ProtectDrive

Administration Guide

Revision: A01

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

Copyright

Eracom Technologies
28 Greg Chappell Drive
Burleigh Heads, Queensland 4220
AUSTRALIA

	National	International
Voice:	(07) 5593 4911	+ 61 7 5593 4911
Fax:	(07) 5593 4388	+ 61 7 5593 4388

Website: www.eracom-tech.com

Disclaimer

Eracom makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Eracom reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon Eracom to notify any person or organization of any such revisions or changes.

Publication Improvements

Eracom invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be dispatched to the above address.

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation consisting of the following two (2) documents:

ProtectDrive User Manual	This document represents a subset of the ProtectDrive Administration Guide. All end-user functionality of ProtectDrive is covered in this document. This does not include any of the System or User Management, Hard Drive Decryption or Disaster Recovery functionality as these topics were reserved for the Administration Guide. Topics such as the User Authentication, User Password Management, Hard Drive Encryption and ProtectDrive Data Backups are covered in this document. This document allows End-Users to understand how to operate ProtectDrive. It allows System Administrators to better prepare users for the every day operations of ProtectDrive.
ProtectDrive Administration Guide	This document concentrates on all aspects of deploying and operating ProtectDrive in networked and stand-alone Widows environments.

If you encounter a technical issue that you can not solve, please contact your supplier or Eracom Support.

Eracom Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Eracom and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact details:

Within Australia: 1800 63 4796
International : +61 7 5593 4796 (See your support certificate for toll free numbers)

email: support@eracom-tech.com

Revision History

Revision	Release Date	Description
A00	August 2005	A14 User Manual was restructured into ProtectDrive Administration Guide (Rev A00) and ProtectDrive User Manual (Rev B00).
A01	October 2005	Implemented new installer, updated disaster recovery.and troubleshooting

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Chapter 1
Introduction

Product overview

In today's computing environment hard drives (HDD) have become mass repositories of proprietary information. The widely used Windows operating systems provide adequate system privacy whether on a stand-alone machine or a networked computer. However, insufficient data security protection exists in a case of system (or HDD) loss due to malicious intent. Unless appropriate data protection measures are taken, any HDD can be removed from the system, and data on it can be read. Furthermore, the system can be accessed via its Floppy Disk Drive (FDD), Serial (COM), and/or Parallel (LPT) ports. To bridge these data security gaps Eracom has developed ProtectDrive (PD) system security and data encryption application.

Eracom ProtectDrive is a multi-user Windows Active Directory aware computer security application that provides the following functionality listed in order of appearance during normal ProtectDrive operation:

Preboot User Authentication	Used to derive unique decryption keys for decrypting the operating system files and the rest of the encrypted hard drive(s). Support for Smartcards and Tokens as well as Windows Domains Usernames and Passwords.
Preboot Password Fallback, Password Recovery, and New User Introduction	Smartcard/Token user password fallback and Windows Domain user preboot password recovery procedures including new user introduction at preboot.
Single Sign-On or Manual Windows Authentication	ProtectDrive provides Automatic Windows (Domain) user authentication following successful preboot authentication. Manual authentication is also available as an alternative.
Configurable System and User Policy	FDD, COM, LPT device access control. Policy management using the MMC Snap-ins. Automatic System and User Policy data replication from the server.
Hard Drive Encryption	Strong data encryption made completely transparent to the user.
Disaster Recovery Tools	MS-DOS utilities used to recover corrupt and/or inoperable systems.

Who should read this document?

This document is intended for System Administrators planning to deploy ProtectDrive on stand-alone as well as networked multi-user computer systems with either single-boot or multi-boot configurations.

Chapter 2
ProtectDrive Functional Description

Supported Preboot User Authentication Credentials

In order to boot an encrypted operating system partition ProtectDrive needs to get access to the *Decryption Keys* prior to the operating system boot. These keys are used for decrypting the operating system files as well as the rest of the encrypted hard drive(s). For this purpose ProtectDrive introduces the *Preboot User Authentication.* The decryption key is encrypted by a unique data key derived from the user authentication credentials. After user authentication the disk key can be decrypted and the operating system can be loaded. In support of this functionality ProtectDrive maintains its own *Preboot User Database* (dB).

