to secure users, machines, assets, and interactions for enterprise and public sector organizations that must optimize their cybersecurity posture while navigating underlying IT complexity. The company's flagship offering, Axiad Cloud, is a comprehensive, secure, and integrated authentication platform that allows customers to move to a passwordless future without the friction and risk of fragmented solutions. Axiad supports the widest range of credentials in the industry including FIDO, mobile MFA, Windows Hello for Business, YubiKeys, smart cards, TPM and biometrics.