TECHNICAL BRIEF

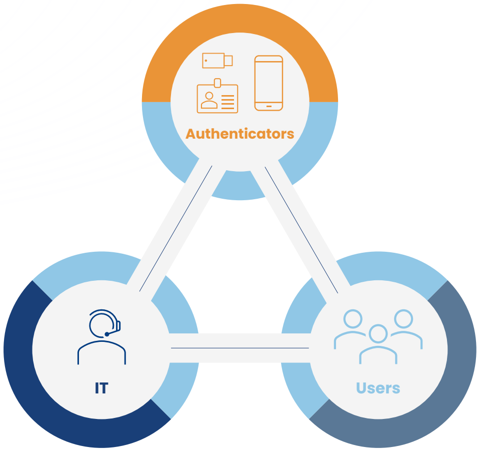
AXIAD

Authentication Management at Scale

OVERVIEW OF USE CASE

As many a CISO has observed, even the best security fails when end users won't tolerate it and IT doesn't have the cycles to make it work. Methods such as FIDO and Certificate-Based Authentication provide rigorous phishing-resistant authentication. So, what is keeping organizations from widespread adoption?

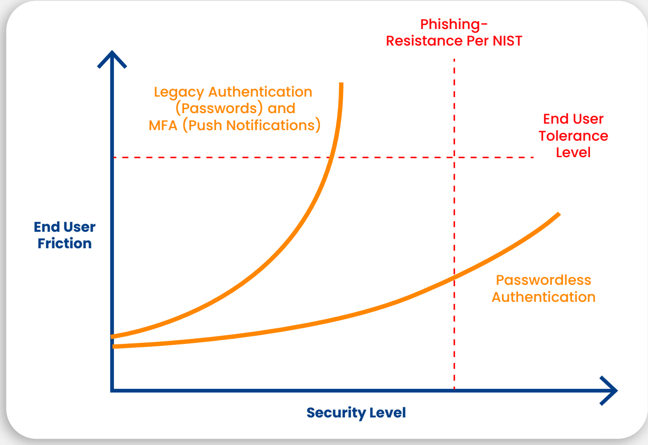
The answer is authenticators and associated credentials involve high manual effort for IT to manage. At scale, management of authenticators and credentials ("Authentication Management") is prohibitive when factoring in issuance, account recovery, renewal, and revocation efforts: across the lifecycle. Existing identity products, while providing authentication for end users, do not provide these capabilities.



CHALLENGES AT SCALE

Authentication Management challenges are significant and can break the organization's back at scale.

- **End User Experience:** Today, organizations are pinned between the high friction of legacy authentication (passwords) and legacy MFA (push notifications) versus the difficulties in provisioning phishing-resistant authentication. This friction often leads to end users circumventing authentication security or resisting new methods of authentication. So, end user experience must be addressed:
  - **Security Levels:** Security must be tailored to the security requirements and needs of each end user group.
  - **Provisioning:** Provisioning for end users must be convenient and efficient.
  - **Self-Service:** Key needs such as account recovery and renewals must be self-service rather than subject to help desk delays.
- **IT Oversight:** Due to authentication siloes by Operating System, IAM, etc., IT is not able to visualize the state of authentication management. To do so, IT needs new capabilities:
  - **Unification:** Authentication siloes must be bridged by a unified approach.
  - **Visibility:** The overall state of the authenticator and credential rollout and current status must be visible.
  - **Lifecycle Management:** IT must be able to manage authenticators and credentials as a lifecyle that can efficiently handle provisioning and renewals at scale.
- **IT Resource Limits**: A recent whitepaper calculates that each end user authentication provisioning request takes approximately 30 minutes to complete.[1] At scale, IT teams simply do not have the resources to manage multiple, complex, and unique authentication systems manually. IT needs a unified approach with built-in efficiencies to roll out and manage phishing-resistant authentication.