The ProtectDrive Preboot User dB has the following characteristics:

Maximum Number of Users/Certificates	200
Username Length/Syntax	1-20 characters
Password Length/Syntax	6-20 **case-sensitive** characters

ProtectDrive is capable of preboot authenticating users on stand-alone (Local Windows only) as well as Windows Domains systems. The following user authentication credentials are supported by ProtectDrive:

Smartcard/Token and PIN

This requires the presence of a Public Key Infrastructure including: Active Directory Service, Token Runtime Environment, and the Certification Authority Service.

ProtectDrive supports the following Token Runtime Environments: eToken Base Cryptographic Service Provider, Schlumberger Cryptographic Service Provider, Siemens Card API CSP

Username/Password/Domain Name

This method of user authentication is used on both Windows Domains and Local Windows systems. On Local Windows systems the Domain Name represents the Local System Name. Total number of domains including the Local System Name can **not** exceed **150**.

Misplaced/Forgotten User Authentication Credentials

ProtectDrive will accommodate users who have misplaced their authentication credentials. This refers to such instances where a user has misplaced their Smartcard/Token or forgotten their Windows Domain Password, for example. ProtectDrive System Policy provides automated procedures for handling these preboot authentication scenarios.

Unattended Reboot Followed by Automatic Preboot Authentication

Various system administration functions not related to ProtectDrive may at times require an unattended reboot followed by automatic preboot authentication. ProtectDrive provides this functionality with the use of a special User Account. System Registry amendments are required to implement this functionality.

Windows User Authentication

Single Sign-On

ProtectDrive System Policy can be configured to *automatically* authenticate users to Windows. Users are automatically logged on to their respective Windows Domain or Local Windows accounts following their successful preboot authentication. This method of automatic Windows authentication is referred to as Single Sign-On.

Manual Windows Authentication

As an alternative to the Single Sing-On mode ProtectDrive System Policy can be configured to provide standard Windows authentication screens allowing the user to manually authenticate into their respective Windows (Domain) account.

Hard Drive Encryption and Decryption

All data encryption is invisible (transparent) to the user. ProtectDrive automatically encrypts and decrypts multiple HDD partitions. When encrypted data is being read from the HDD, ProtectDrive decrypts it “on the fly”- ready for display to the user or for use by other applications and software processes. All data written back to the HDD is automatically re-encrypted. Consequently, normal system operation remains unaffected.

Configuring ProtectDrive System and User Policy

Windows Domain client ProtectDrive System Policy can be managed remotely using the **Microsoft Management Console (MMC) Active Directory Users and Computers Snap-in**. ProtectDrive automatically applies System Policy to individual systems from the Domain Controller. Active Directory Schema Extensions implementing the **PD Settings** are automatically deployed during installation of the ProtectDrive Server-Side Components.

System Policy can be managed locally using the ProtectDrive **Local Machine Configuration Utility** deployed as part of the installation of the ProtectDrive Client-Side Components.

Users are assigned to client systems as well as user device access permissions are configured using the **PD Users Tab**. User Policy defines individual user access permissions to the floppy drive(s), COM and LPT ports. User Policy is automatically replicated from/to the Active Directory.

ProtectDrive Disaster Recovery

Disaster recovery preparation begins with periodic ProtectDrive system data backups. The ProtectDrive backup utility creates **Recovery Files**, which can be used to later decrypt a failed system. These files must be stored off the client system.

ProtectDrive also provides a set of command line **Recovery Tools** used to perform disaster recovery tasks such as data decryption and Preboot User dB management. These Recovery Tools are included on the ProtectDrive distribution CD.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 3
System Requirements

Minimum Hardware Requirements

- 32-bit Intel-compatible CPU computer system
- 32 MB of RAM
- CD ROM drive or access to a server based installation directory
- 10 MB of free disk space on drive **C:**

Supported Storage Hardware

ProtectDrive encrypts/decrypts all fixed (non-removable) system HDD partitions with a drive letter assigned (no hidden partition support).. This includes all IDE/EIDE, SATA, SCSI drives and RAID arrays. ProtectDrive does not in anyway interfere with the normal operation of the storage sub-system with the following exceptions:

- It is not possible to format any partition on the system HDD.
- ProtectDrive does not support post-installation addition, removal, or substitution of hard drive(s).
- During installation ProtectDrive accounts for all partitions present on the system. Post-installation partition resizing, converting, masking active or re-partitioning is not supported. This includes the Master Boot Record manipulation.

