Power LogOn®

For Government (Online)

COTS IT- Centralized MFA



UEI: **X4CCM6HULMX6**
CAGE: **5AU22**
DUNS: **829366660**

Add Cyber Access Management

- ✓ COTS, true MFA solution
- ✓ Self-evaluated: Zero Trust, NIST CSF, SP 800-53, -63B, -171, CMMC L1, FIPS 201, 140-3.
- ✓ Uses existing CAC, PIV, PIV-I, CIV and TWIC cards as issued
- ✓ Uses the PIV or CAC credential with a Power LogOn PIN
- ✓ Secure IAM and ICAM
- ✓ IT-centralized management
- ✓ AD, LDAP, RDP, & VM compatible
- ✓ Installs in the cloud, on servers, or on stand-alone computers or workstations
- ✓ Typical installation time is less than two hours



Power LogOn works with existing employee ID badge systems

IT-Centralized Management

Employee-managed passwords are cybersecurity's weakest link, and Power LogOn closes that gap. It automatically enforces IT's security policies without any employee interaction.

Power LogOn gives IT the power to issue, replace or revoke employee Power LogOn credentials.

Easily integrates with Active Directory, LDAP, Terminal Services remote desktop (RDP) thin clients, and VPN connections.

Prevent Unauthorized Access

- ✓ **True Multi-Factor Authentication -** Card + PIN, card + biometric, or card + PIN + biometric
- ✓ **Users don't know or type passwords** - guards against social engineering, brute force, and many other attacks
- ✓ **Account addresses verified before auto-fill** - guards against spam and phishing attacks
- ✓ **Passwords are encrypted, salted and changed often -** guards against Pass-the-Hash attacks.
- ✓ **Auto-logoff when card is removed from reader** - Reduces network access vulnerability

Credential Convenience

Combining an enterprise password manager with a government-issued CAC/PIV/PIV-I/CIV ID badge for fast, easy security, lost-card discovery, and data breach management.

Power LogOn is a COTS on-premises solution that is ideally suited for IT environments requiring a high level of security where computers can be connected to networks and the internet.

- ✓ Customer specs with or without X.509 certificate requirements
- ✓ Works with standard smartcards, not just PKI-enabled cards
- ✓ High security level: AES-256 encryption plus SHA-256 hashing, with hash salting and optional TLS
- ✓ Works with contact and contactless Smartcards, mag stripe, and RFID technologies



Windows Logon Screen



Account Access Screen

Fast, Easy and Affordable

Can be tailored to the government's Zero Trust, CMMC and DFARS cybersecurity authentication requirements

Used by federal civilian agencies, DoW branches, state and local governments, and tribal governments.

Implements secure MFA, identity, access management, and identity card access management for online enterprise password security

Need certificate-based logon for air-gapped Windows workstations? See Power LogOn GOV-COA.

Power LogOn

Multi-Factor Authentication and Enterprise Password Management



General Information:

- ✓ **Primary Application:** Identity management, multi-factor authentication, and enterprise security
- ✓ **Secondary Application:** Strong passwords, safeguards against many hacker techniques
- ✓ **Operating System:** Windows 11 and earlier
- ✓ **Servers:** Windows Server 2025 and earlier; on-premises SQL Server 2025 and earlier
- ✓ **Clouds:** AWS, Azure, Google Cloud, or any other cloud supporting virtual machines
- ✓ **Web Browsers:** Auto-launch Edge, Firefox, and Chrome
- ✓ **Authentication factors:** Possession, Knowledge, Inherence, Encryption Keys, CUID, and Challenge/Response

Authentication & Security:

- ✓ Self-evaluation against: Zero Trust, CMMC Level 1, FIPS 201, FIPS 140-3, NIST CSF, SP 800-53, 800-171 and 800-63B
- ✓ Up to 500 character length passwords
- ✓ Identity, keylogger, and social engineering protection
- ✓ Phishing email protections
- ✓ Unlimited accounts stored in LDAP directories
- ✓ Password generator and configurator
- ✓ Change password reminder
- ✓ PIN and/or biometrics protection
- ✓ Four wrong PINs locks the account
- ✓ Up to 20-Character PIN Size
- ✓ Alpha, numeric and punctuation PIN character types
- ✓ Card data backup
- ✓ Works with Prox, 13.56 MHz Smartcard, NFC and more
- ✓ Card Removal Actions: User Log Off, Computer Lock Down, Computer Shut Down, Nothing, or Custom
- ✓ Secure card data printout
- ✓ Stored passwords: AES-256 encryption plus SHA-256 hashing, with hash salting
- ✓ Challenge/Response Authentication

Full Featured:

- ✓ Self-evaluated against: Zero Trust, CMMC Level 1, FIPS 140-3, FIPS 201, NIST Cybersecurity Framework, NIST SP 800-53, 800-171 and 800-63B.
- ✓ Third-party software API Integration
- ✓ CAC, PIV, PIV-I, CIV, & TWIC compatibility
- ✓ Add, view, edit and delete cardholders / Transaction and SIEM logging
- ✓ Security monitoring
- ✓ Database import and export / Supports Terminal Services
- ✓ Lost or stolen card hotlist
- ✓ Recycle cards and licenses
- ✓ Generate reports & recover card data
- ✓ IT Administrator PIN Reset

Enterprise Security:

- ✓ Windows bootup logon
- ✓ Network logon
- ✓ Auto-launch web browser
- ✓ Auto-fill user name and password, and submit
- ✓ Inter-/Intra-/Extra-net logon
- ✓ Auto-record internet passwords
- ✓ Auto-launch Windows applications
- ✓ Windows applications logon
- ✓ Unlimited accounts stored in Active Directory

System Requirements

Card Administrator

Operating System:
Windows® 11 and earlier

Server:
Server 2025 and earlier; on-premises SQL Server 2025 and earlier

The use of Virtual Server technology is recommended

Employee's Computer

Operating System:
Windows® Win11, and earlier

© ALL INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED "AS IS"; ACCESS SMART ASSUMES NO RESPONSIBILITY FOR ITS ACCURACY AND/OR COMPLETENESS. CONFIRM the trademark sentence is still right.. Power LogOn, Access Smart, and Powered by Smartcard Technology are registered trademarks licensed by Access Smart, LLC. All other trademarks and trade names are the properties of their respective companies. In no event will Access Smart be liable for damages arising directly or indirectly from any use of the information contained in this document.

4049 Northwood Pl • The Villages, FL 32163-2293 • Phone: (949) 218-8754

Smart Access Cyber Access Control