

PREVIEW

BioLogon™ Suite

FINGERPRINT IDENTIFICATION TECHNOLOGY

Improved Security at the Touch of Your Finger

Convenient to Install and Use

- The absolute in user authentication security
- Installs easily from CD-ROM
- User friendly
- Easily matches varying finger presentations
- Instantaneous response
- Configures with selectable domain/server/workstation protection
- Uses familiar interfaces and Wizards

A NEW STANDARD IN SECURITY FOR DESKTOP, NETWORK ACCESS, AUTHENTICATION, APPLICATIONS, FILE PROTECTION AND ENCRYPTION

BioLogon™ Suite provides the highest level of security available. At the touch of your finger, you will be able to gain access to systems, lock applications and enable encryption procedures. The BioLogon Security Suite System eliminates passwords and uses the optimum personal identifier for user authentication: your fingerprint. Like the BioLogon 1.0 system, the BioLogon 2.0 family of products uses the fingerprint biometric to add definitive personal identification to access protection.

Purchase the complete suite or combine the BioLogon 2.0 primary network / client system access control product individually with the add-on application modules. We are proud to introduce these new products:

- **BioLogon™ 2.0** OS logon security system for the network with enhanced security policies
- **BioShield** a unique application that allows the user to protect any application with the touch of a finger
- **BioCrypt** protects data and messages by using your finger to encrypt a document
- **BioCard** combines fingerprint and a smart card to provide the ultimate in privacy and security

BETTER THAN PASSWORDS

System security is a growing concern today. Password security systems have inherent flaws. People forget passwords, they lose them, or an outsider steals them. And correcting the problem diverts valuable systems administration time and money from more productive activity. The BioLogon™ Suite of products replaces passwords with a system that is unparalleled in ease of use and security, more than any other authentication system. The user simply places an index finger on the scanner and Identicator's robust applications and fingerprint matching and enabling technology verify, lock and activate encryption products within milliseconds. You get a more secure access, and you get it faster than a password can be typed!

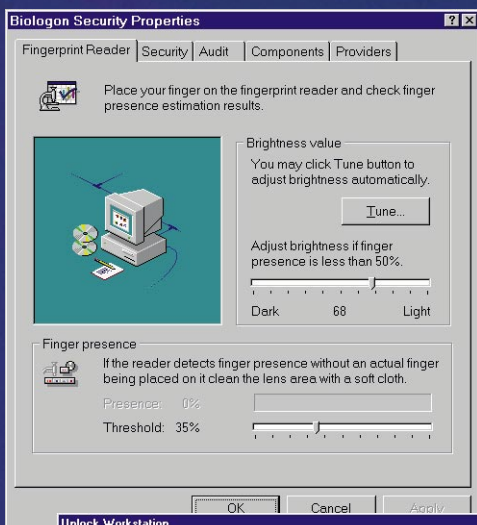


BioLogon™ Suite

FINGERPRINT IDENTIFICATION TECHNOLOGY



New Features
and Functions



BioLogon 2.0's many enhanced features and functions provide the ultimate in personal authentication security systems for the network and client workstation.

- Two finger enrollment
- Flexible security policy: choice in configuring how users access the enterprise network or local computer
 - Fingerprint only
 - Fingerprint and password
 - Fingerprint or password optional
 - Password only
- Remote system administration
- Fingerprint validation on any domain controller
- Automatic load balancing for fingerprint authentication
- Encrypted data exchange between the workstation and domain controller using Microsoft Crypto Provider

Simplifies Administration

- Integrates policy management into Windows NT User Manager, eliminating the need to learn new administration tools
- Increases flexibility in security policy management
 - Provides choice in how users access the enterprise network or local computer
 - Offers choice between enterprise-wide security procedure or individual desktop security
 - Allows Remote System Administration so that the system administrator can configure security policy and security level on remote Windows NT or 95/98 workstations
 - Validates fingerprints on any Domain Controller, not just Primary Domain Controller
- Enables system-wide administration from the system administrator workstation, which can then be easily distributed with Enterprise silent install
- Performs automatic replication of biometric data to Backup Domain Controllers without administrative attention
- Performs remote user enrollment without administrative attention, in less than 15 seconds, from the user workstation

Family Suite of Products

BioShield

Protect any application with the touch of a finger. BioShield requires no custom programming. If the application is already protected with a password, the user can use the fingerprint instead of the password. A password-protected application can be configured by BioShield to remember the password and insert it automatically into the application when the user's fingerprint is verified.