Floppy, CD/DVD Devices and COM/LPT Ports

3.5” FDD are excluded from encryption/decryption. However, ProtectDrive controls configurable user Read/Write privileges to these devices. Post-install addition, removal, or substitution of FDD is fully supported. ProtectDrive accounts for the total number of FDD in the system and does not interfere with their normal operation

All removable devices or media devices such as CD-RW, DVD-RW, and Iomega Zip Drive are excluded from encryption/decryption. ProtectDrive does not interfere with the normal operation of these devices.

ProtectDrive System Policy and User Policy provide configurable default and individual user access rights to all Floppy Drive(s), COM and LPT ports.

Supported Operating Systems

ProtectDrive has been tested and works with the following Operating Systems:

- Windows 2000 Pro, Service Pack 4 (SP4)
- Windows 2003 (SP1) (only the ProtectDrive Server Component is supported)
- Windows XP Pro Build 2600, SP1 and later

ProtectDrive supports the use of FAT, FAT32, NTFS4, and NTFS5 file systems.

Please note that MS-DOS can be used during ProtectDrive Disaster Recovery. Inaccessible or corrupt ProtectDrive systems can be booted to MS-DOS from a floppy disk or CD-ROM. Drives that require special DOS drivers (e.g. SCSI) or TSRs are only accessible to the ProtectDrive Recovery Tools, if the respective drivers are loaded.

Supported Networks

ProtectDrive is Active Directory aware and fully supports Windows Domains. It does not interfere with normal operation of any of the Windows network services including Remote Desktop connections. Windows Domain as well as Local Windows users are able to authenticate successfully into systems secured by ProtectDrive.

All hard disk partitions encrypted with ProtectDrive are configurable as shared volumes at the discretion of the System Administrator.

ProtectDrive will not interfere with user authentication via the Novell Netware client.

Chapter 4
ProtectDrive Software Compatibility

ProtectDrive has been tested and does not interfere with normal operation of most MS Windows compliant software, applications, services, and utilities. Some care needs to be taken, however, when using the following:

DOS Drivers and TSRs

When booted from a DOS floppy (or CD) ProtectDrive sees hard disks accessible via DOS drivers and TSRs if the appropriate drivers are loaded.

Windows and 3rd Party Boot Managers

At system start-up ProtectDrive manipulates the Master Boot Record (MBR) while verifying its integrity. All software that needs to manipulate the MBR for its own purposes is **incompatible** with ProtectDrive. This also applies to the standard Windows boot manager.

Windows Disk Manager Utility

Any post-installation disk repartitioning, resizing, and mirroring configuration changes are prohibited by ProtectDrive. If any of the above operations are required decrypt all disks and uninstall ProtectDrive before proceeding.

Windows Folder Compression Utility

Windows folder compression is fully supported with one exception. The ProtectDrive system files directory (**C:\SECURDSK**) must not be compressed. Compressing this directory will interfere with the normal operation of ProtectDrive.

Windows System Restore Utility

Windows System Restore points created prior to the ProtectDrive install are rendered useless. System can only be restored to any restore point created following the ProtectDrive install.

Windows Fast User Switching Utility

ProtectDrive disables the standard Windows "Welcome" screen along with its fast user switching functionality.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 5
Deploying ProtectDrive

Before You Begin

Storage System Preparation

Before deploying ProtectDrive ensure that your data storage system is well planned, and that no further rearranging of any of the partitions will occur. Use Windows Disk Management as needed to repartition, set up disk mirroring, resize partitions etc.

Run **`CHKDSK /f`** to ensure file system health on all drives intended for encryption.

Backup all important data in case of a power failure during the ProtectDrive install. This may render the storage system inaccessible.

Registration Disk Preparation

When you purchase a copy of ProtectDrive, Eracom will provide a floppy diskette containing Recovery Keys (**`SYSKEY.BIN`**) issued by Eracom. Should this diskette be misplaced or damaged, Eracom will replace it based on your original registration *Serial Number*. This disk is required during each install and uninstall of ProtectDrive. It is also required in preparation for the ProtectDrive Network Roll-Out installation.

Recovery Disk Preparation

Eracom recommends the creation of a Recovery Disk (floppy or CD) containing the ProtectDrive Recovery Tools and Recovery Keys. This disk is required by the:

- ProtectDrive Disaster Recovery Tools
- Preboot Password Recovery Procedure
- New User Preboot Introduction Procedure

Follow these steps to create a Recovery Disk.

