Axiad and Okta
SOLUTION OVERVIEW

Securely and easily access workstations and applications

Okta's single sign-on (SSO) provides organizations with access to all their business applications in one location. Axiad Certificate-Based Authentication (CBA) for IAM provisions and manages phishing-resistant authenticators and credentials even at scale without changing how Okta authenticates end users. IT can incorporate phishing-resistant CBA to enable end users to securely access their workstation, then log into Okta-managed applications via SSO. By integrating Okta with Axiad Cloud, organizations can benefit from a more comprehensive identity and access management solution with advanced security features, streamlined identity management processes, and an improved user experience.

Complement Okta's login offerings

Implement Seamless Authentication

Log in to your workstation with a provisioned YubiKey or personal identity verification (PIV) card to access all your Okta-managed applications with certificate-based authentication.

Enhance Security with Cloud-based Authentication

Provide cloud-based certificate and credential management to enable Okta web sign-in with smart card/PIV, enabling passwordless and phishing-resistant MFA for any Okta-managed application.

Reduce End User Friction

Secure your workstation without needing multiple forms of authentication or resource-intensive agents. Ensure MFA is set up before an employee can gain full access to company systems with Axiad's authentication management capabilities.

Meet Government Compliance Requirements

Enforce phishing-resistant multi-factor authentication (MFA) with certificate-based authentication, an essential part of the U.S. Executive Order to adopt a Zero Trust architecture.

Provide Secure and Unified Login for Okta User Accounts

Sequence

1. End user authenticates to their workstation via Windows Hello for Business, YubiKey, or smart card/PIV card.
2. The smart card service sends a request to the organization's domain controller to validate the certificate.
3. If the certificate is valid, the workstation's operating system will authenticate the end user.
4. After authenticating to the operating system, the end user can use the same certificate provisioned to their smart card to access any Okta-managed resources or applications that they are authorized to use based on their Okta Organization's configurations.

A Censuswide authentication survey report concluded:

35%

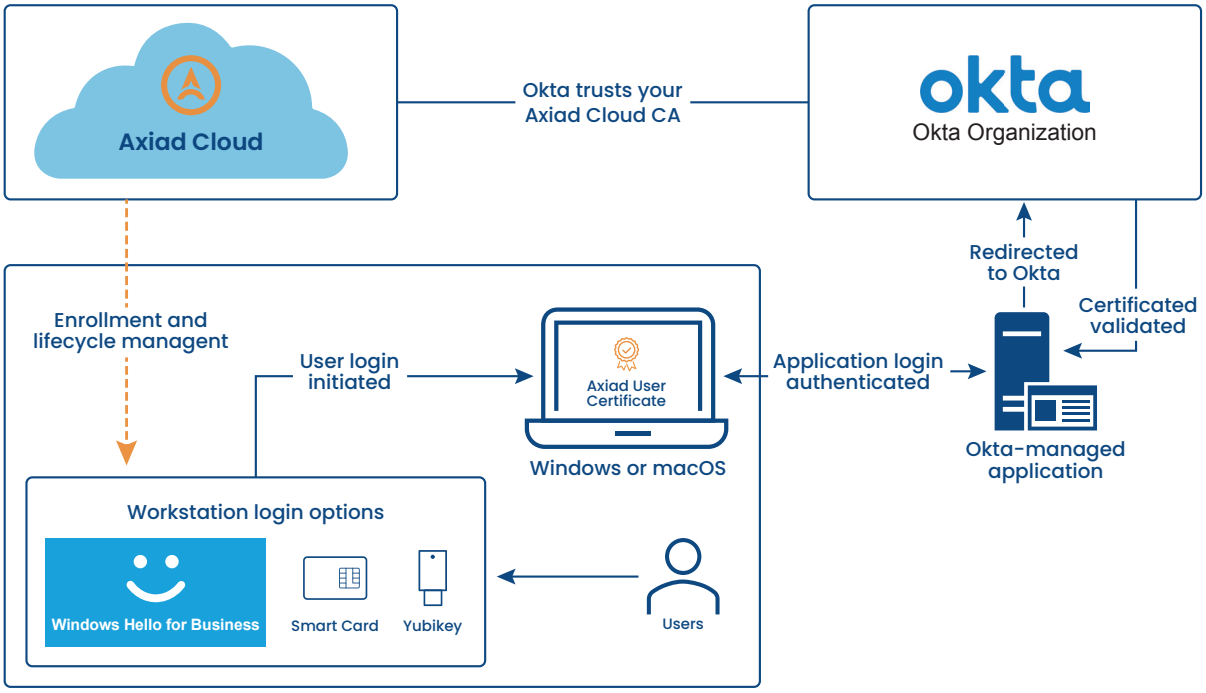
35% use 7 different authentication methods across their organization

52%

52% find workarounds to overly complex security

98%

98% of breaches could be prevented by the right MFA



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.