passfaces™
STRONG AUTHENTICATION

Passfaces for Windows

Passfaces for Windows offers the strong authentication provided by Passfaces' patented technology in a Windows environment. It works in all Microsoft® Windows network environments and applications allowing network managers to replace password logons with Passfaces to increase overall network security. Passfaces access is available for local and remote desktop logon, network resource access, RAS, and terminal services. Passfaces requires Windows IIS web server for remote access.

"I Never Forget a Face"

It's true, we never forget a face. We might not be able to associate a name with a face, but the brain can recognize a face for months, or even years after the first encounter. It's that scientific fact that serves as the basis for Passfaces technology. Users are given a random set of faces (typically 3 to 7) to serve as their password. They are taken through a "familiarization process" that imprints the faces in their mind. Users then log into protected systems by selecting their assigned faces from five different groups, each containing nine faces. These groups are presented one at a time until all five of the Passfaces have been correctly identified.

Passfaces for Windows meets Microsoft's requirements for complex passwords and eliminates usability problems for end users.

How Passfaces for Windows Works

Passfaces is loaded onto your network server like any other application. Each work station within the network is required to run a small piece of code to use the application. Passfaces uses the Active Directory within the Windows operating system for access security but replaces passwords with Passfaces. A *System Administration console*, provided with the software, gives the system administrator the ability to configure and manage Passfaces functionality. Passfaces for Windows provides these administrative functions:

- Deploy Passfaces to individuals or groups
- Set number of Passfaces (1 to 7) for each user or group
- Allow Passfaces only (no passwords)
- Reset user to a known or default password

Independent Testing by Enterprise Solution Group (ESG)

ESG concluded that Passfaces is unique in the authentication market and that using the human ability to recognize faces creates a nearly infallible authentication model. The key differentiator is the harnessed power of cognometrics. The reduction in Help Desk calls requesting password resets is a quantifiable benefit.

Scores were assigned and tabulated based on a scale of 1-5 with 5, Exceeding Expectations.

Test Results

Initial Training Process 4.5
Ease of Use 5.0
Installation Process 4.0
Documentation 4.5
Support Program 4.5
Platform Availability 4.0
Cost of Ownership 5.0

Supported Servers:
Windows 2003, 2000, NT 4.0

Supported Authentication:
Local Machine, NT Domain Controller, Active Directory

Supported Clients:
Windows XP, 2000, NT 4.0, Me, 98, 95

Supported Interfaces:
Desktop logon, IIS Basic Authentication, Outlook Web Access, Terminal Services, RAS, Remote Desktop, SSL VPN

Requires Windows IIS Web Server for remote access

Passfaces for Windows is completely reliable because it is always available, offers greater network security and does not require additional hardware for authentication that can get lost or be left at home.