Using the BioShield toolbox, the user can attach fingerprint verification to the following elements:

- Application start-up: the application will not start until the user is validated through his fingerprint
- Menu item: if the menu selection is protected with BioShield, the user's fingerprint is required to use the selected menu item
- Button: any button in the application, toolbar or dialog can be protected by BioShield

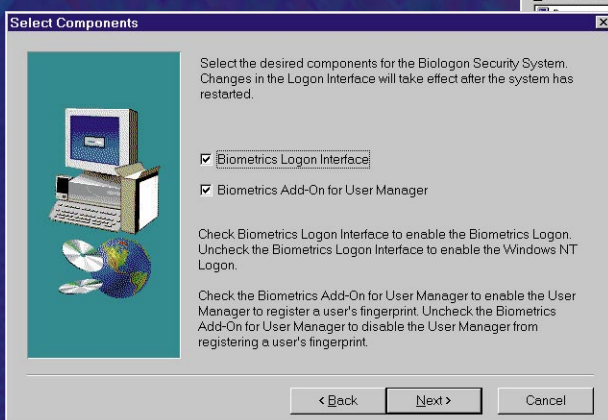
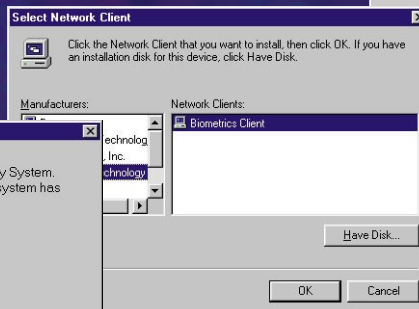
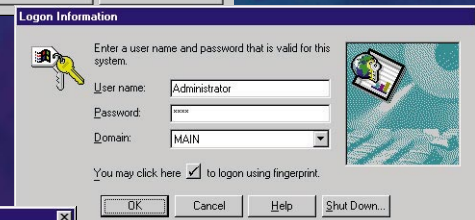
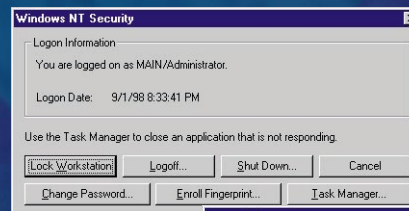
BioCrypt

Generate extensive encryption and decryption algorithms with the touch of your finger. BioCrypt encrypts user data and requires the user's fingerprint for decryption. Files are easily encrypted/decrypted right out of Windows Explorer. Multiple files and directories can be selected and encrypted or decrypted for a single operation. The encrypted files can be opened by an associated application (such as doc files with Microsoft Word) when the user presents his fingerprint.

BioCard

BioCard combines the use of a smart card with the protection of fingerprint identification. The fingerprint unequivocally ties the user to the smart card to create a closed loop security product. BioCard also makes it possible to store confidential or proprietary information on the card itself. BioCard can also be used for two factor authentication access to networks or desktops.

- Centralized security policy management for flexible security configuration
- Storage of encrypted biometric data on the card
- Enrollment options
 - User can enroll himself on the smart card using Self-enrollment Wizard
 - System administrator can enroll the user via the User Manager



IDENTICATOR
TECHNOLOGY

Operating System Platforms

- Windows® 95
- Windows® 98
- Windows NT® 4.0
- Available for Novell® Netware® in Q1 1999

Available Languages

- English
- International English
- French
- German
- Japanese
- Spanish



CALIFORNIA OFFICE CORPORATE HEADQUARTERS

1150 Bayhill Drive
San Bruno, CA 94066
Phone 650-873-8650
Fax 650-873-8653
idc@identicator.com

WASHINGTON, DC OFFICE

12300 Twinbrook Parkway, Suite 420
Rockville, MD 20852
Phone 301-468-2444
Fax 301-468-6455

System Security Architecture

- Enterprise logon
- Domain Trust organization and relationship
- Decentralized user administration
- Remote administration of the biometric workstation
- Biometrics data stored encrypted with Microsoft Default or Enhanced Crypto Provider
- Three-phase transmission protocol to send encrypted biometric data across the network
 - Support for strong encryption
 - Session key changes every minute
 - Private/public key pair changes every 24 hours
- Support for the automatic biometric data replication to BDC
- Support for fingerprint validation on any domain controller
- Support for automatic load balancing if there are multiple domain controllers

System Requirements

- 486/66 system or better
- 16MB of RAM
- CD-ROM drive
- Available parallel port for fingerprint reader
- Microsoft® Windows 95/98 with IE 3.02 or later
- Microsoft Windows 95/98 OSR2 or Microsoft Windows NT 4.0 with service pack 4
- Identicator reader required
- Pentium II processor recommended for optimum performance

