OmniPass Enterprise

Secure Your Organization's Sign-Ons Today

Secure Your Organization

Whether you belong to a small or large business, security is a top priority. OmniPass Enterprise Edition allows desktops, laptops and tablets running OmniPass Client Edition to securely connect into the enterprise. OmniPass Enterprise Edition is a cost effective, server based back-end that offers enterprise wide identity and password management as well as data protection that is easily deployed and easily managed by your IT department. OmniPass Enterprise Edition provides organizations a well integrated strong authentication and identity management system that ties easily into existing infrastructures and management tools as shown below:

- Support for Active Directory
- Support for ADAM
- Support for Novell eDirectory
- A standard MMC console plug-in

Softex OmniPass is the software solution that allows enterprises to easily comply with these new security requirements. OmniPass removes weak, unsecure passwords and replaces them with strong user authentication that can be centrally managed by the IT department.

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.

Key Features at a glance

- Secure login to the PC using strong user authentication.
- Support for multi-device and multi-factor authentication including Smart Cards, Biometrics TPM and Hardware Tokens.
- Enterprise class password management and single sign-on for websites and applications to implement a completely "password free"environment in an organization. Works with all applications include SAP, Oracle and connectivity products such as 5250 and 3270 emulators as well as IE, Chrome and Firefox browsers.
- Encrypted file sharing in the enterprise. OmniPass Enterprise Edition allows encryption keys for each user to be stored in the Active Directory allowing any user in the domain to securely share encrypted data with other users without any key management or transfer.
- VPN and certificate access.
- Standard Microsoft Management Console (MMC) for managing user accounts and settings, as well as management of authentication hardware such as the TPM.
- Choice of centralized or remote enrollment for user authenticatio devices (e.g. fingerprint, Smart Card or TPM enrollment).
- Enterprise level event logging. This allows for authentication, encryption and other user operations to be logged into the Active Directory or the ADAM server. Allows IT staff to produce an audit trail of user operations to help comply with governmental regulations such as HIPAA, Sarbanes-Oxley, and Gramm-Leach-Bliley Act.
- Integrated License Management to simplify the procedure of auditing and tracking.
- Multi-language Support.
- Supports Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2.

Password Management

Data Security, user verification and password management are critical to locking down single systems and systems in an enterprise environment. “Password reset becomes a large expensive bucket of support for companies,” says Kris Brittain, a research director at the Gartner Group. According to Gartner, an employee forgets his or her password an average of four times a year and each call to a corporate help desk to reset a password costs $30 to $35.OmniPass allows an IT department to completely eliminate passwords from the organization. OmniPass provides a powerful but easy to use password wizard that allows an IT professional to create templates for all enterprise applications and websites. These templates can then be attached to a user, or a group of users eliminating the need for users to setup the login user-id and password to corporate resources Passwords can be randomly generated and the user never needs to know the actual passwords for any application or website - an authentication is the only method of access. If users don’t know their passwords, they can not forget them, thus saving the organization the cost and of passwords while strengthening access security. All accesses to corporate applications and websites can be logged for regulatory compliance with HIPAA, Sarbanes-Oxley and others.

> *“Password reset become a large expensive bucket of support for companies”*
>
> *Kris Brittain*
> *Gartner Group*

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

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.

Data Encryption

OmniPass allows users to secure individual files and folders with a fingerprint, smart card or other device. Users can simply browse to a specific file or folder and right click to enrypt or decrypt the selected file(s). An authentication is required to access data that is encrypted When used in conjunction with a TPM device, OmniPass can restrict data access to a given computer, not allowing files to be transferred to an unsecured computer. OmniPass encryption uses the existing PKI encryption technology and the Crypto API architecture that is already built into Windows.

OmniPass Enterprise Edition also supports the sharing of encrypted files and folders. Simply right click the file and select “OmniPass Sharing…” and a list of other OmniPass users in the domain is shown and access can be given to any other user. OmniPass handles all the key management so that the user does not have to worry about key exchanging or other complicated procedures to share an encrypted file or folder. The shared user must also perform authentication using his authentication rules before access to the encrypted file will be granted.

Remote Access Support

Many enterprises today are using remote access technologies like Citrix, Terminal Services and Remote Desktop Protocol (RDP) to grant users remote access to workstations andservers in the organization.Typically these technologies are not well integrated with strong authentication technologies like fingerprint, smart card and token authentication.

OmniPass provides the ability to use strong authenication to validate remote user access. The fingerprint readerconnected to the remote terminal can be used to authenticate a user access into applications and websites running in a Terminal Service or Citrix environment.

VPN & Digital Certification

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.

About Softex

Softex, founded in 1992 in Austin, Texas, is a market leader and provider of security software and solutions with innovative products focused on Enterprise Single Sign On (ESSO), Identity and Access Management (IAM), and Data Protection of Self-Encrypting Drives. Softex offers both on-premise and Cloud-based security solutions to HealthCare, Financial, Corporate, Government and OEM markets with a focus on strong user authentication and helping its customers meet industry compliance. Softex serves many of the top tier companies, such as Lenovo, Hewlett-Packard, Fujitsu, Samsung, Accenture and Motion Computing.

For more information about Softex, visit www.softexinc.com

Corporate Headquarters

Softex Inc.

9300 Jollyville Road
Suite 201
Austin, TX 78759 U. S. A.
(512) 452 8836 Main
(512) 795 8702 Fax
www.softexinc.com

Regional Headquarters

Softex Infotech Pvt. Ltd.

No. 16, Shram Sadhana Bldg.,
Hindu Colony Lane No 1,
57 Dr. D. V. Pradhan Road, Dadar (E),
Mumbai - 400014 INDIA
+91-22-2414 6432 Main
www.softexinc.com

DOC#: SFTX-DS-OPEE-V4-042915