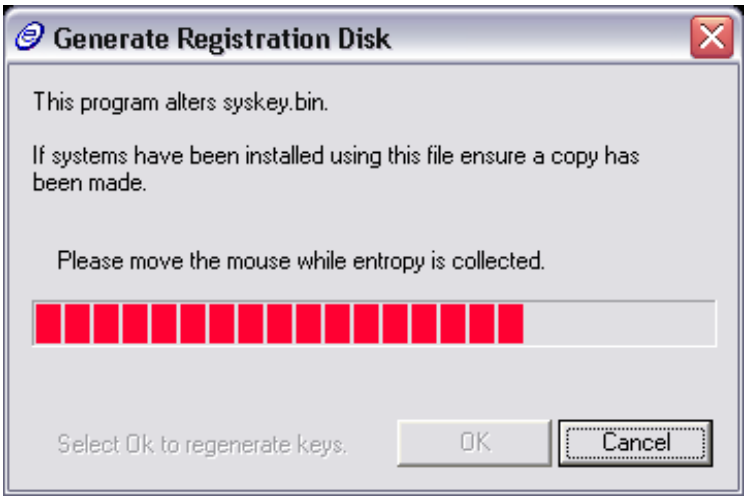
1. Copy **`SYSKEY.BIN`** to a floppy.
2. Copy the ProtectDrive Recovery Tools from the **`\RECOVERY`** directory on the ProtectDrive distribution CD-ROM.

Creating Custom SYSKEY.BIN

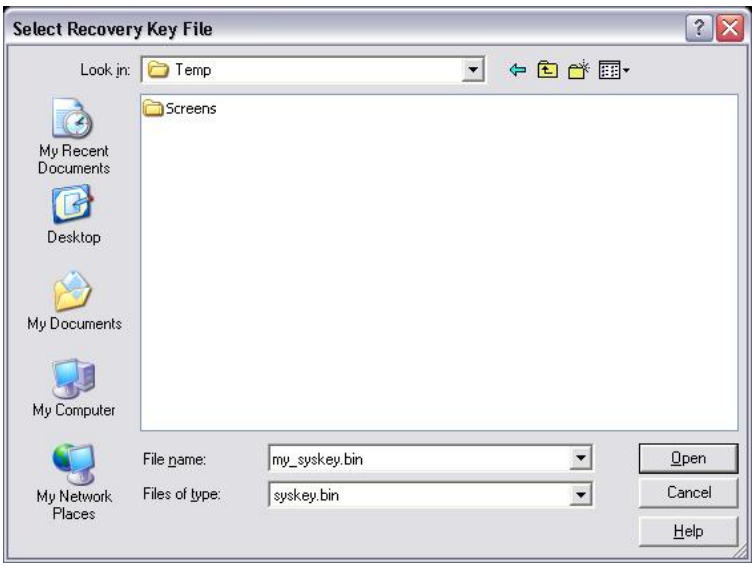
Eracom provides **GENRKEYS.EXE** utility for creating custom Recovery Keys. Recommended procedure is as follows:

Make a backup copy of the Eracom provided floppy containing **SYSKEY.BIN** files.

Run **GENRKEYS.EXE**. The system will proceed to collect entropy for the random number generator. Once completed press OK.



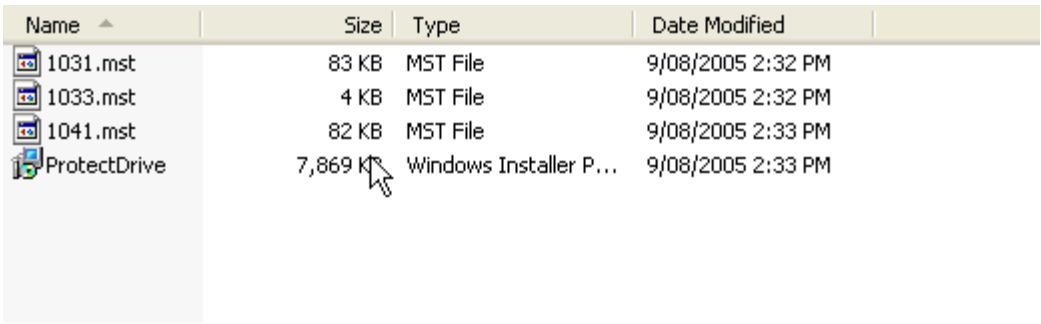
Provide the system with a copy of the floppy made in step 1 above. The newly created **SYSKEY.BIN** will be saved.



