



VeraShield

id fend VeraShield is designed as a logical access control solution to work with all Windows® network configurations, including single computer, Workgroups, single Domain controller, and multi-Domain networks. The Id fend VeraShield system extends the standard Windows® security interface layer at the operating system level by providing biometric authentication using facial recognition on top of the existing password protection.

On any login or unlock attempt to a computer with VeraShield, the User's identity is verified using face recognition.

In compliance with standard Windows operating procedures, the Id fend VeraShield system allows a user to logon to any computer within the network domain, using biometric authentication. The only noticeable difference to the user is the live video embedded within the standard logon screens. To the User, VeraShield is non-intrusive and does and not require any additional steps during the logon operation. The User performs the normal Logon procedure, entering Username and Password, however at the end of the session, the User looks towards the camera. If the User's identity is verified the Login or unlock procedure will proceed, otherwise the Login or unlock operation is denied.

In addition, the Id fend VeraShield system provides several optional features for continuous security monitoring (CSM) while the user is logged on to the network, including:

- Shutdown following failure of facial authentication (customizable by period and number of authentication attempts)
- Immediate shutdown following user absence
- Shutdown if the current logged in User is not detected
- Shutdown on detection of multiple individuals (faces)
- Shutdown on detection of a denied user (denied user may be anyone registered within a domain)

The Id fend VeraShield system is integrated with the Windows® Event Viewer which contains robust database editing facilities and associated event logging so that all biometric security operations pertaining to VeraShield triggered shutdown events are logged and retrievable by time/date, user, computer and event type.



VeraShield

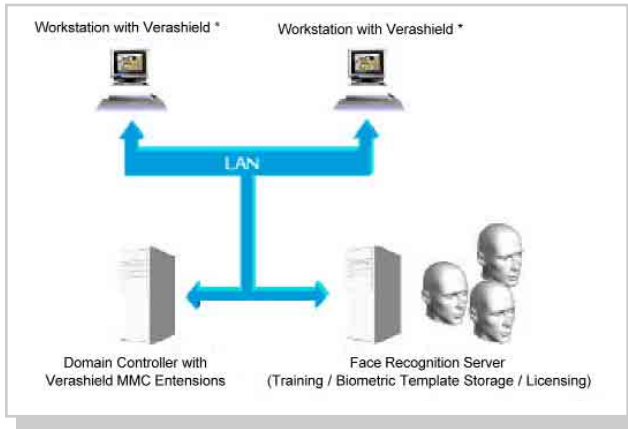
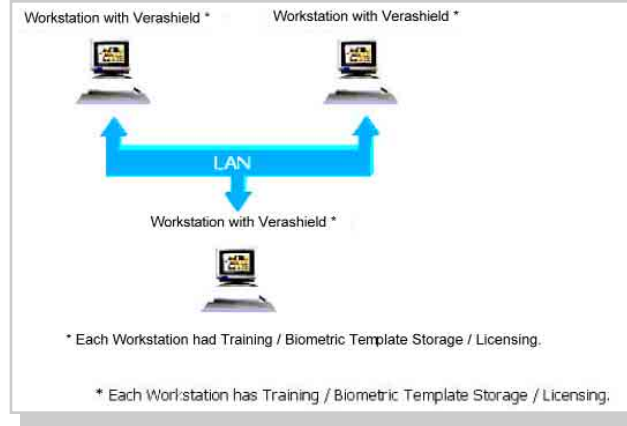
Supported Configurations

VeraShield can provide face recognition-based security in all Windows® network configurations, including single computer, Workgroups, single Domain controller, and multi-Domain networks. VeraShield can continue to verify Domain Users even when the computer is disconnected from the network. Microsoft Management Console (MMC) snap-in components customized for the Idfend VeraShield facial biometric security layer allow the LAN administrator to set all VeraShield and CSM options independently for each user (using standard MMC forms). The LAN administrator can either deny or allow individual users to customize their own security level settings.

Standalone or Workgroup Configuration

In a Standalone or Workgroup configuration, each Computer has its own Face Recognition Server installed and handles its own storage and training of User specific biometric templates. In a Workgroup, Users must be enrolled separately on each Computer. Biometric templates are not shared in a Workgroup.

Figure 1. Workgroup configuration. Each Computer operates independently. Templates are not shared.



