

Power LogOn[®] For Manufacturing

Multi-Factor Authentication and Enterprise Password Management



Add Cyber Access Management

- ✓ MFA compliance with state data protection laws, insurance companies databreach protection policies, and government CSSM, 800-171 specs.
- ✓ Passwords are never managed or stored on our servers
- ✓ Secure Identity and Access Management
- ✓ Password Management added to existing physical access cards
- ✓ IT Centralized Password Management
- ✓ Card Life Cycle Management
- ✓ Password Management via VM and Active Directory
- ✓ Installs on your Cloud, Enterprise Servers, Small Business Networks, or Stand Alone Computers



Power LogOn works with existing employee ID badge systems

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 a network access vulnerability

Credential Convenience

When employees carry too many credentials, they increase the odds of a cyber breach should a credential be lost or stolen. Early discovery of the loss greatly reduces the damage a perpetrator can implement.

The combination of multiple functions (physical access, photo ID, cyber access) onto a single badge makes security management, loss discovery and vulnerabilities fast and easy. Compatible with different card technologies, contact smart-cards, contactless smartcard, mag stripe, RFID and others, gives IT a wide range of flexibility.

When an employee leaves the company, and their badge is surrendered back the HR, users can't back-door their way into the network because they no longer carry all the authentication factors.



Windows Logon Screen



Account Access Screen

Fast, Easy and Affordable

Power LogOn builds on your existing enterprise security infrastructure making it fast to install: no rip and replace.

Power LogOn offers a low cost of ownership with no annual subscription or renewal fees, and licenses are transferable to address employee turn-over.

Can be tailored to the different cybersecurity frameworks, regulatory compliance measures, and technical controls. Some of the regulations include NAIC Insurance Data Security Model Law, 23 NYCRR 500, HIPAA, GDPR, and CMMC.

Implement secure cyber identity and access management with Power LogOn!



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 Certified
- ✓ **Clouds:** AWS, Azure, Google, or any other cloud supporting Virtual Machine
- ✓ **Web Browsers:** Auto launch IE, 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
- ✓ 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
- ✓ Session Key Negotiation
- ✓ Key Diversification
- ✓ Challenge / Response for Card/Server Authentication

Enterprise Security:

- ✓ Windows Bootup Logon
- ✓ Network Logon
- ✓ Auto Launch Web Browser
- ✓ Auto User Name & Password Fill and Submit
- ✓ Inter-/Intra-/Extra-net Logon
- ✓ Auto Record Internet Passwords
- ✓ Auto Launch Windows Applications
- ✓ Windows Applications Logon
- ✓ Unlimited Accounts Stored in Active Directory
- ✓ Data Storage Encryption Integration



© 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.

Full Featured:

- ✓ Cybersecurity frameworks 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

System Requirements

Card Administrator

Operating System:

Windows® Server 2025, 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® Win 11 32/64, Win10 32/64, Win 8.x 32/64, Vista 32/64, Win7 32/64,

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.