Passwordless for Air Gapped and Critical Environments

BROCHURE

Challenges

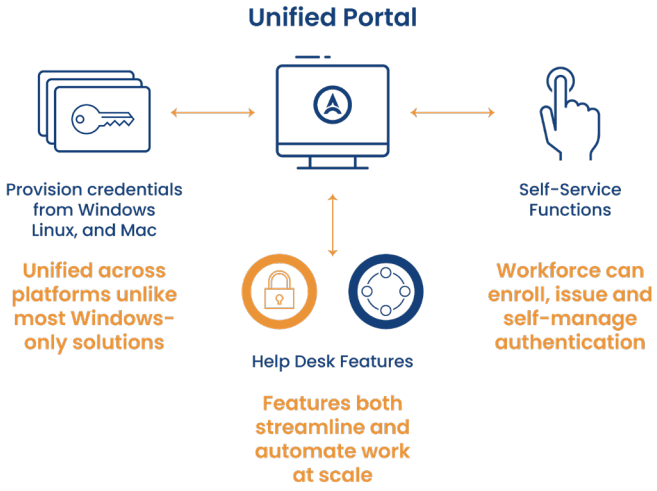
As exemplified from the Colonial Pipeline and other attacks, critical infrastructure (water, natural gas, and transportation) organizations, government agencies, and defense contractors are a target for threat actors. Due to the high stakes of a compromise, strong multifactor authentication (aka "passwordless MFA") is a requirement for government agencies. The White House Executive Order (EO) 14028 on Improving the Nation's Cybersecurity[i] and Fact Sheet[ii] also recommend passwordless MFA for critical infrastructure organizations. Critical infrasructure systems operate in a unique fashion as compared to enterprise datacenters:

- **On-premises, Air Gapped Environment:** Many of these systems operate in air gapped environments either due to security or to practical considerations such as not having network access on a remote drilling platform.
- **Specialized Systems:** These systems include Operational Technology (OT), specialized hardware and software that monitors or controls industrial equipment, assets, processes and events.[iii]
- **Production-centric:** These systems are optimized to control ongoing operations rather than transactions. As such, they are highly complex and changes are both difficult and expensive to implement.
- **Rugged Conditions:** As conditions are often extreme as seen on ships, drilling platforms, and other locations, authentication needs to support physical authenticators such as PIV cards, Smart Cards, and YubiKeys.
- **Lack of IT Support:** Air gapped and remote locations frequently have limited onsite IT support.

Product Overview

Axiad Unified Credential Management System (UCMS) provides unified, consistent, and efficient credential management for end users. A UCMS package, Passwordless for Air Gapped and Critical Environments, is deployed as an airgapped on-premises offering for critical infrastructure organizations, government agencies, and defense contractors. With support for strong authentication credentials across the organization, the product automates lifecycle credential management at scale. The package helps organizations with very high security needs or very significant on-premises application investments to achieve passwordless authentication seamlessly.

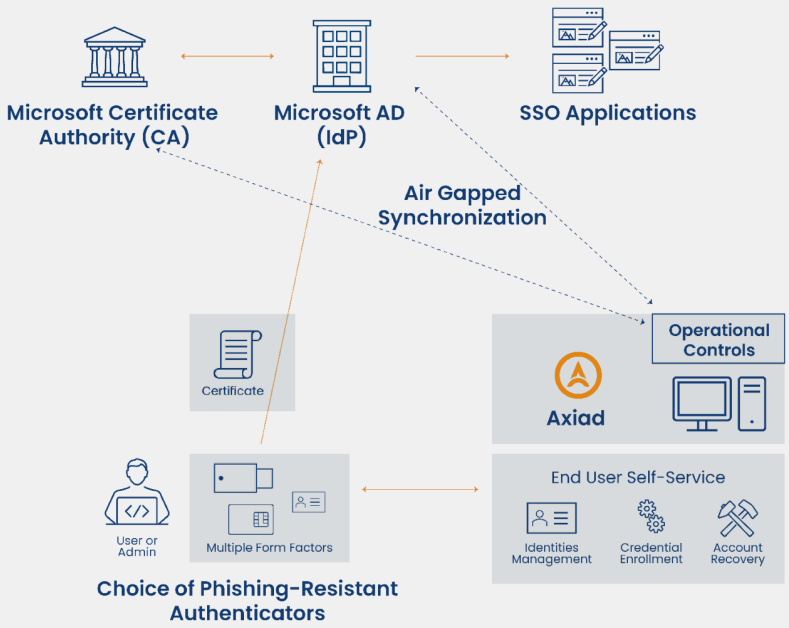
User Authentication Credential Management



