Passfaces for Windows offers Passfaces' patented strong authentication technology for a Windows environment. It works in all Microsoft® Windows networks and applications allowing network managers to replace or augment password logons with Passfaces to increase overall network security. It strengthens internal Windows domain security and access to Windows applications including:

- Remote email via Outlook Web Access
- Applications hosted through Citrix Metaframe
- Custom Web Applications
- Intranets and Extranets

Passfaces is a unique, out of the box, rapid deployment authentication product that can be used for both local and remote desk top logon. It eases the user burden of password complexity, reduces password related help-desk calls, and stops lost productivity caused by forgotten passwords. Passfaces has built in user training and offers low cost of ownership.

Passfaces Technology
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 end user usability problems.

How Passfaces for Windows Works
Passfaces for Windows works locally on workstations within a local area network and remotely using a standard Web browser. Passfaces' modular format lets you implement only what you need. The simple, effective administration interface makes managing Passfaces a snap and allows gradual user migration to Passfaces. Since Passfaces for Windows uses existing Active Directory user accounts, no additional user database is required. Built-in user training makes deployment fast and easy.

Product Features

- Workstation Authentication (LAN) Passfaces Client replaces Windows password logon
- Off-line authentication for roaming notebooks
- Remote Authentication (via Web browser)
- Integrates with Microsoft IIS (Internet Information Services) Web Server for remote (browser) access
- All major web browsers supported without plug-ins or software installation
- Works seamlessly with "Basic Authentication" (e.g. Outlook Web Access) or forms based authentication

Supported Servers:
Windows 2003, 2000, NT 4.0

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

Supported Clients:
Supports all versions of Windows server and client systems (2003, 2000, XP, 98, 95, Me, NT).

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 Architecture
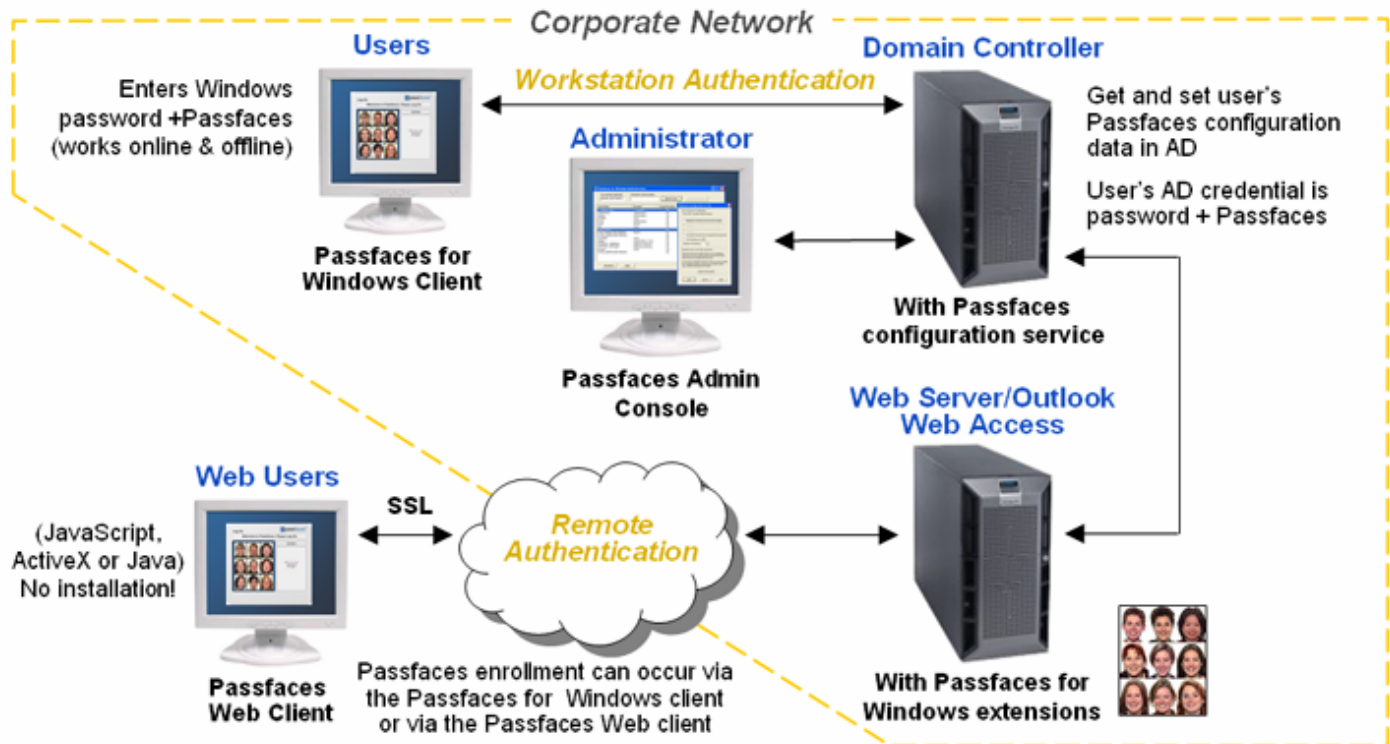
Network Module
The Network Module adds Passfaces authentication to Windows workstations. It works with Windows "cached-credentials" to support off-line authentication and supports local machines, Windows NT domain, Active Directory, terminal services and remote desktop. It is Microsoft VPN compatible and will co-exist with other replacement GINA modules. The Network Module can be used with or without the Web Services module.

Web Services Module
The Web Services Module adds Passfaces authentication to intranet sites and web applications. It is ideal for Outlook Web Access, is Citrix Metaframe compatible and can be configured to work with SSL VPNs. The Web Services Module can be used with or without the Network Module.

System Administration Console
The 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