Domain Configuration

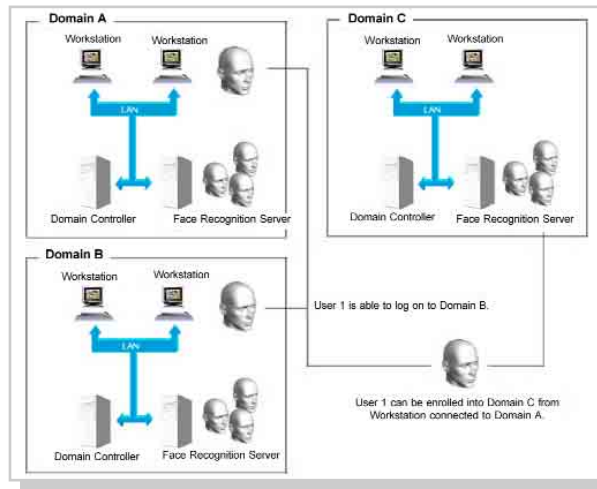
When operating in a Domain, each Computer performs verification locally, but biometric templates are stored and trained centrally within the Domain at the specified Domain Controller. Users and their biometric templates are available to the entire Domain. A Domain User may enroll at any Computer in the Domain, and be verified at any Computer in the Domain.

Figure 1. Domain configuration. Templates are stored and trained centrally.

Multiple-Domain Configuration.

Users and their biometric templates are portable across Domains if the Domains have a trust-relationship.

Figure 2. Users are portable across Domains that have a trust relationship



Continuous Security Monitoring Features

VeraShield also uses face recognition as well as motion detection to protect the User's Computer on a continuous basis, while the User is logged in. VeraShield can initiate a shutdown action if the User leaves the Computer unattended, or if a denied or anonymous person comes into the camera's field of view.

VeraShield can take one of four shutdown actions to protect the User's Computer:

- Lock the Computer.
- Log off the current User
- Shutdown the computer.
- Place the computer into hibernation (where this is applicable).

The behavior of the VeraShield logon procedure and continuous monitoring functions are identical whether the computer is part of a Domain, a Workgroup, or is Standalone.

VeraShield may also be setup to verify the User's identity on a periodic basis. If the User's identity cannot be verified following a preset number of facial verification attempts, VeraShield will initiate the specified shutdown action.

VeraShield can also be set to use motion detection to determine if a User is present. If VeraShield does not detect motion, representative of a User located in front of the camera, the specified shutdown action will be initiated. Motion detection may be enabled or disabled for any Computer.

Technical Specifications - Discovery

Database	Supports an unrestricted number of users
Speed	Average latency for Head Tracking: < 1 second One-to-one matching: < 1 second.
Operating System	Windows 2000/Servers/XP
Input	Windows Digital Media-compatible video capture device
Engram (Template) Size	8Kbytes (compressed) 12Kbytes (uncompressed).
Motion	Detects moving as well as stationary faces.
Pose	Software works optimally when matching frontal images. Face finding detects faces up to 90 degrees left and right from frontal view.
Race and Gender	No impact on performance relating to race or gender.
Idfend HNeT Engine	Learns, remembers and recognizes. HNeT emulates the human brain in structure and function, becoming more familiar with your face each time it see you, adjusting for differences due to aging and cosmetics without increasing the size of the biometrics template.
Eyeglasses	Designed to match faces with or without eyeglasses, does not support matching with sunglasses.
Lighting	Optimal performance is achieved in diffuse ambient lighting. Does not require special lighting or background. Performance is optimal when the subject is not back-lit, otherwise intensity compensation may be required.
Color and Resolution	Functions with equal performance on color or gray scale images. Operates from standard NTSC video input.
Head Size	Detect faces less than 1/10th of the height of the video frame. Recognition performance is not significantly affected by low resolution facial images.
Accuracy	The Idfend Face Recognition System was the most accurate technology tested in the International Biometric Group's Round Three Comparative Testing for IT Security and E-Commerce. Idfend scored 0% False Acceptance Rate, meaning that it caught all imposters and also scored an excellent False Rejection Rate of 3.1%.*

*Testing conducted in 2001

Requirements

Operating Systems

- Microsoft® Windows® 2000 Professional
- Microsoft® Windows® 2000 Server
- Microsoft® Windows® 2000 Advanced Server
- Microsoft® Windows® XP Professional

Hardware

- 256 MB RAM
- 1.0 GHz Intel® Pentium® 4 Processor
- 20 GB Hard Drive
- Windows® Digital Media-compatible video capture device
- 10 Mb network adapter (for network versions only)

VeraShield does not currently accommodate the following features of Windows® 2000 Professional and Windows® XP Professional. However, note that security is never compromised.

- Not compatible with automatic login procedure.
- Does not accommodate password expiry warning.