ProtectDrive Install (MSI) Package

ProtectDrive is deployed using a Windows Installer (MSI) package. The following files will install both the ProtectDrive Server-Side and Client-Side components.

Configuring the Active Directory Group Policy Object responsible for automatically launching the **`PROTECTDRIVE.MSI`** will result in the Network Roll-Out of ProtectDrive to multiple client systems.



Customizing the MSI Package

If silent installation is desired (e.g. Group Policy Object deployment), System Administrator needs to set all the required parameters of the **Property** to require no user interaction during installation. This may be achieved by modifying the MSI package. MSI is a database table and System Administrators can tune the **`PROTECTDRIVE.MSI`**.

There are number of tools publicly available for this task. Microsoft provides free database tool called Orca, for example.

`http://support.microsoft.com/kb/255905/EN-US/`

The following **Properties** effecting the installation are modifiable:

ERA_CIDKY_PATH	The absolute path that contains **`CIDKEY.CID.`** ProtectDrive installation looks for this file in the current folder where **`PROTECTDRIVE.MSI`** located. However, you can modify this path to the desired location. E.g **`\\SERVER\SHARE`**.
ERA_INSTALL_TYPE	**`Client (default)`** for client installation, **`Server`** for server installation, and **Server1** for sever installation without the schema extensions.
ERA_INSTALL_AD_COMPOBJ_SNAPIN	Set to (0) by default. Set it to (1) to install the Active Directory Computer Object Snap-in
ERA_INSTALL_AD_USEROBJ_SNAPIN	Set to (0) by default. Set it to (1) to install the Active Directory User Object Snap-in.
ERA_INSTALL_ADMIN_GUIDE	Set to (0) by default. Set it to (1) if you wish to install the ProtectDrive Administration Guide.
ERA_INSTALL_CLIENT	Set to (1) by default. Set it to (0) **not** to install the Client component. This is also set to (1) automatically if **ERA_INSTALL_LOCAL_MC** is set to (1).

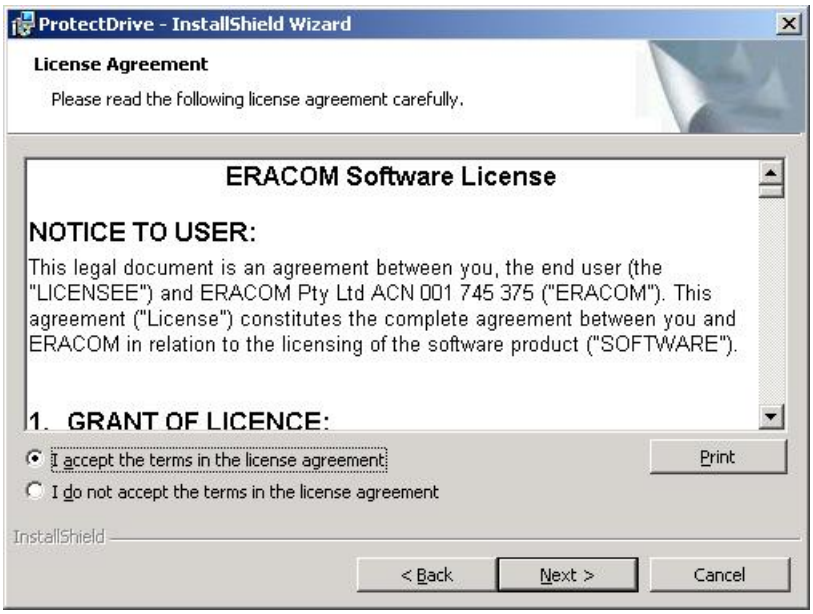
ERA_INSTALL_KEY_RECOVERY	Set to (0) by default. Set it to (1) to install **RPADMIN.EXE.** See Chapter 9 - Extraordinary Authentication Scenarios for additional information.
ERA_INSTALL_LOCAL_MC	Set to (1) by default. Set it to (0) **not** install the **Local Machine Configuration** utility.
ERA_INSTALL_USER_MANUAL	Set to (1) by default. Set it to (0) **not** to install the ProtectDrive User Manual.
ERA_SELECTED_CSP	The desired and installed Cryptographic Service Provider for this installation. If you use Smartcards or Tokens, you need to set this. This value must be one of those listed in **ERA_SUPPORTED_CSPS** (see below)
ERA_SUPPORTED_CSPS	ProtectDrive will only support Cryptographic Service Providers listed in this property.

