OmniPass
Enterprise-Class Password Management

A Windows application to manage passwords, secure data, and protect users online

Whether you are a home, small business or large corporate user, the OmniPass family of products can protect user data, solve the problem of multiple passwords and poor password practices (simple passwords that are written down on a notepad) and increase security all while simplifying the end user experience.

OmniPass allows a user to encrypt/decrypt data and login to their local PC, home or corporate network, websites and applications with a wide choice of authentication mechanisms (fingerprint scanners, smart cards, TPM...etc.) or a single password (SSO). For corporations this reduces operational costs and improves employee productivity, for individuals it makes using their PC much more convenient and secure.

Scaleable Authentication Framework

OmniPass is designed to work in conjunction with a wide variety of authentication devices. OmniPass supports the most advanced biometric technologies from companies such as Fujitsu(PalmSecure), AuthenTec, UPEK and Validity. These biometrics technologies are available as peripherals or integrated into notebooks.

OmniPass supports smart cards from major suppliers such as Gemalto, G&D, ActivIdentity, AET and the latest security chip technology being added to most laptops - the Trusted Platform Modules (TPM). OmniPass also supports authentication tokens, proximity badges and other proprietary security devices from multiple vendors. New authentication technologies are being created every day and the OmniPass Scalable Authentication Framework (OSAF) allows support for those technologies to be easily added to our product.

Centralized or Remote User Enrollment

User authentication information is stored along with the other information on the server, so that a user can be enrolled using any device from any machine. When the user tries to log into another PC in the domain, the authentication data is retrieved from the server to perform the match; the user never needs to enroll separately on the second machine. The centralized enrollment can be used for any authentication technology, fingerprint, smart cards, security token, etc. Centralized user enrollment allows users to be enrolled at a badge creation station for added security, however, OmniPass can be configured to remote enroll a user on first login if required.

Secure Windows Logon

OmniPass extends the Windows Logon protection by adding security and convenience to authenticate users with a fingerprint, smart card or other device before granting access to the Windows desktop. OmniPass enables strong authentication by allowing users to authenticate with single or multiple authentication factors. For enterprise users, OmniPass login policies are configurable per user or on a per machine basis. OmniPass provides a new Emergency Policy Override feature which allows policies to be overriden by an end user or enterprise help desk in emergency situations.

Key Features at a glance

- Secure Single Sign-On and Enterprise class Password Management including support for IE, Chrome and Firefox browsers.
- Multi-device and Multi-factor Authentication.
  - Biometrics
  - Smart Cards
  - TPM Support
  - Hardware Tokens
  - File and Folder Encryption
- Encrypted file sharing.
- VPN and certificate access.
- QuickAction support - includes QuickLaunch and Fast User Switching (FUS) support.
- Supports Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2.
- Easy to use GUI.
- Simple Installation Program.
- Simple method to import existing passwords.
- Multi-language support.
- Works with OmniPass Enterprise Edition.

Enterprise Class Password Management

For enterprises, annual costs of password management can add hundreds of dollars per user. For individuals, password management makes using a PC more complex than necessary. Whether you belong to an enterprise or you are a consumer, managing user identities and authentication has become a complex problem.

OmniPass is a powerful tool that enables you to reduce costs and conveniently manage your passwords and identities. OmniPass creates and maintains an encrypted "vault" for your passwords. The first time a password secured website or application is used; the user simply enters the original password and then tells OmniPass to "Remember that Password". From that point forward, anytime that website or application is accessed again, OmniPass will prompt the user to authenticate using the specified security devices and authentication rules. Once authenticated the OmniPass vault will "unlock" the appropriate password and grant access to the application or website, without typing a user id or a password!

The password manager of OmniPass can now support all enterprise level applications, such as terminal emulators, SAP, Oracle and others. OmniPass also supports the IE, Chrome and Firefox browsers.

QuickAction

QuickAction allows simple and quick access to functions commonly performed on a PC with an easy swipe of a fingerprint or insertion of smart card, etc. A user can configure a finger swipe to launch and login to a designated application or website, lock the workstation, or to logoff or shutdown the PC. QuickAction also allows users to easily switch between user accounts (fast user switching). For users that may not be familiar with fingerprint technology, QuickAction will launch a tutorial or help a user to enroll a fingerprint when the fingerprint sensor is touched with an unregistered fingerprint.

File and Folder Encryption

Traditional file encryption and decryption utilities encrypt/ decrypt files on-demand one file or folder at a time. OmniPass is closely tied Windows Explorer to provide a better user experience. Users browse to a specific file or folder and right click to encrypt or decrypt the selected file(s). Encrypted folders are available as regular Windows folders instead of special files.

The user can then drag and drop files and view or modify the file contents and manage encrypted folders just like a normal Windows folder! The user can also assign other users to share individual files or folders. Shared users are granted access to the file or folder after they are authenticated. When used in conjunction with a TPM device, OmniPass can secure file/folders to a given system, not allowing the files to be transferred to unsecured computers!

VPN and Digital Certificates

OmniPass allows users to access VPNs and other applications that use digital certificates (PKI). OmniPass incorporates the generation of secure digital certificates as part of the enrollment process, making the process simple for end users and enterprises that are not familiar with complicated PKI systems. Certificates generated for a user are archived on the server and automatically downloaded and installed on any computer that the user logs into. The end result is that users can protect access to their VPN logins with a fingerprint swipe, smart card or other authentication from anywhere.