LAYOUT PREVIEW v5 · 22 November 2026 · DRAFT for review · Not for publication or distribution
NEW 11/21 open / OPTION held exceeds v14 space

Power LogOn®

for Operational Technology (OT)

Ransomware was in 61% of manufacturing breaches.

Verizon 2026 DBIR, Manufacturing



Manufacturing plants and utility companies run on operational technology (OT), the computers that control physical equipment.

Cyber attackers don't break into a PLC. They hack access into your HMI, engineering workstation or the SCADA server. They typically break an operator's password. One compromised account can stop the line, introduce defects, or cause serious community safety issues. These attacks can be very costly in time, money and reputation. Power LogOn addresses this by removing the weakest link: employee-managed passwords.

OT's Top Fears and Power LogOn Answers

OT Managers' Top Cybersecurity Fears	The Power LogOn Experience
Shared operator credentials One username and password for the whole shift, or worse, no logon at all.	**Know who's accessing each station** Each operator has a unique ID badge and PIN. Logs show who logged on to which station, and when.
Ransomware shutting down operations Every hour offline costs money, service, and customer trust.	**Password security is out of employees' hands** Helps protect against keyloggers, shoulder surfing, pass-the-hash, and other credential attacks.
Stolen remote-access passwords One stolen VPN or remote desktop password lets an attacker in from anywhere.	**Card and PIN on Windows, VPN and remote desktop logons** True MFA protects every logon, so a stolen password alone is worthless.
Passwords written down, reused, or shared Employees are inundated with passwords, so they write them down, reuse them, and share them.	**Password policy enforced, operators unburdened** IT sets the password policy. Power LogOn enforces it. Operators can't circumvent policy because they don't know, type, or manage passwords.
Stations left open at shift change The next person can walk up and take over the station under someone else's name.	**Reducing unauthorized access at shift change** Operators remove their badge, and Power LogOn logs them off. The next shift logs on as themselves.

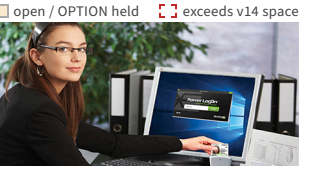
Additional Power LogOn Advantages

The Advantage	The Explanation
Uses what you already own	Works with your existing ID badges, readers, Active Directory and Windows. No rip and replace.
Up and running fast	Installs in about one hour.
No waiting on password resets	Operators keep working instead of sitting idle.
Fewer credentials to carry	One badge for the door and the computer.
Guards against phishing, social engineering & spoofed sites	Employees don't know their passwords. Power LogOn confirms the site address before an auto-fill
Protects your reputation	A breach can cost customers and sales, and can lead to layoffs and bankruptcy.
Addresses cybersecurity best practices	Helps with identification and authentication guidance, Zero Trust, CIS Controls v8, cyber insurance MFA and CMMC Level 2.



Power LogOn works with existing employee ID badges

Power LogOn
for Operational Technology (OT)



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 and earlier, including Windows IoT Enterprise, Embedded and LTSC editions
- ✓ **OT Computers:** HMIs, engineering workstations, SCADA servers, historians, thin clients, Windows controllers, and industrial PCs running soft PLCs
- ✓ **Servers:** Windows Server 2025 and earlier; on-premises SQL Server 2025 and earlier
- ✓ **Clouds:** AWS, Azure, Google Cloud, or any other cloud supporting virtual machines
- ✓ **Web Browsers:** Auto-launch Edge, Firefox, and Chrome
- ✓ **Authentication factors:** Possession, Knowledge, Inherence, Encryption Keys, CUID, and Challenge/Response
- ✓ **Remote Access:** VPN and RDP; Laptop Mode keeps passwords encrypted on the laptop

Authentication & Security:

- ✓ Helps address identification and authentication guidance on the Windows HMIs, workstations and servers.
- ✓ Account addresses verified before auto-fill.
- ✓ Passwords are encrypted, salted and changed often.
- ✓ Up to 500 character length passwords
- ✓ Four wrong PINs locks user's account
- ✓ **True Multi-Factor Authentication -** Card + PIN. Card + Biometric. Card + PIN + Biometric.
- ✓ Password generator and configurator
- ✓ Up to 20-Character PIN Size
- ✓ Alpha, numeric and punctuation PIN character types
- ✓ Stored passwords: AES-256 encryption plus SHA-256 hashing, with hash salting
- ✓ Works with Prox, ISO 14443/15693 13.56 MHz contactless (iCLASS, MIFARE, DESFire), NFC and other RF credentials, plus contact smartcards
- ✓ Configurable card-removal actions, set per station: log off, lock, shut down, disconnect a remote session, do nothing, or run a custom script
- ✓ Change password reminder

Enterprise Security:

- ✓ Windows bootup logon
- ✓ Network logon
- ✓ Auto-launch web browser
- ✓ Inter-/Intra-/Extra-net logon
- ✓ Auto-record internet passwords
- ✓ Auto-fill user name and password, and submit
- ✓ Auto-launch Windows applications
- ✓ Windows applications logon
- ✓ Unlimited accounts stored in Active Directory or LDAP

Credential Convenience:

- ✓ Works with most employee ID badges
- ✓ One badge for physical and logical access control
- ✓ Works where phones are banned
- ✓ Multi-function badges increase security
- ✓ Removes the hassle of managing passwords

IT-Centralized Management:

- ✓ Power LogOn gives IT the power to generate, issue, replace or revoke employee Power LogOn credentials.
- ✓ Passwords stay on your own servers; nothing runs on Access Smart servers.
- ✓ Power LogOn is affordable with low annual subscription pricing.

System Requirements

Card Administrator

Operating System:
Windows® 11 and earlier

Server:

Server 2025 and earlier; on-premises SQL Server 2025 and earlier.

The use of Virtual Server technology is recommended

Employee's Computer

Operating System:
Windows® 11 and earlier, including Windows IoT Enterprise, Embedded and LTSC editions; thin clients connected to a Terminal Services server

© 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.

4049 Northwood Pl · The Villages, FL 32163-2293 · Phone: (949) 218-8754