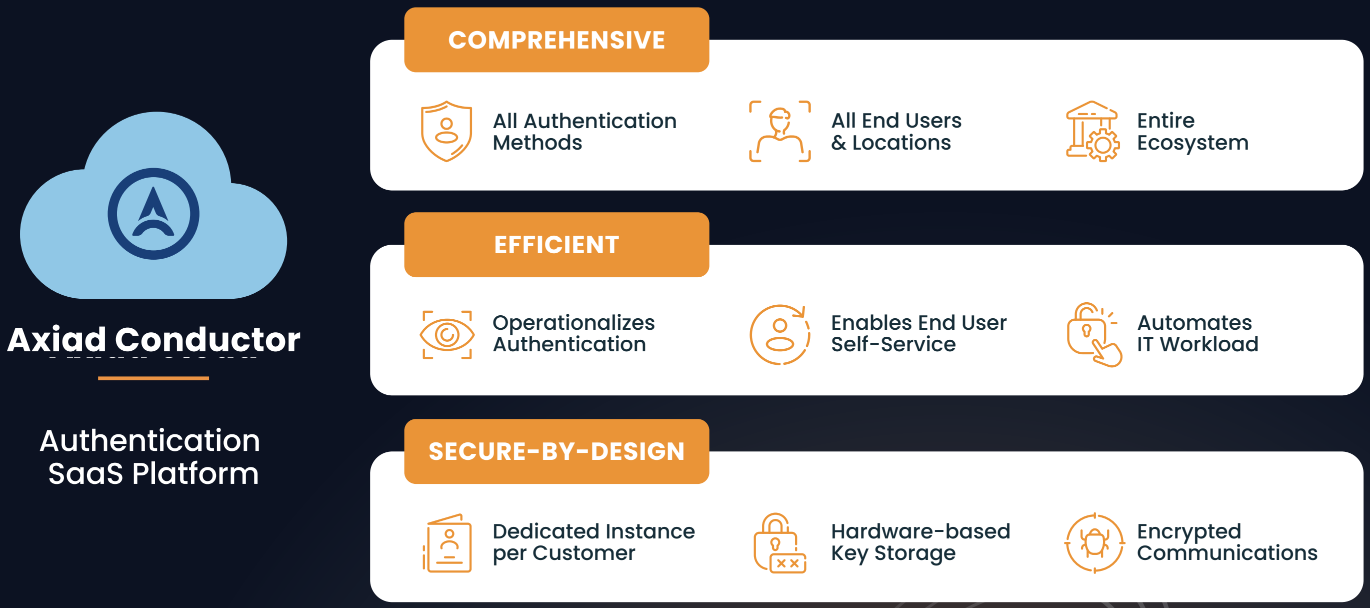


Summing up, clearly IT cannot survive without systematic Authentication Management, including end user self-service where it does not compromise overall security.

INTRODUCING AXIAD CONDUCTOR

Overview

Axiad Conductor is a comprehensive, efficient, and secure authentication SaaS platform that eliminates silos across the environment. Architected for best-practices security, it enables "mix-and-match" use of the Axiad Conductor product line. It can be applied in heterogeneous IT environments – e.g., organizations operating Windows, Mac, and Linux operating systems or with multiple existing IAM systems in place – allowing organizations to remove gaps and inconsistencies in how they authenticate across complex ecosystems, and ultimately to become more programmatic in their overall cybersecurity practices.



Axiad Conductor

Authentication SaaS Platform

COMPREHENSIVE

- All Authentication Methods
- All End Users & Locations
- Entire Ecosystem

EFFICIENT

- Operationalizes Authentication
- Enables End User Self-Service
- Automates IT Workload

SECURE-BY-DESIGN

- Dedicated Instance per Customer
- Hardware-based Key Storage
- Encrypted Communications

Capabilities

- **Comprehensive:** Supports all authentication methods across users, machines, and more while interoperating with the entire Identity ecosystem
- **Efficient:** Streamlines and automates help desk workload, enables end user self- service, and minimizes overall IT overhead
- **Secure-by-Design:** Architecture designed with best-practices security including a private instance for each customer, key storage in specialized hardware, and encrypted communications.

HOW AXIAD HELPS YOU

Overview

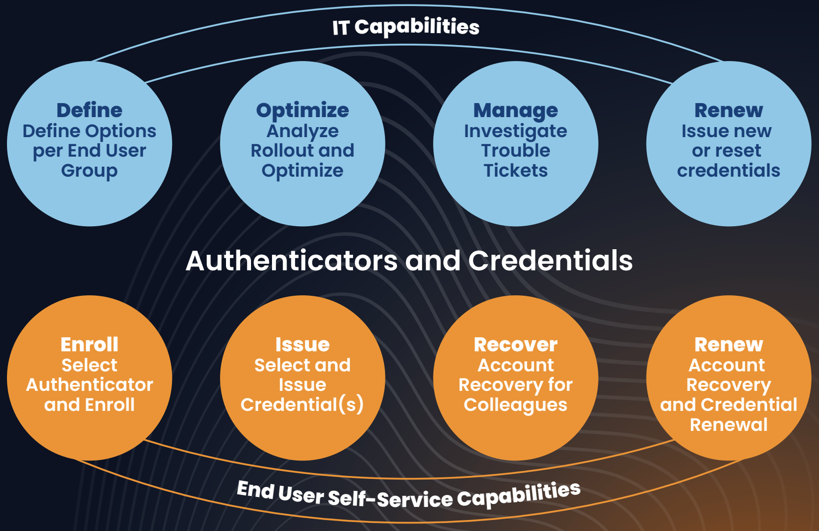
Axiad's SaaS Conductor Platform operationalizes an **Authentication Management Lifecycle** at scale:

