

CAA North & East Ontario Puts a Lock on User Security with OmniPass

As some clubs have already experienced with great success, Softex Incorporated's [OmniPass](#) single sign-on solution provides system administrators with a secure and streamlined approach to managing users' numerous enterprise and web application passwords. OmniPass protects corporate applications from unauthorized access by storing all passwords in a secure 'vault'. Instead of a separate password for each application, OmniPass can be configured to use a single sign-on ('master password') that uses authentication rules and/or a security device such as a fingerprint reader or biometric mouse to verify the user's identification, and grant them access to applications.

CAA North & East Ontario (CAA-NEO) is one club that has implemented OmniPass. In addition to AXIS, CAA-NEO is using OmniPass to manage the login for websites (AICWEB, CAA Connect, Virtual Travel Money and EZTickets) and enterprise applications such as email and Instant Messaging.

Security Risk Management & Compliance

In fact, the security risk of maintaining so many passwords was the key reason CAA-NEO implemented OmniPass. Dana Carter, Information Systems Manager for CAA-NEO, says having a single 'master password' has improved password management practices with users: "Previously some users would have their passwords posted on their cubicle wall for everyone to see, which posed a big security risk. By having a single sign-on, users only need to remember one password, which is stored in the OmniPass vault. Users are very happy about not having to remember so many passwords, and as a result, are no longer posting them on sticky notes."

At an organizational level, using OmniPass fulfills the security requirements for PCI and TQS #5, allowing CAA-NEO to comply with the standards set by the PCI Security Standards Council and CAA National, respectively. This is because OmniPass protects enterprise applications, and sensitive client and corporate information, from unauthorized access.

Carter says how OmniPass is managed distinguished it from similar solutions: "OmniPass is tied to our Active Directory, and is integrated into our application systems. The password database is maintained completely within our environment, not offsite through a remote server, so the passwords never leave our network. For that same reason, nobody can see the passwords, so we can rest assured that passwords are private and secure, and that no outside party can access them."

Implementation Process

Because OmniPass is maintained within CAA-NEO's network, Carter and the information systems team were able to take an enterprise-wide approach to implementation. Every workstation in the organization has OmniPass installed on it, at all locations. For some of the locations, OmniPass was physically installed on workstations during a routine hardware upgrade visit; others were implemented remotely, that is, over a VPN connection.

"We wanted to ensure the Travel Store would be able to get up and running with OmniPass as quickly and effectively as possible. Some Travel Store locations required a more hands-on installation and training approach, while others less so. And wherever possible, we wanted to provide a warm hand-off, so that users in that particular location were confident and comfortable using OmniPass," explains Carter.

However, like any new application, some training, documentation and setup was required; both for the software itself and to guide the change management process. Due to the number of users to be trained, and the distance of store locations, CAA-NEO deployed a 'train-the-trainer' method based on instructions and how-to tips that resulted from testing conducted by the information systems team and 'super users'.

The Travel department was the first to have OmniPass installed on their workstations, because on average Travel employees have dozens of website passwords, and would receive the highest return from using the product. Other departments quickly followed, with users helping one another to learn and use OmniPass to immediate benefit.

Password Management

CAA-NEO is using several methods to authenticate the user through OmniPass. Some employees are using fingerprint readers, others biometric mice, and a few log in by answering a security question (e.g. "what's your mother's maiden name"?) But the majority of users are set up with the single password sign-on method.

The club found fingerprint readers and biometric mice were best suited to employees that worked exclusively in the office. Otherwise staff that worked from home would require the same security device to be installed on their home workstation. The single password sign-on functionality, not needing additional hardware, can be used from any workstation within CAA-NEO's network, including virtual and remote workstations.

OmniPass can automatically assign the user a password, in which case the user doesn't actually know the password. In that scenario, the password is tied to a security device; it's the fingerprint reader that logs them into their applications. Or users can create their own password. CAA-NEO selected the latter option for several reasons:

“For users, there is a comfort level associated with creating and knowing their password. There’s a fear [in the user’s mind] that if OmniPass were to ever go down, or if the security/biometric device stopped working, that the user couldn’t log into the system. Also, some systems, such as the employee time tracking system, are hosted outside the corporate firewall and not managed through OmniPass. For those types of systems, where the employee may be logging in from their home computer, they have to know their password,” states Carter.

Benefits of Increased Data Security

In addition to enhanced password management and security, CAA-NEO is experiencing significant benefits in regards to time savings. OmniPass has eliminated the time needed by users to research or look up the passwords they have stored or written down. It also reduces entry errors associated with complex or case-sensitive passwords, where users would have keyed the password two or three times. There is also time saved by the technical support team, who are spending less time resetting passwords for users that were locked out of applications.

Carter says the time savings alone have demonstrated the value of the OmniPass solution: “The investment we put into learning, implementing and maintaining OmniPass has been easily offset by the benefits we have gained by not having to do as many password resets, and unlocking accounts.” In terms of return-on-investment (ROI), CAA-NEO has experienced a net reduction in administrative overhead, specifically the number of resources and effort required to maintain accounts and passwords. When comparing the effort needed to manage OmniPass versus that of maintaining system/website accounts, Carter considers their return in OmniPass to be ‘in the black’.

At a user level, Carter discovered that once users start using OmniPass and experiencing its benefits first-hand, any resistance to it was overcome, and it became something they accepted and endorsed. In fact, “Many users have become reliant on the product, which is a true measure of its adoption within the organization. If people feel like they can’t do their job without a product, that their reliance on it invokes that type of response, to me that shows OmniPass is well on its way to being fully adopted and embraced by users,” affirms Carter.

On a closing note, CAA-NEO found that one of the simplest measures of success and justification for implementing OmniPass was the perception of benefit by the end-users; it ‘reduced their pain’ of managing passwords. That in itself makes a strong case for any club looking to implement OmniPass themselves, which Carter strongly recommends.

For more information about OmniPass, please contact [Pierre Lapalme](#), Director of Sales and Marketing (Tel: 1-800-463-2688 x 209).