



Top Intellectual Property Firm Implements Secure Data Access Policy Without Inconvenience to Employees

The Organization

Stetina Brunda Garred & Brucker (SBG&B) Law Firm

The Challenges

- Comply with privacy legislation
- Reduce IT help desk costs
- Increase security

Power LogOn Solution

SBG&B needed:

- Password security & management
- Building access
- Network integration
- Low cost of ownership

The Results

- Different passwords for each account
- ID Badge & logical access.
- Transferable licenses. No subscription fees
- Log into multiple Windows' computers, applications, Internet & server networks.
- Auto logoff when card is removed

Stetina Brunda Garred & Brucker (SBG&B) is a prominent AV-rated patent, trademark and copyright law firm located in Aliso Viejo, California. It is a full-service intellectual property firm that procures patents, trademarks and deals with intellectual property issues throughout the world with a network of foreign associates located in more than 80 different countries.

Like all legal firms, SBG&B must operate under a strict policy to protect the integrity of its records and the confidentiality of its clients from hackers and other vulnerabilities both inside and outside the firm's walls. Well aware of the fact that computer security experts have stated that 80 percent of all network security problems are caused by bad passwords*, Rose Richardson, the firm's IT director, was looking for a solution that would enable her to enforce stronger password policies within the firm without adding additional burdens to attorneys and other office staff.

"In order to ensure the highest standards of network security, passwords need to be more complex than the usual one-word, easy-to-remember ones used by most people," said Richardson. "It is also good practice to change passwords on a regular basis. However, making a safe password policy a priority in a busy firm such as ours can be a challenge."

Employees in the firm use multiple passwords not only to access networks and confidential files but to logon to Internet sites such as Thomson's Saegis, the United States Patent and Trademark Office and LexisNexis for research. Richardson knew that she needed a solution that could not only provide strong password security but that could also be capable of generating and storing the numerous passwords that would be needed to provide safe access to multiple types of files and web sites.

"We decided to go with Access Smart's Power LogOn because it seemed to be the easiest to implement and the most secure," said Richardson. "After the quick software install, I plugged in the card reader to the USB port and allowed the user to choose a PIN. That was it."

Case Study



Power LogOn Features

Security

Strong Passwords: Unique, 20-character long passwords for every account, using any of the available 96 keyboard characters, in random order.

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.

Keylogger Protection: Auto-start Internet Explorer or Application, password auto-form fill & auto-submit.

Convenience

Users never have to remember or type any log on user names or passwords. Now, organizations can implement strong password assignment policies with convenient password management for their employees.

Affordable

Software can be loaded onto an unlimited number of computers, because the user license is on the card not the software.

Power LogOn licenses are transferable and recyclable. No annual subscription or renewal fees.

Power LogOn works with a number of different card technologies (i.e. RFID, contact smart chips, magstripe, & bar code).

(cont.)

The computer does not see Power LogOn as a storage device. So, in the event that an unauthorized person tries to hack into a computer, they will not be able to tell that the card storing all of the passwords is even present. In addition, each smartcard will lock up after an incorrect PIN is entered three times, adding further security in the event that a computer and its smartcard fall into the wrong hands.

After installing Power LogOn to the computers of several of the firm's employees, Richardson found that they could easily access password-protected files and web sites without having to remember, type or even know the passwords. Power LogOn could also be programmed to automatically change passwords in a specified time-frame to implement further data access security without requiring any action from the employee.

The administrative controls also enable the firm to maintain autonomy among different departments. Certain individuals could have access to files in one department and not another by preprogramming the smartcard to suit the individual employee's access permissions.

Founder and Partner Kit Stetina also found Power LogOn swift and hassle-free to implement. "When I start up my computer, I enter my PIN and am able to automatically login to any password-protected file or web site," said Stetina. "I don't need to take extra time to assign different passwords to each file, change them once a month or look them up every time I need to access data, as the smartcard does all of this for me. This convenience allows us to implement the highest level of data access security while not affecting our productivity. I would definitely recommend Power LogOn to our clients, other legal firms and any business to safeguard against unauthorized access to confidential information."

When asked about future consideration for the company's smartcard access capabilities, Stetina replied "We are currently looking into integrating our Power LogOn system on to our employee access badges so that the same card that gets us into the building is also the same card that provides access to all of our computer data. Access Smart's smartcard technology truly has the potential to evolve the standard of safe access in the office environment."