

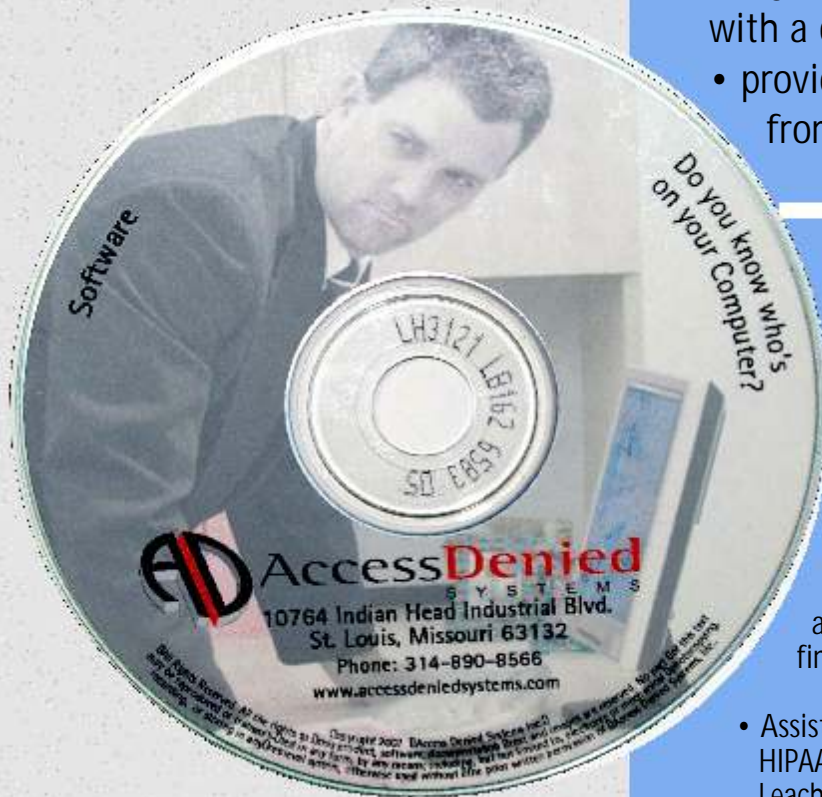


Access DeniedTM

S Y S T E M S

Mercury EnterpriseSecurity SystemTM (SWMRCS)

Enterprise End-Point Security Management Tool



The Mercury EnterpriseSecurity System will:

- integrate workstation security with a central location
- provide user security monitoring from a central location
- Reduces costs associated with password management and helps minimize desk calls regarding passwords.
- Provides multi-factor security to control the growing threat of insider/employee data theft.
- Enhances customer confidence around securing personal and financial data.
- Assists with regulatory compliance, i.e., HIPAA, Sarbanes-Oxley Act, Gramm Leach Bliley Act.
- Utilizes the Active Directory within Windows 2000 or 2003 Server to maintain control of the workstations.
- Compatible with all of the various ADS endpoint security options.

Internal data security threats are no longer just an IT issue, but a business survival issue

The Mercury EnterpriseSecurity System™

Contains: (Model SWMRCS)

- Mercury Enterprise Security System Software (on CD)
- Mercury Enterprise Security System Manual (on CD)

Technical Specifications

System Requirements

Operating System Requirements: Windows 2000 or XP
Ports: 2 USB Ports
Disk Requirements: 15MB Free Space on C: Drive, CD Drive
Computer: IBM or Compatible
CPU: Pentium III or newer
RAM memory: 256 MB or greater

Base Receiver

Operating System Requirements: Windows NT, 2000 or 2003 Server with Active Directory setup and running
Disk Requirements: 15MB Free Space
Computer: IBM or Compatible
CPU: 166 MHZ or faster
RAM memory: 256MB or more

The Way It Works

Mercury EnterpriseSecurity System™ is a client-server based system that integrates each of the workstations' individual Access Denied Systems security solutions such as the ProximitySecurity System, the Bio ProximitySecurity System, the Bio SonarSecurity System or the ADS Passive ProximitySecurity System into a homogeneous endpoint security solution with a centralized management tool.

The Mercury Enterprise Security System resides on the current network server and extends the Active Directory to store all configuration information, for the various endpoint solutions, including biometric and tag information for the user on the Domain level. Utilizing the Active Directory requires the biometric information to be entered only once per user and makes it available anywhere on the network as long as the computer is a member of the domain and has an Access Denied Endpoint solution.

For Domain Users, The Mercury Enterprise Security System encrypts both badge and biometric information with a special encryption algorithm and stores the data within the Active Directory.

For local users, the information is encrypted with a special encryption algorithm and is stored in the registry. Passwords are also stored in this encrypted form. The workstations are configured with the Proximity Security System, the Bio Proximity Security Systems, the Bio Sonar Security System or the ADS Passive Proximity Security System. Each network may have an unlimited number of workstations and workstations may have different ADS security systems attached.

All the configurations and controls of the workstation are configured, maintained and monitored via the Active Directory. Event logs detailing the workstation usage are created and may be printed out with the Active Directory reporting function.

Key Benefits

- Single point management functions for endpoint Access Denied Systems solutions.
- Monitoring reports maintain logs of workstation and user activity.
- Ease of computer security maintenance and eliminating passwords for end users results in high user acceptance.
- Reduce support calls regarding password issues.



Access Denied
SYSTEMS

© ADS Inc. 2008 - All Right Reserved

Access Denied Systems, Inc.

10764 Indian Head Industrial Blvd.

St. Louis, Missouri 63132-1102

Phone: (314) 890-8566 Fax: (314) 890-9949

www.accessdeniedsystems.com