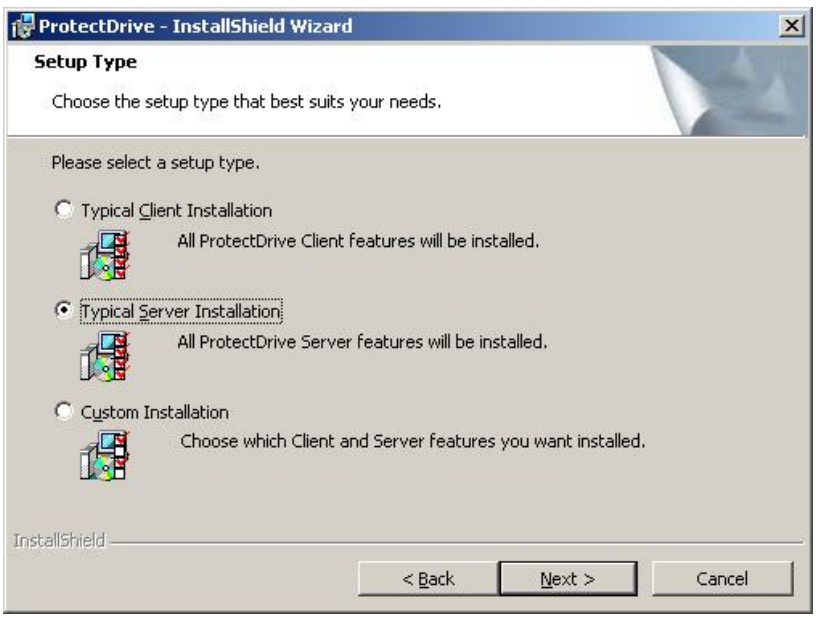
Deploying Server-Side Components

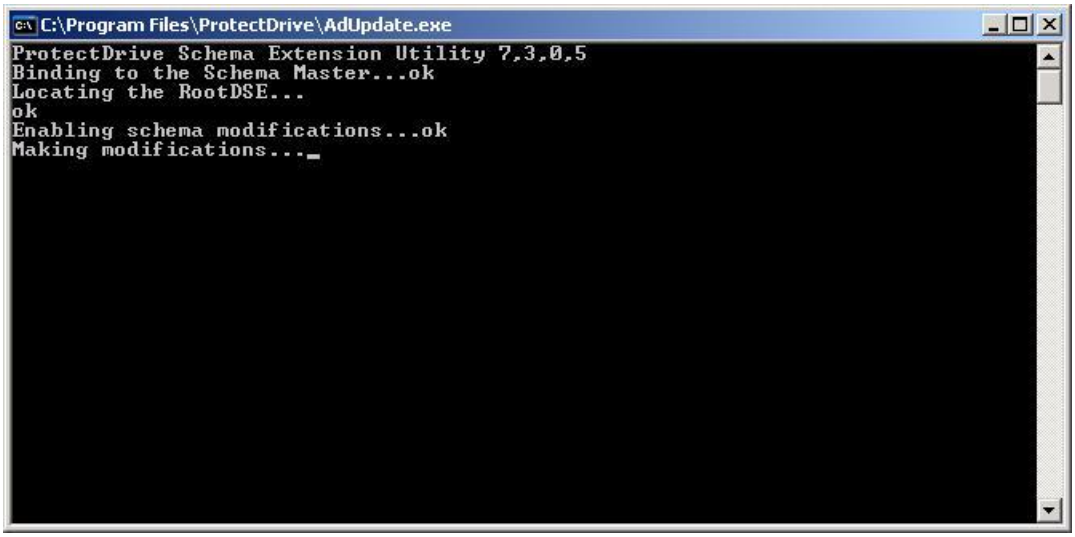
Installing the Active Directory Schema Extensions