Unified, Consistent, and Efficient end user authentication management lifecycle, deployed as an on-premises product

- **Unified:** A single package manages all end user authentication credentials throughout their lifecycle.
- **Consistent:** Credentials are consistent across OSs, applications, services, and more.
- **Efficient:** Unified Portal streamlines and automates workload for IT and end users

How It Works



Initial and Ongoing Operations

- Installation and operations are offline and air gapped
- Syncs with Microsoft CA and Microsoft AD via air gapped network only

Authentication is Unchanged

- End user self-services enrollment of authenticator(s) and provisioning of credential(s)
- Passwordless authentication is fully enabled without modifying how authentication is performed by Microsoft AD

Unique Credential Management Capabilities in Air Gapped and Critical Environments

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

- **Air gapped Operations:** Provides full functionality while isolated from public-facing networks.
- **Non-disruptive:** Does not require changes to existing authentication systems, either for the workstation or applications.
- **Unified:** A single approach serves all end user authentication credentials, everywhere across the environment.
- **Consistent:** Credentials are consistent across OSs, applications, services, and more.
- **Efficient Credential Management:** Passwordless deployment and account recovery processes are highly efficient.
- **Unified Portal:** Provides a single pane of glass for Users and IT with utilities that both streamline work and automate tasks.
- **Self-Service Features:** Features such as AirLock and MyCircle empower the workforce to enroll, issue, and self-manage their authenticators and credentials.

Features

Unified: Serves all credential needs, everywhere across the environment

- **Broad Authenticator / Credential support:** Supports dedicated physical (such as PIV card and USB Key) and platform (such as Virtual Smart Card) authenticators and credentials
- **Standards-based Certificate:** Leverages an international standard X.509 certificate to interoperate across a broad range of vendor products, compatible with the PIV card

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

- **Broad OS support:** Provisions credentials from Microsoft Windows, Apple OSs, Linux, and more
- **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 utilities

- **Unified view of all MFA credentials:** Manages phishing-resistant MFA credentials
- **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 utilities 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 Utilities:** Supports a range of certificate request and delivery utilities

Supported Environments:

- Can be deployed on Windows or Linux Operating system
- Operates in air gapped environments

Technical Specifications

Vendor Product	Supported Versions
Server OS	• Windows Server • Linux RedHat/Centos, Ubuntu
Hypervisors	• Microsoft Hyper-V • VMware ESXi • Citrix Hypervisor • Oracle VirtualBox
Client OS	• Windows 10/11 • macOS
Browsers	• Microsoft Edge • Google Chrome
Credentials	• Gemalto IDPrime MD 830, MD 930 • IDEMIA PIV 8/8.1 • Virtual Smart Card • YubiKey 4/5

Technical Specifications – continued

Vendor Product	Supported Versions
Hardware Security Modules	• Utimaco CryptoServer • Thales Luna
Certificate Authorities	• Microsoft Certification Authority • PrimeKey EJBCA • HID IdenTrust • Idnomic PKI (formerly OpenTrust)
Database	• Microsoft SQL Server • MySQL • Oracle DB • PostgreSQL
Identity Provider	• Any SAML/Oauth + SCIM capable IdP, including but not limited to Microsoft Active Directory and Microsoft AD FS
Compliance and Standards	• FIPS 201, FIPS 140-2, NIST SP800-171, NIST SP800-63B

Benefits

Instant Passwordless

Government-grade phishing-resistant passwordless authentication can be added seamlessly

Air Gapped Operations

Supports air gapped environments with key functional and operational capabilities

Increased Investment Life

Upgrades authentication and infrastructure investments to extend their life

[i] White House Executive Order (EO) 14028: Executive Order on Improving the Nation's Cybersecurity, May 12, 2021.

[ii] White House Executive Order (EO) 14028 FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks, May 12, 2021.

[iii] Gartner: Gartner Glossary, Operational Technology (OT)