

Power LogOn[®] For Critical Infrastructure

Multi-Factor Authentication and Enterprise Password Management



Add Cyber Access Management

- ✓ Fulfills manufacturing's cybersecurity standards
- ✓ Your passwords are managed and stored on prem, and not in our servers
- ✓ IT centralized password management
- ✓ No more passwords for users to Remember, Type, or Know
- ✓ Supports cloud cybersecurity compliance with FedRAMP, NIST SP 800-53 and 207, CSA, CIS, SOC-2, and others
- ✓ Identification authentication management (IAM, ICAM)
- ✓ Avoids expensive and complex certificates
- ✓ LDAP, VM and AD compatible
- ✓ Installs on Cloud, Enterprise Servers, Small Business Networks, or Stand-Alone Computers
- ✓ Helps institutions meet their government's CMMC requirements



Power LogOn works with existing employee ID badge systems

IT Centralized Management

Centralizing password management fixes cybersecurity's weakest link: **Employee-Managed Passwords!**

Power LogOn gives the IT Administrator the power to control every employee's password operation to auto-enforce security policies across multiple computers, networks, clouds, and applications.

Power LogOn integrates with AD, VM, LDAP, TS, remote desktops, thin clients, cloud-based systems, and VPN connections to assign specific card-based user privileges.

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 attacks
- ✓ **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

Credential Convenience

Power LogOn consolidates functions and user credential data onto a single ID badge so that employees no longer need to carry multiple cards, phones or tokens to access different company facilities and resources.

Decreasing the number of credentials that employees carry not only improves user convenience; it also decreases the likelihood that sensitive data will be lost, forgotten or stolen. Combining high security features with user convenience makes identity management, loss discovery, and plugging vulnerabilities easier, faster, and more reliable.

Combine multiple card technologies - RFID, mag stripe, custom graphics, bar codes, and so much more - onto one CR-80 card body. IT and HR only need to issue and manage a single credential.



Windows Logon Screen



Account Access Screen

Fast, Easy and Affordable

Certificate-based systems have high installation costs and can take a year or more to implement. If technology is too cumbersome on employees and IT, they will often circumvent security for convenience. All these and other issues delay deployment and increase the odds of a cyber-attack going. Power LogOn solves these and many other security issues facing emergency responders.

Power LogOn resides in your existing Server's Active Directory and is pushed down runs onto vehicle computers, desktop computers and laptop computers.

Power LogOn is affordable with low annual subscription pricing, and licenses are transferable to address employee turn-over.

Implement cybersecurity identity and access management with Power LogOn

Learn more at: www.Access-Smart.com



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, Win 10, Win 8.x, and Win 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:

- ✓ FIPS 140-3 Verified, NIST 800-63b
- ✓ 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.