CASE STUDY

Smart Access Cyber Access Control

Government Cyber Lab Requires PIV Password Management

A US government agency's Cyber Lab needed to improve their server security to comply with new government cybersecurity mandates. Their solution requirements included: must work with their existing PIV credentials, meet all government cybersecurity requirements, make passwords extremely complex and easy to change daily, keep operational costs low, prevent employees from knowing their passwords, and make the end-user experience easy and convenient, even for non-techie upper managers. Power LogOn delivered these and many other benefits.

The Challenge

To protect digital information and stay ahead of hackers, and control which employees had access to specific servers. The list of required specifications, including:

- ✓ **FIPS 140-2 and FIPS 201 compliant, AES-265, SHA-256 data encryption**
- ✓ **IT centralized password security and management**
- ✓ **Multi-Factor Authentication using existing government PIV credentials**
- ✓ **Active Directory and VMware compatible**
- ✓ **Ability to easily manage the passwords of over 700 servers**
- ✓ **Control each employee's access rights individually or in groups**

The Solution

Already in use: Government issues PIV credentials, smartcard readers

Purchased: Power LogOn software and licenses

Before Power LogOn, the Cyber Lab was using Single-Factor Authentication, spreadsheet style, user-generated password manager with access to every server.

- **Use the existing PIV credential to avoid re-badging and re-qualification**
  Power LogOn works with an existing PIV credential and uses existing card information to reduce costs and FIPS 201 compliant.
- **FIPS 140-2 Compliant**
  InfoGard, and independent NIST lab, " verified" that Power LogOn meets and exceeded FIPS 140-2 requirements .

- **Strong Passwords**

  20-character long passwords for every account, using any of the available 96 keyboard characters, in random order. Employees does not generate any passwords.

- **Phishing and Pharming Protection:**

  Power LogOn stores the URL / path of the logon account. If the site's URL does not match, Power LogOn does not release the password.

Customer Feedback

Productivity has increased by 20% because of the simple, double-click, automated efficiency of Power LogOn vs. their previous multi-step cumbersome password manager. More importantly, that simple double-click sets into motion eight layers of assurances and multi-factor authentication that protects the security of highly sensitive data.

Cost savings have been applied to both direct and indirect costs. The previous password manager carried an annual renewal fee, which the agency no longer has to pay. In addition, the reduced load on IT of help desk calls to reset forgotten passwords has saved hours of salary time, as well as time taken away from more important security tasks.

Power LogOn is compatible with the latest Microsoft Windows and SQL Server versions. Clients connect to the Power LogOn Administrator server using .NET web services, which makes the system scalable anywhere from small offices with a handful of clients to multi-site installations with thousands of users.

Power LogOn Administrator Integration Kits

Test Power LogOn for 90-days at no risk. We offer different configuration options

Contact Smartcard version

Contactless Smartcard version