

Power LogOn[®]

For Government (Online)

COTS IT Centralized MFA

UEI: X4CCM6HULMX6
CAGE: 5AU22
DUNS: 829366660



Add Cyber Access Management

- ✓ COTS, true MFA solution
- ✓ Self-evaluation for Compliance: Zero Trust, CMMC-L1, FIPS 140-3, FIPS 201, DoW STIGs, NIST 800-53, 800-171, 800-63b AAL-3, and more
- ✓ No CAC/PIV/PIV-I/CIV rebadging, or re-configurations
- ✓ Can use existing government issued digital certificates, but not required
- ✓ Secure IAM and ICAM
- ✓ IT centralized management
- ✓ AD, LDAP, RDP, & VM compatible
- ✓ Installs in Cloud, Servers or stand-alone computers or workstations
- ✓ Typical installation time is less than two hours



Power LogOn works with existing employee ID badge systems

Credential Convenience

Combining enterprise password manager into a government issued CAC/PIV/CIV/PIV-I ID badge for fast and easy security, lost 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 internet.

- ✓ Customer specs with or without X509 certificate requirements.
- ✓ Does not require additional PKI infrastructure modifications
- ✓ High security level: AES-256 and Hash-256, Hash Salting, Secure cross-internet communications protocols
- ✓ Works with, contact, contactless smartcards, mag stripe, and RFID technologies

IT Centralized Management

Centralized password management fixes cybersecurity's weakest vulnerability: *User managed passwords!* It does this by automatically enforcing IT's security policies with any employee interaction.

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

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

Prevent Unauthorized Access

- ✓ **True Multi-Factor Authentication** - Something you Know (PIN), Have (Badge) and Are (biometrics)
- ✓ **Users don't know or type passwords** - guards against social engineering, brute force, and many other attack
- ✓ **Account addresses verified before auto fill** - guards against SPAM, phishing, and pharming attacks
- ✓ **Passwords are encrypted and salted** - guards against Pass-the-Hash attacks
- ✓ **Auto logoff when card is removed from reader** - Reduces network access vulnerability



Windows Logon Screen



Account Access Screen

Fast, Easy and Affordable

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

Used by Federal civilian agencies, DoW branches, State/Local governments, and tribal governments.

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

If you require certificate-based, offline authentication (COA), check out Access Smart's Power LogOn offline solution.



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, Windows 10, 8.x, and 7
- ✓ **Servers:** Win Server 2025, 2022, 2019, 2016 and SQL Server 2022 and 2017
- ✓ **Clouds:** AWS, Azure, Google, or any other cloud supporting Virtual Machine
- ✓ **Web Browsers:** Auto launch IE, Edge, Firefox, and Chrome browsers
- ✓ **Authentication factors:** Possession, Knowledge, Inherence, Encryption Keys, CUID, and Challenge/Response

Authentication & Security:

- ✓ Self evaluation for FIPS 140-3, NIST 800-63b compliance
- ✓ Up to 500 character length passwords
- ✓ Identity, Keylogger, and Social Engineering protection
- ✓ Phishing and Pharming E-mail protections
- ✓ Unlimited number of accounts stored in LDAP directories
- ✓ Password generator and configurator
- ✓ Change password reminder
- ✓ PIN and/or Biometrics protection
- ✓ False authentication card lock
- ✓ Up to 20 Character PIN Size
- ✓ Alpha/numeric/punctuation PIN Character Type
- ✓ 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
- ✓ Card storage data encryption: AES-256, SHA-256, data salting
- ✓ Response for Card/Server Authentication

Full Featured:

- ✓ Cybersecurity framework compliant
- ✓ Third-Party software API integration
- ✓ Multiple smartcard compatibility
- ✓ Add, View, Edit & Delete Cardholders
- ✓ Event logging in records
- ✓ Time and attendance
- ✓ Security monitoring
- ✓ LDAP directories supported
- ✓ Database importing & exporting
- ✓ Supports terminal services
- ✓ Lost or stolen card hotlist
- ✓ Recycle cards and licenses
- ✓ Generate reports, & card data recovery
- ✓ IT Administrator PIN Reset

Enterprise Security:

- ✓ Windows startup login
- ✓ Network login
- ✓ Auto launch web browser
- ✓ Auto fill USER NAME & PASSWORD, and Submit
- ✓ Inter-/Intra-/Extra-net login
- ✓ Auto record internet passwords
- ✓ Auto launch Windows applications
- ✓ Windows applications login
- ✓ Unlimited accounts stored in Active Directory



© ALL INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED "AS IS"; Access Smart ASSUMES NO RESPONSIBILITY FOR ITS ACCURACY AND/OR COMPLETENESS. 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.

System Requirements

Card Administrator

Operating System:

Windows® Server 2023, 2022, 2019

Server:

Server hardware should have at least 4 GB of RAM for smaller installations, and 8+ GB is recommended for 50+ users.

The use of Virtual Server technology is recommended

Employee's Computer

Operating System:

Windows® Win11, Win10, Win 8.x, Vista, Win7

Computer:

Pentium® 233 MHz or higher, or compatible; CD-ROM drive; VGA or higher graphics; 128MB of RAM; Available USB, PCMCIA or ExpressCard port; and 70MB available hard disk space.