- Tens of thousands of End Users
- Complex global environments with multiple OSs and on-premises / web applications
- Multiple IAM systems
- Broad range of Authenticators
- Broadest range of Credentials on the market today
- All major Authentication methods

TO ACCOMPLISH THIS MISSION, AXIAD PROVIDES AUTHENTICATION MANAGEMENT LIFECYCLE FOR BOTH IT AND END USERS:

- **IT capabilities:**
  - **Define** the authenticator options and corresponding credentials
  - **Optimize** the Rollout of MFA across the organization
  - **Manage** any incidents
  - **Renew** with new or reset credentials
- **End User capabilities:**
  - **Enroll** the authenticator(s) of choice
  - **Issue** credentials onto the authenticator
  - **Recover** colleagues' accounts without IT intervention
  - **Renew** credentials either for account recovery or at expiration

Authentication Management Lifecycle at Scale


IT Capabilities
Define
Define Options per End User Group
Optimize
Analyze Rollout and Optimize
Manage
Investigate Trouble Tickets
Renew
Issue new or reset credentials
Authenticators and Credentials
Enroll
Select Authenticator and Enroll
Issue
Select and Issue Credential(s)
Recover
Account Recovery for Colleagues
Renew
Account Recovery and Credential Renewal
End User Self-Service Capabilities

The lifecycle can be broken down by main processes:

1. Provisioning by IT and End Users
2. Authentication Management Lifecycle — IT
3. Authentication Management Lifecycle — End Users.

1. Provisioning by IT and End Users

Once IT defines the authenticators and credentials by end user group, provisioning tasks (enrollment of authenticator and issuance of credentials) are self-service.

Define

IT sets up the list of authenticators (such as YubiKeys, Smart Cards, Windows Hello for Business, Axiad ID mobile authenticator, and more) that are allowed for the organization overall and for each group of users as needed. IT also specifies the credentials that are allowed such as X.509 Certificates, OTP, FIDO2, and more.

Enroll

Once setup is done, all provisioning operations can be self-service by end users. Where allowed by IT, the end user can select the authenticator from the pool and enroll it with Axiad.

Issue

When the credential is requested, it is then automatically issued and stored on the selected authenticator.

Initial Setup

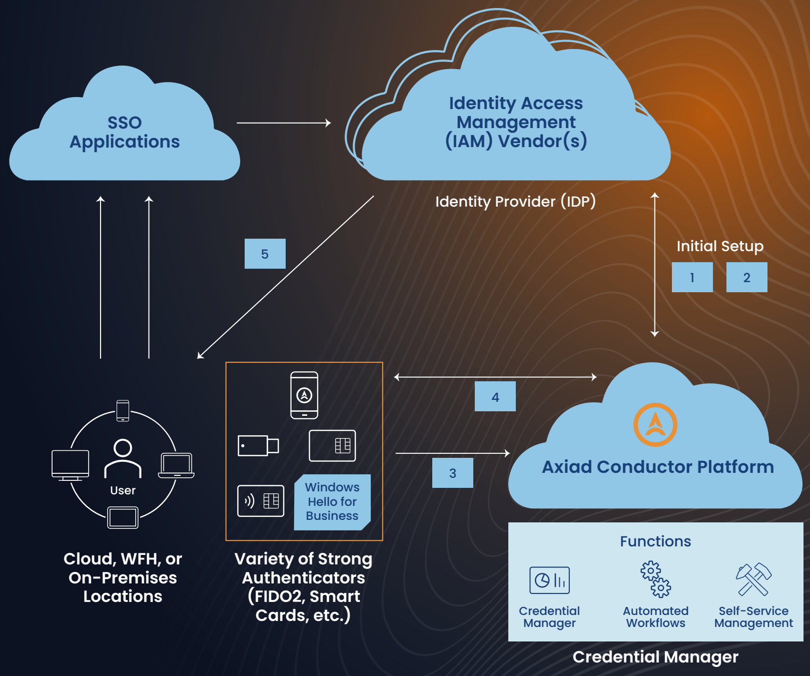
1. Axiad Conductor and Identity Provider synchronize End User identities
2. IT provides list of authenticators and credentials permitted for each End User group

Self-Service Provisioning

3. End user self-services authenticator enrollment and requests credential
4. Axiad issues credential and stores on authenticator

Existing Authentication Process (Unchanged - Axiad is not in path)

5. Process of authentication is unchanged as Axiad is not in authentication path (authentication 2.



Authentication Management Lifecycle by End Users

Recover

When Account Recovery is needed, Axiad enables self-service based on user groups. Leveraging policies defined by the IT team, colleagues within a defined “circle of trust” are authorized to reset each others’ credentials. Productivity savings include time spent on the phone with Help Desk, Help Desk’s time, and of course delays when outside of normal working hours.

