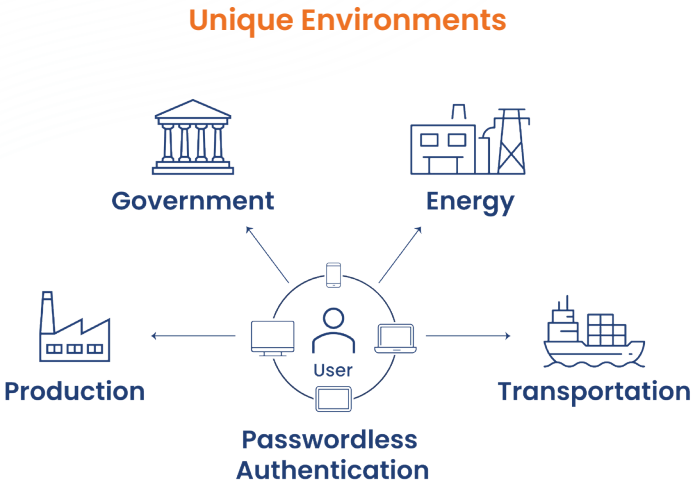
AXIAD

Passwordless for Air Gapped and Critical Environments

OVERVIEW OF USE CASE

Government agencies, critical infrastructure organizations, and defense contractors are automating monitoring, detection, and production controls with increasingly sophisticated systems. However, these advances are accompanied by a cost: geometric increase in the security exposure surface and in potential downsides (such as operational disruption) should threat actors compromise the system.

To minimize exposure, these "frontline" (using the Gartner term[1]) systems are implementing air gapping via a production network that is fully isolated from public networks. Due to the high stakes of a compromise, strong passwordless authentication is required for government agencies by the White House Executive Order (EO) 14028 on Improving the Nation's Cybersecurity[2] and Fact Sheet[3] for these systems.



Strong passwordless authentication in air gapped and critical infrastructure environments presents unique challenges for authentication management. Government agencies, critical infrastructure organizations, and defense contractors need passwordless authentication management that overcomes these challenges while leveraging current on-premises environments.

Challenges

As they cannot leverage cloud-based Identity products – such as Microsoft Entra ID or Identity and Access Management (IAM) products – air gapped environments present unique challenges for authentication management:

- **Fully Air Gapped Operations:** Must be installed, maintained, and run without a network connection.
- **Passwordless Authentication:** To provide passwordless phishing resistant authentication, support for dedicated physical (such as PIV card and USB Key) and platform (such as Virtual Smart Card and passkey) authenticators and credentials must be provided.
- **Authenticator Options:** A recent Gartner report indicates that many frontline environments (oil rigs, manufacturing, and even retail) prohibit the use of smart phones.[4] To span a wide range of device readers, multiple authenticator form factors must be supported.
- **Stringent Authentication Needs:** To comply with security standards, need to authenticate to workstation prior to application authentication.
- **Leverage On-premises Environment:** An authentication management approach must leverage the current on-premises environment.

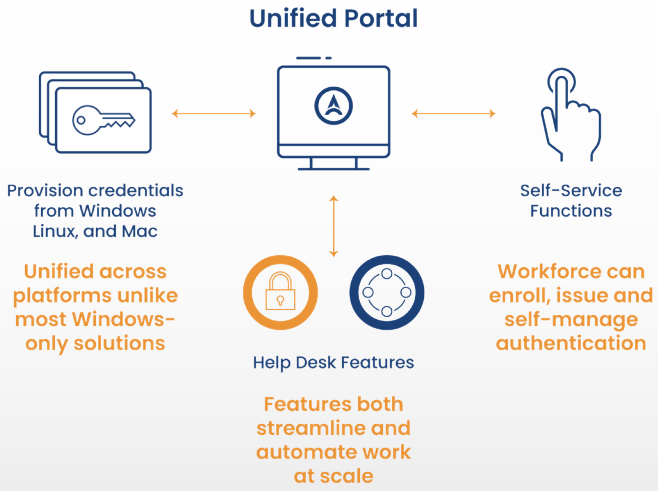
- **Limited IT Support:** The system must operate without reliance on on-site IT or extensive Help Desk support.
- **End User Manageability:** The system must minimize end user friction via usability and self-service capabilities.

Unique Requirements of Air Gapped Environments Lead to Unique Challenges

Introducing Passwordless for Air Gapped and Critical Environments

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 air gapped on-premises offering for critical infrastructure organizations, government agencies, and defense contractors. With support for strong authentication credentials across the organization, the package handles the authentication management lifecycle at scale. The package helps organizations with very high security needs or very significant on-premises application investments to achieve passwordless authentication seamlessly.

