

# Unified Credential Management System (UCMS)

## Brochure



### Challenges

Once an afterthought, credentials and keys are becoming increasingly important. As credential life has been shortened over time, outages due to certificate expirations have risen to over 81% of companies surveyed. Further, recovery costs from these outages is very high at an average of \$15 million.

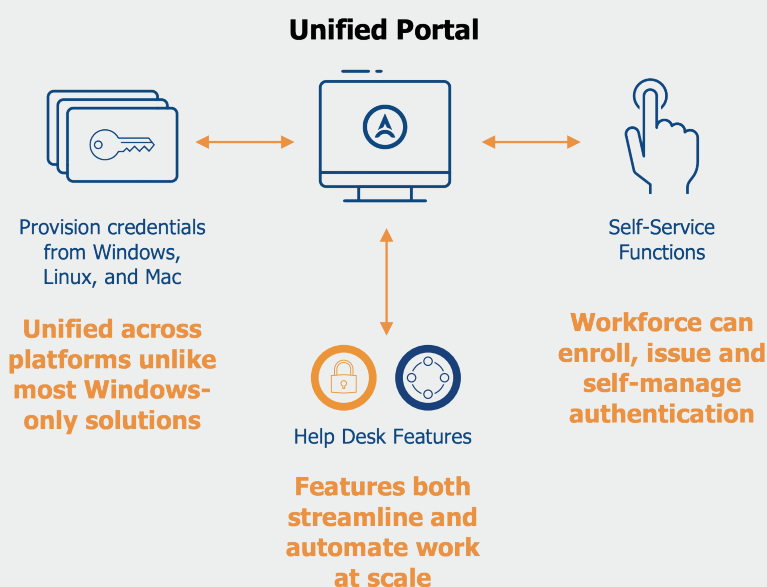
Credential management for both end users and devices is a critical need for all organizations today. However, most credential management approaches are limited to a specific environment or OS.

A unified credential management approach is urgently needed for both enterprises and government agencies.

### Product Overview

Deployed as an on-premises offering, Axiad Unified Credential Management System (UCMS) provides unified, consistent, and efficient credential management for end users. With support for all authentication credentials across the organization, the product automates lifecycle credential management at scale and everywhere needed. Axiad UCMS helps large organizations with very high security needs or very significant on-premises application investments to enhance security while minimizing IT overhead.

### On-Premises User Authentication Credential Management



Unified across platforms unlike most Windows-only solutions

Features both streamline and automate work at scale

Provision credentials from Windows, Linux, and Mac




Self-Service Functions

Workforce can enroll, issue and self-manage authentication

Help Desk Features



### Credential Management Challenges

-  **53%** Companies who don't know how many certificates they have\*
-  **81%** Companies with cert expiration outage in 24 months \*\*
-  **\$15M** Average recovery cost from certificate outage\*\*\*

- ### How Axiad UCMS is unique
- 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 workflows 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:** Multiple features empower the workforce to enroll, issue, and self-manage their authentication tokens

## Key Features

**Unified: Serves all credential 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
- **Standards-based Certificate:** Leverages an international standard X.509 certificate to interoperate across a broad range of vendor products

**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 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

**On-premises Environment: Can be deployed on Windows or Linux Operating system**

## Technical Specifications

Vendor Product	Supported Versions
Server OS	<ul style="list-style-type: none"> <li>• Linux RedHat/Centos, Ubuntu</li> <li>• Windows Server</li> </ul>
Hypervisors	<ul style="list-style-type: none"> <li>• Microsoft Hyper-V</li> <li>• VMware ESXi</li> <li>• Citrix Hypervisor</li> <li>• Oracle VirtualBox</li> </ul>
Client OS	<ul style="list-style-type: none"> <li>• Windows 10/11</li> <li>• macOS</li> </ul>
Browsers	<ul style="list-style-type: none"> <li>• Google Chrome</li> <li>• Microsoft Edge</li> </ul>
Credentials	<ul style="list-style-type: none"> <li>• Gemalto IDPrime MD 830, MD 930</li> <li>• IDEMIA PIV 8/8.1</li> <li>• Virtual Smart Card</li> <li>• Windows Hello for Business</li> <li>• YubiKey 4/5</li> </ul>

## Technical Specifications – continued

Vendor Product	Supported Versions
Hardware Security Modules	<ul style="list-style-type: none"><li>• Utimaco CryptoServer</li><li>• Thales Luna</li></ul>
Certificate Authorities	<ul style="list-style-type: none"><li>• PrimeKey EJBCA</li><li>• Microsoft Certification Authority</li><li>• HID IdenTrust</li><li>• Idnomic PKI (formerly OpenTrust)</li></ul>
Database	<ul style="list-style-type: none"><li>• Microsoft SQL Server</li><li>• MySQL</li><li>• Oracle DB</li><li>• PostgreSQL</li></ul>
Identity Provider	<ul style="list-style-type: none"><li>• Any SAML/Oauth + SCIM capable IdP, including but not limited to Azure AD, Microsoft AD FS, Microsoft Active Directory, KeyCloak, and PingFederate</li></ul>
Compliance and Standards	<ul style="list-style-type: none"><li>• FIPS 201, FIPS 140-2, NIST SP800-171, NIST SP800-63B</li></ul>

## Benefits

### Attain Maximum Flexibility

Ready deployment on Windows, Linux, or Mac maximizes flexibility for your organization

### Future Proof Your Investment

Stay functional and in line with evolving mandates and new credential needs

### Streamline Workload

Streamline management across the lifecycle of multiple authentication methods

## Footnotes

\* State of Machine Identity Management Report, Ponemon, 2021, <https://www.keyfactor.com/state-of-machine-identity-management-2021/>

\*\* Report: 81% of companies experienced a certificate-related outage in the past two years, Venturebeat, 2022, <https://venturebeat.com/technology/report-81-of-companies-experienced-a-certificate-related-outage-in-the-past-two-years/>.

\*\*\* Why Expired Digital Certificates Have Become A Bigger Threat, SC Media, 2022, <https://www.scmagazine.com/perspective/cloud-security/why-expired-digital-certificates-have-become-a-bigger-threat%E2%82%AC>.



## 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.

