

Modules.

IWS Desktop Security Content Manager ensures privacy and 100% data integrity of files by allowing users the option to encrypt and decrypt file content without restrictions to the number of files that can be secured or unsecured. IWS Desktop Security Content Manager module works on the file level and performs file encryption independent of Microsoft® Windows Encrypted File System (EFS). To safeguard against automated attacks, password attempts are limited before the application must be restarted.

IWS Desktop Security Depot for Windows® Applications captures and registers all password information and provides quick and efficient logon to password protected applications, preventing unauthorized users from gaining access to personal or critical files. Utilizing the TPM chip, IWS Desktop Security Depot for Windows automatically encrypts and stores appropriate username and passwords in a central repository, replacing the use of redundant and complex passwords with one master TPM protected password for all applications. Follow the intuitive wizard and register each password to simplify practical and complex passwords.

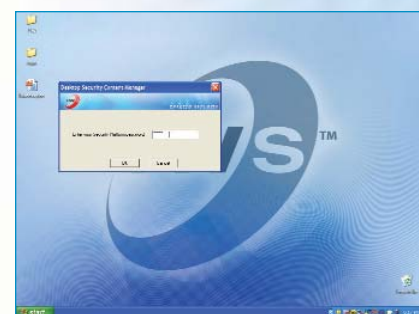
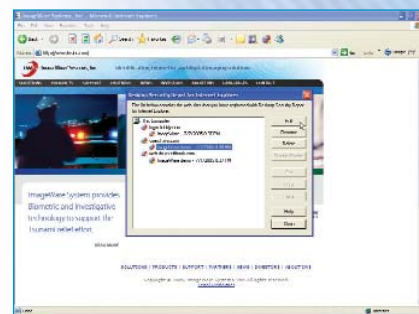
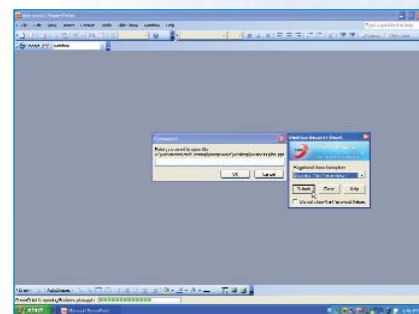
IWS Desktop Security Depot for Internet Explorer stores username and passwords in the central repository for various Web sites, allowing quick and easy enrollment and single sign-on. After user registration, IWS Desktop Security Depot will automatically provide the settings for future logon. Each IWS Desktop Security Depot account is unique allowing users to have more than one IWS Desktop Security Depot account for a single application or Web site and each account is associated with a description unique for that log on. Stored username and passwords can easily be viewed, edited, deleted and re-registered.

Highlights.

- Enhance network/systems security and protect against unauthorized access to sensitive data with strong user credential and data management on the client side
- Improve user convenience with single sign-on and password management
- Support government regulations such as HSPD-12, HIPAA, Sarbanes-Oxley and other federal requirements and compliance standards
- Ensure business continuity and data security through strong authentication methods incorporating biometrics, TPM chips, smart cards and USB tokens
- Fully localizable

Feature Benefits.

- Support for multiple biometric, smart card and USB token devices
- Integration with IWS™ Biometric Engine™ for searching and match capabilities (1:1, 1:N, X:N and N:N)
- Integration with IWS™ EPI™ Builder for the production and management of secure credentials such as PIV and FIPS 201 cards
- Support for both BioAPI and BAPI standards
- Supports a single sign-on feature that securely manages Internet Explorer, Windows application ID and password information
- Supports file encryption features
- Supports various operating systems, including Windows XP Pro and Windows Server 2003



Ask how our consulting services can help optimize your IWS Desktop Security configuration.

Please contact sales@iwsinc.com or call **800.842.4199**