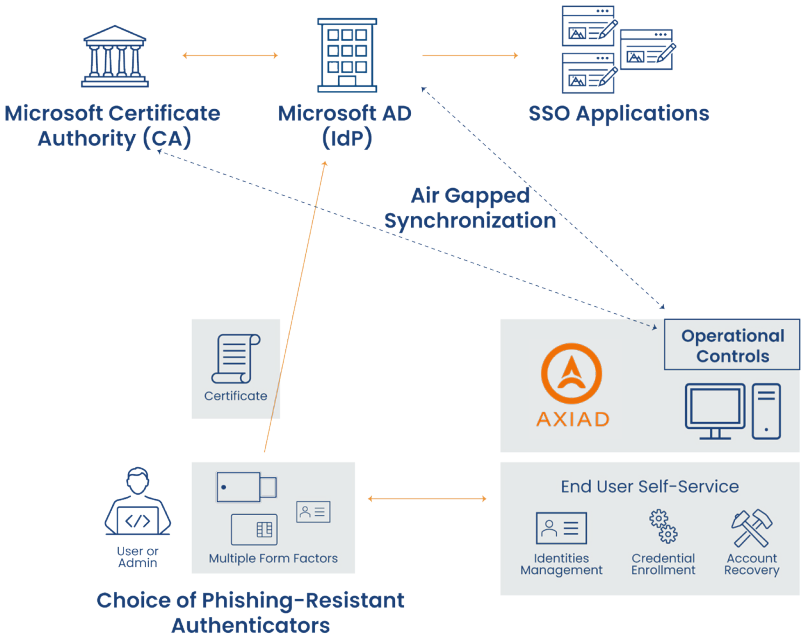
User Authentication Credential Management



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

Passwordless for Air Gapped and Critical Environments is architected for air gapped on-premises environments. Initial installation and updates are performed from a thumb drive. The package enables passwordless authentication across the existing on-premises environment including Microsoft AD, Microsoft CA, and more.



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

Meeting the Needs

Passwordless for Air Gapped and Critical Environments fully meets the needs of air gapped environments for government agencies, critical infrastructure organizations, and defense contractors.

- **Fully Air Gapped Operations:** Must be installed, maintained, and run without a network connection.
  - Passwordless for Air Gapped and Critical Environments has proven success in running in air gapped environments. It does not require a public connection to operate. Onsite personnel can maintain the package intermittently by installing updates from a thumb drive.
- **Passwordless Authentication:** To provide passwordless phishing resistant authentication, support for dedicated physical (such as PIV card and USB Key) and platform (such as Virtual Smart Card) authenticators and credentials must be provided
  - The package supports a full range of authenticators including dedicated physical (PIV card, Smart Card, and USB Key) and platform (Virtual Smart Card) authenticators and credentials. Certificatebased approaches such as Certificate-Based Authentication (CBA) are also supported.
- **Authenticator Options:** To span a wide range of device readers, multiple authenticator form factors must be supported.
  - As discussed above, many frontline environments prohibit the use of smart phones and not all machines are able to read each authenticator. As a result, authentication must support a full range of authenticators. Passwordless for Air Gapped and Critical Environments enables multiple authenticators, each with different credentials to be assigned and managed per end user. That way, any mix of ongoing and temporary (project-based) authentication can be managed.
- **More Stringent Authentication Needs:** To comply with security standards, need to authenticate to workstation prior to application authentication.
  - Many existing authentication approaches do not encompass workstation authentication. A security gap is the result since the workstation is not secured with a passwordless, phishingresistant authenticator. Passwordless for Air Gapped and Critical Environments includes an AirLock feature that ensures that the end user has set up the authenticator prior to being able to access applications. Further, AirLock ensures that the end user authenticates to the workstation each time prior to being able to access applications either standalone or via SSO (via Microsoft AD).

- **Leverage Current Environment:** An authentication management approach must leverage the current on-premises environment.
  - The on-premises ecosystem is a different software stack from the cloud ecosystem and typically leverages the Microsoft ecosystem. Passwordless for Air Gapped and Critical Environments fully leverages Microsoft AD, Microsoft CA, Windows Server, and other components of the on-premises environment to ensure authentication is highly secure and consistent, all without requiring upgrades.
- **Limited IT Support:** The system must operate without reliance on on-site IT support.
  - Since the system must be able to operate without reliance on on-site IT support, Axiad provides upgrades and maintenance via thumb drives that can be installed by local personnel. Axiad support provides real-time guidance for installing upgrades and maintenance.
- **End User Manageability:** The system must minimize end user friction via usability and self-service capabilities.
  - Since IT is typically not onsite in air gapped environments, end users must be able to self-service authentication management. Passwordless for Air Gapped and Critical Environments includes the AirLock and MyCircle features. These features enable the entire Credential Enrollment and Account Recovery (CEAR) lifecycle to be self-serviced by the End User. The End User can select one or more authenticators and enroll the appropriate credentials (such as FIDO passkeys and Certificates) on each. Thereafter, AirLock provides reminders to renew credentials via the Axiad Unified Portal. Finally, MyCircle ensures account recovery can be performed by getting approval from a designated "circle of trust" rather than via a lengthy phone call to Help Desk.

Unique Authentication Management Capabilities

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.

Unique capabilities provide superior authentication management in air gapped environments

Benefits for this Technical Brief

Maximize Security

Passwordless authentication eliminates passwords that can be compromised and used in attacks

End User Acceptance

By providing end user selfservice and intuitive utilities, end user acceptance is maximized

Minimize Security Overhead

By streamlining effort for end users and IT, overall security and remediation overhead is minimized

---

[1] Gartner: How to Authenticate Frontline Workers, G00792741, June 2023

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

[3] 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.

[4] Gartner: How to Authenticate Frontline Workers, G00792741, June 2023

AXIAD

About Axiad

Axiad is an identity security company tackling the growing threat of compromised credentials, which drive over 70% of enterprise breaches. The sprawl of human and non-human identities across organization silos creates security blind spots that existing tools fail to secure. Axiad tackles this problem head-on, detecting identity risks and poor credential hygiene across systems, providing actionable insights, and enhancing security without needing a complete overhaul. Axiad makes identity simple, effective, and real. Discover more at axiad.com or follow us on LinkedIn.