Renew

Credentials must be periodically renewed per the organization’s and/or the service provider’s policies. Axiad prompts the End User to renew or revoke the credential without needing IT intervention. As a result, end users more efficiently manage their credentials and so minimize disruptions due to expired credentials.

3. Authentication Management Lifecycle by IT

Optimize

Because of consolidating authenticator and credential management into a single platform, IT gets actionable visibility into the rollout of authenticators and credentials. Axiad tabulates end users by authentication method such as UserID / Password, Legacy MFA (Push Notifications), and MFA (CBA, FIDO2, and more). As a result, IT can efficiently roll out authentication to groups of end users. Optimization, such as deciding which groups of end users should leverage strong authenticators such as YubiKeys and Smart Cards, can then be performed by IT. Status of the rollout is tracked so that IT can view progress and adjust as needed.

Manage

When End Users report issues that they cannot resolve via self-service, Axiad’s Unified Portal enables IT to investigate the issue and take the appropriate action such as issue a new authenticator, reset a credential, or report the issue for further investigation.

Renew

Just as for initial rollouts, Axiad utilities enable IT to roll out new credentials or to renew existing across the end user base.

ORGANIZATIONAL OUTCOMES

Strong positive outcomes are driven by Axiad's approach:

- **Increased application deployment speed:** Today, authentication must be designed, deployed, and tested for each custom and vendor application and across the environment. With a unified authentication management approach, a new application just needs to specify the authentication needed and risks and bottlenecks are addressed as part of ongoing Authentication Management operations.
- **Match Security Spend to Business Need:** An outcome of authentication optimization is that the security level and corresponding spend can be matched to the business need. Instead of a one-size-fits-all authentication approach, each business group gets the security that they need.
- **Improve End User Satisfaction:** Passwordless authentication, despite embodying a more rigorous level of security, is much easier to execute for end users. As a result, end user satisfaction will increase – a win-win for IT!
- **Increase End User Efficiencies:** Eliminating the time that end users spend on password lookup and on hold with Help Desk measurably increases the efficiency of all end users – including the exec team. A key metric from a security behavior report indicates that end users spend over 12 minutes per week just finding and resetting passwords – with a total cost per organization of over $5.2 million per year.[2]
- **Maximize IT / Help Desk Leverage:** Axiad transforms authentication management into an ongoing activity that can be optimized, can be scheduled for major items such as implementing a new authenticator, and can be made radically more efficient as compared to today's ad-hoc approaches.

UNIQUE AUTHENTICATION MANAGEMENT CAPABILITIES

As of this writing, Axiad's approach provides capabilities that cannot be matched elsewhere:

- **Authentication Can Be Operationalized:** Operations teams can treat authentication management as any other operational process and lifecycle.
  - Actionable Visibility: The state of authentication rollouts across the environment is visible and actions that can shape the rollout are known.
  - Predictable events and intervals: Authentication management is treated as a lifecycle with known events (renewals and revocations) at given intervals for action (such as at credential renewal or at end of lifecycle).
- **Security optimized to business need:** Security level and corresponding costs can be matched to business need.
  - Robust Authentication Options: The broadest range of authentication methods, authenticators, and credentials across the broadest environment are managed by a single platform, eliminating siloes and reducing the chances of a breach.
  - End User Control / Satisfaction: End User control is maximized by low-friction processes and control over credentials for themselves and for co-workers.
- **Lifecycle Efficiencies:** Every step of the lifecycle is made more efficient for both IT and End Users.
  - IT efficiencies: Maximized since formerly one-off manual processes are instead offloaded via self-service or automated via purpose-built utilities.
  - End User efficiencies: Features are optimized for end user convenience and overall security.

BENEFITS FOR THIS USE CASE

End User Satisfaction

With guided, efficient, and consistent authentication management, end user satisfaction is maximized – at all levels of phishing resistance

Business-Justified Security

By matching the authentication level to the need, security is overall efficient and appropriate to the job function being performed

Operationalized Authentication

Unlike today, authentication management can be managed as an IT operational set of processes that are predictable, replicable, and measurable

1. Okta, "Top 5 Reasons to Automate Identity Lifecycle", https://www.okta.com/resources/whitepaper/top-5-reasons-to-automate-identity-lifecycle/.

2. Yubico, "2019 State of Password and Authentication Security Behaviors Report", 2019 State of Password and Authentication Security Behaviors Report (yubico.com), 1/28/2019.