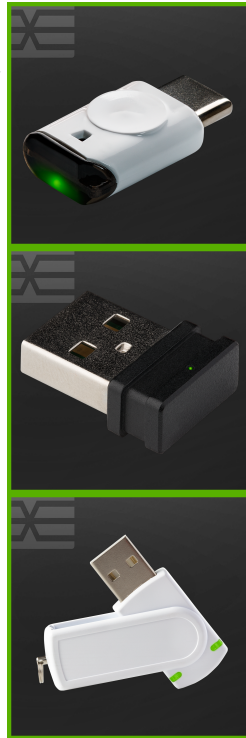# Power LogOn®
For Working From Home

uTrust Token + Multi-Factor Authentication and Enterprise Password Management

Add Cyber Access Management to Server

- ✓ Multi-Factor Authentication
- ✓ Identiv uTrust Tokens (Pro Mini-C, Pro Mini, and Pro +)
- ✓ Your passwords are managed and stored on prem, and not in our servers
- ✓ Secure Identity Access Management (IAM)
- ✓ Combines Java card or card reader
- ✓ IT Centralized Password Management
- ✓ Home and Mobile environments
- ✓ Avoid Certificate Expense and Complexity
- ✓ Access Existing Server and Cloud Infrastructure
- ✓ Password Management via VM and Active Directory
- ✓ Installs on Home computers to access Cloud, Enterprise Servers, Small Business Networks, or Stand Alone computers
- ✓ SLIM, ELEGANT DESIGN

Power LogOn & uTrust Tokens combines MFA, Password management, card and reader into one unit.

IT Centralized Management

Centralizing password management fixes cybersecurity's weakest link: <u>user managed passwords</u>! It does this by automatically enforcing your security policies across multiple applications. IT has the power to manage company access passwords.

Easily integrate with Active Directory, LDAP, Terminal Services, remote desktops, thin clients, and VPN connections to assign specific card-based user privileges.

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

Credential Convenience

The compatibility of Identiv's line of uTrust Tokens and our Power LogOn® multi-factor authentication with enterprise password management for login protection of security-critical mobile and remote computers. This combination is perfect for work-at-home employees and employees who travel with their laptop. No bulky cards and desktop readers to manage. These compact tokens combine a smartcard and reader into one ultra-small package.

"Access Smart's ability to provide true multi-factor authentication using Identiv's uTrust Tokens expands the security and convenience — while lowering the costs — of user logins," said Dr. Manfred Mueller, Identiv GM, Identity. "Our partnership raises the bar in enterprise cybersecurity by putting remote access security back into the hands of IT and login convenience into the hands of employees."

Windows Logon Screen
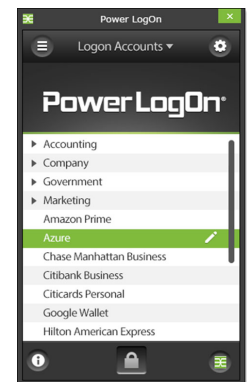
Account Access Screen

Fast, Easy and Affordable

Certificate-based systems can take a year or more to implement. Expensive technology can delay government cybersecurity compliance. And if technology is too cumbersome, employees will find ways to circumvent it. All of these issues increase the odds of a cyber attack going unnoticed, making your company vulnerable to a breach, fines, lawsuits and bankruptcy.

Power LogOn solves these issues and more.

Power LogOn is affordable, with no annual fees. It can reside on an existing Sever's Active Directory and be pushed down to individual computers. Implement secure IAM with ... Power LogOn!

Power LogOn

uTrust Token + Multi-Factor Authentication and Enterprise Password Management

General Information:

- ✓ **Primary Application:** Identity management, multi-factor authentication, and enterprise security for Mobile and Work From Home
- ✓ **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, SQL Server 2019, and 2014 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
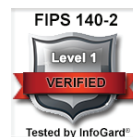
Authentication & Security:

- ✓ FIPS 140-2 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
- ✓ Password Data Backup
- ✓ CCID, PC/SC, Java Card, USB Type A/C compliant
- ✓ Token Removal Actions: User Log Off, Computer Lock Down, Computer Shut Down, Nothing, or Custom
- ✓ Secure Token Password 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 Token Hotlist
- ✓ Recycle Token and Licenses
- ✓ Generate Reports, & Token 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

SQL Server 2014 Certified

Windows 10 Compatible

FIPS 140-2 Level 1 VERIFIED — Tested by InfoGard®

HIPAA

GSA FIPS 201 APPROVED

NFC

Powered by Smartcard Technology®

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, Win 7 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.

Access Smart Cyber Access Control