Power LogOn®

Multi-Factor Authentication
Enterprise Password Management

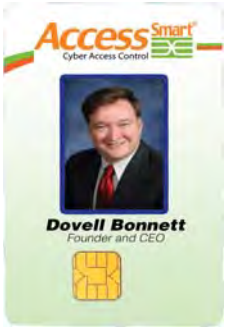
Data Protection and Compliance

Businesses don't have a password problem, they have a password management problem... Until now!

Power LogOn allows IT adminstrators to auto-implement security policies that safeguard sensitive data and personal information. It's affordable, easy to integrate into existing systems, and it makes logon secure and convenient.

The Need for Two-Factor Authentication

An unattended computer connected to the network is a cyber vulnerability and for some industries a privacy violation. Weak passwords and sharing of passwords are a major concern for IT.



Two-factor authentication is the industry standard for implementing secure computer and network access. Since user names and passwords are still the most common form of authentication, it's time to make them secure.

Power LogOn meets the government and industry requirements for multi-factor authentication enterprise password management. Power LogOn enables strong passwords. Users can't share any passwords. Computers and applications are locked down when the card is removed.

IT Centralized Management

Centralized management enforces security policy across multiple applications by fixing cybersecurity's weakest link: User managed passwords.

Power LogOn allows IT to set the card's password operations to match their security policies. Power LogOn easily integrates with Active Directory, LDAP, Terminal Services, remote desktops, thin clients, and VPN connections so IT can assign specific card-based user privileges.

Secure Access

Credentials must safeguard against unauthorized access and credential falsifications. Here are some of the ways Power LogOn secures networks:

- ✓ **Multi-factor authentication** - safeguards against outsider intrusions.
- ✓ **Users don't know passwords** - safeguards against social engineering attacks.
- ✓ **Account addresses verified before auto fill** - safeguards against spam, phishing and pharming.
- ✓ **Passwords are not typed** - safeguards against keyloggers and "over-the-shoulder" attacks.

Multi-function Credential Convenience

Too many different access ID credentials, tokens and devices employees carry become a major cyber vulnerability. For example, one card for photo ID and physical access, a token to access the network, and a smartphone to remember passwords. The more devices one carries, the higher the odds that one or more will be lost, stolen or forgotten. Combining multiple functions onto a single ID badge makes security management, loss discovery and plugging a vulnerability faster and easier.

Power LogOn works with existing employee ID badge systems. Multiple card technologies like RFID, magnetic stripe, custom graphics, bar codes, and so much more can be combined onto one CR-80 card body. IT and HR only need to issue and manage a single credential.

Fast, Easy and Affordable

Expensive security technology makes it harder for management to authorize necessary purchases. When implementation takes too long, the odds of a breach increase exponentially. If technology is too cumbersome, people will find ways to circumvent it. All these issues increase the odds of a cyber attack going unnoticed. Power LogOn solves these issues and more.

Power LogOn is very affordable with no annual renewal fees. Power LogOn can reside on the existing server with Active Directory, and be pushed down to individual computers. Conveniently, the user only has one PIN to remember. It's that simple and easy.

Power LogOn

Multi-Factor Authentication Enterprise Password Management

General Information:

- ✓ **Primary Application:** Multi-factor authentication enterprise password management
- ✓ **Secondary Application:** Strong passwords, safeguards against many hacker techniques
- ✓ **Operating System:** Windows 10 (32/64-bit), 8.1, 7, Vista and XP
- ✓ **Servers:** Win Server 2016, 2012 R2, 2008, 2003, 2000 and SQL Server 2014 Certified (Server 2016 in progress)
- ✓ **Web Browsers:** up to IE 11, Firefox, Chrome
- ✓ **Authentication factors:** Possession, Knowledge, Inherence, Encryption Keys, CUID, and Challenge/Response

Authentication & Security:

- ✓ FIPS 140-2 Verified by InfoGard®
- ✓ Up to 500 Character Length Passwords
- ✓ Online ID Protection, Social Engineering Protection
- ✓ Phishing and Pharming E-mail Protections
- ✓ Keylogger Protection
- ✓ 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, Smartcard, PIV, PIV-I, CAC, RFID 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

Password Security:

- ✓ Windows Bootup Logon
- ✓ Network Logon
- ✓ Auto Launch IE 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

SQL Server 2014 Certified

FIPS 140-2 VERIFIED Tested by InfoGard

HIPAA 2-Factor Authentication

Powered by Smartcard Technology®

Full Featured:

- ✓ FIPS 201 waived
- ✓ Third-Party Software Logon
- ✓ Multiple Smartcard Compatibility
- ✓ Add, View, Edit & Delete Cardholders
- ✓ Directories supported
- ✓ Database Importing & Exporting
- ✓ Supports Terminal Services
- ✓ Lost or Stolen Card Hotlist
- ✓ Recycle Cards and Licenses
- ✓ Generate Reports
- ✓ IT Administrator PIN Reset
- ✓ Administrator Card Issuance
- ✓ Card Data Recovery

System Requirements

Card Administrator

Operating System:
Windows® 10 (32/64 bit) 8.x (32/64 bit), 7 (32/64 bit), Vista, XP, 2000, Server up to 2016, SQL Sever 2014

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 8 GB available hard disk space.

Employee's Computer

Operating System:
Windows® Win10, 8,x, 7, Vista, XP, & 2000

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. Surface Pro 2 and 3

27762 Antonio Parkway, Suite L1-461 • Ladera Ranch, CA 92694 • Phone: (949) 218-8754

Access Smart® Cyber Access Control