Power LogOn®

For Azure and Azure Active Directory

Multi-Factor Authentication with Enterprise Password Management

Add Cyber Access Management to Azure

- ✓ Card-based Multi-Factor Authentication with enterprise password manager
- ✓ Your passwords are managed and stored on prem, and not in our servers
- ✓ Secure Identity and Access Management
- ✓ Add Password Management to existing physical access badges
- ✓ IT Centralized Password Management
- ✓ Card Life Cycle Management
- ✓ Avoid Certificate Expense and Complexity
- ✓ Plugs into Existing Server and Cloud Infrastructure
- ✓ Password Management via Azure AD
- ✓ Secure boot-up, applications, servers, networks, clouds, and website MFA login
- ✓ Installs on Cloud, Enterprise Servers, Small Business Networks, or Stand Alone computers

Power LogOn works with existing employee ID badge systems

IT Centralized Management

IT centralizing password management fixes cybersecurity's weakest link: **employee-managed passwords!** It does this by automatically enforcing your security policies across multiple applications.

Power LogOn gives IT the power to set any card's password operations to auto-implement their security policies.

Easily integrate with Azure's Active Directory, Active Directory, other LDAPs, Terminal Services, remote desktops, thin clients, and VPN connections to assign specific

Prevent Unauthorized Access

- ✓ **Multi-Factor Authentication** - guards against outsider intrusions
- ✓ **User's don't know passwords** - guards against social engineering
- ✓ **Account addresses verified before auto fill** - guards against spam, phishing and pharming
- ✓ **Passwords are not typed** - guards against key loggers and "over-the-shoulder" attacks
- ✓ **Auto log off when card is removed from reader** - Removes a network access vulnerability, and Azure automatically re-encrypts data before closing

Credential Convenience

Combining multiple functions onto an existing single ID badge makes security management, loss discovery and plugging vulnerabilities fast, easy, and economical.

Employees carrying too many credentials and tokens become a major cyber vulnerability. A card for photo ID and physical access, a token to access the network, and a smartphone to remember passwords… the more devices carried, the higher the odds that one or more will be lost, stolen or forgotten. Power LogOn's convenience ensures end users adhere to your security policies.

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. Often without re-badging or re-issuance.

Windows Logon Screen

Account Access Screen

Fast, Easy and Economical

Certificate-based systems can take a year or more to implement. Expensive technology can delay authorization of necessary purchases. And if technology is too cumbersome, employees will find ways to circumvent it. Power LogOn takes IT about an hour to install and deploy. Employees self-enroll. Adds another use to an existing access contol badge.

Power LogOn is affordable, with no annual fees. It can reside on an existing Azure Cloud Active Directory and be pushed down to individual computers.

Implement secure identiy and access management with ... Power LogOn!

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 10 (32/64-bit), 8.x (32/64), and Win 7 (32/64)
- ✓ **Servers:** Win Server 2019, 2016, 2012 R2, 2008 and SQL Server 2014 Certified
- ✓ **Clouds:** AWS, Azure, Google, or any other cloud supporting Vitual Machine
- ✓ **Web Browsers:** Auto launch IE, Firefox, and Chrome browsers
- ✓ **Authentication factors:** Possession, Knowledge, Inherence, Encryption Keys, CUID, and Challenge/Response

Authentication & Security:

- ✓ FIPS 140-2 Verified by InfoGard®
- ✓ 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, 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

Full Featured:

- ✓ FIPS 201 compliant
- ✓ DFARS NIST 800-171 compliant
- ✓ NIST 800-63b AAL-3 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 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

Azure

Windows 10 Compatible

NFC

Powered by Smartcard Technology®

Microsoft SQL Server

DFARS Compliant

CJIS

FIPS VALIDATED 140-2

HIPAA COMPLIANT

System Requirements

Card Administrator

Operating System:
Windows® Server 2019, 2016, 2012/R2, 2008/R2

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® 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.

12400 W. Hwy 71, Suite 350-259 • Austin, TX 78738 • Phone: (949) 218-8754

Smart Access Cyber Access Control