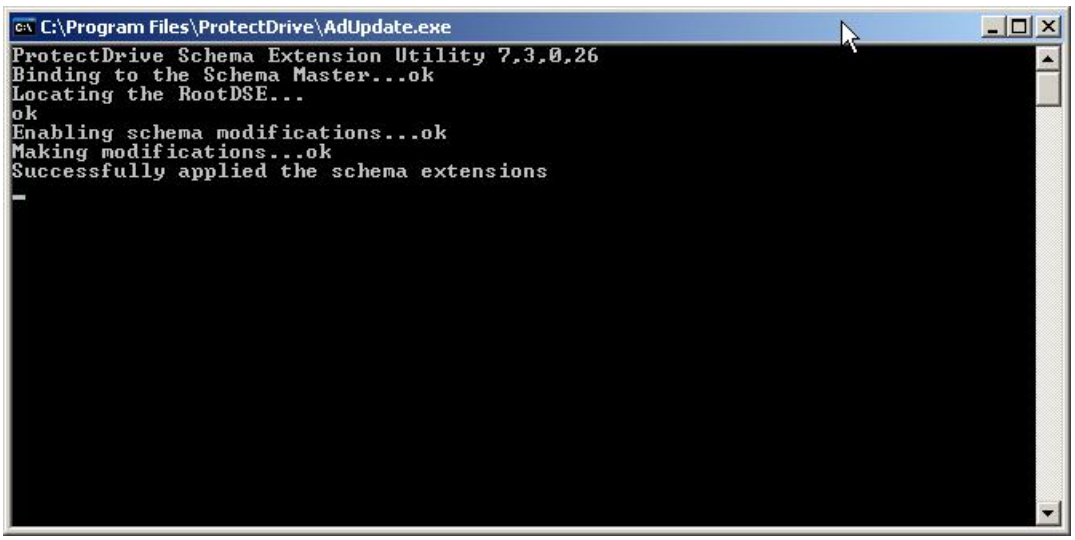
Please note that ProtectDrive Server-Side Components are used exclusively for System and User Policy management via the Windows Active Directory Service. If securing and/or encrypting the server resources is desired, please install the ProtectDrive Client-Side components on the server, then manage ProtectDrive installed on the server as any other ProtectDrive client system on your network.

Launching the **`PROTECTDRIVE.MSI`** will result in the display of the ProtectDrive installation wizard. The wizard automatically installs all ProtectDrive Server-Side components with minimal user interaction as follows:









At this point the Schema has been amended to include features used for management of ProtectDrive client System and User Policies.

Deploying Client-Side Components

ProtectDrive Client-Side components are used for management and encryption of ProtectDrive stand-alone and/or networked systems (members of a Windows Domain).

Note: When deploying ProtectDrive Client-Side components on systems containing multiple hard disks, **disk0** must be the drive where ProtectDrive is installed. Furthermore, ProtectDrive requires that the partition on **disk0** where the Client-Side components will be installed is designated as drive letter **C:** within the operating system.

Preparing the SYSKEY.CID File

This file is required by the ProtectDrive Client-Side installer. It is created from the **SYSKEY.BIN** file located either on the Eracom provided **Registration Floppy** or the custom created floppy described in "Creating a Custom **SYSKEY.BIN**" earlier in this chapter.

Run the **CIDKEY.EXE** utility located in the **\DIAGS** directory on the ProtectDrive distribution CD (or ZIP file).

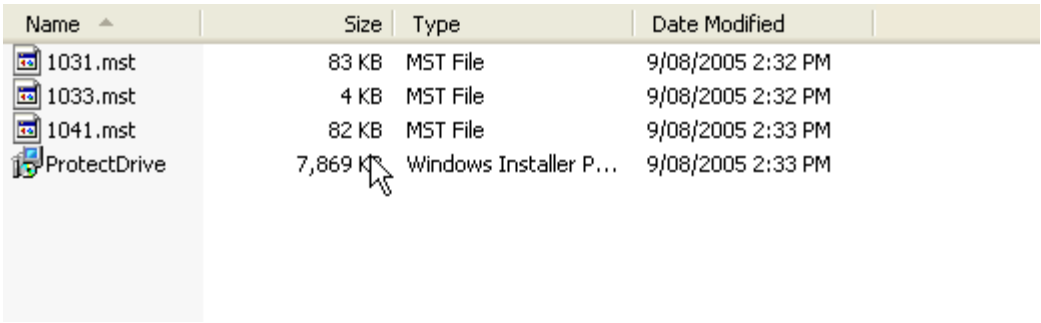
Usage: **CIDKEY.EXE –s SOURCE_DIR –t TARGET_DIR**

SOURCE_DIR	Directory containing the **SYSKEY.BIN** file. Typically this is the **A:**\ floppy drive directory.
TARGET_DIR	Location where the newly created **SYSKEY.CID** will reside.

Installing the ProtectDrive Client-Side Components

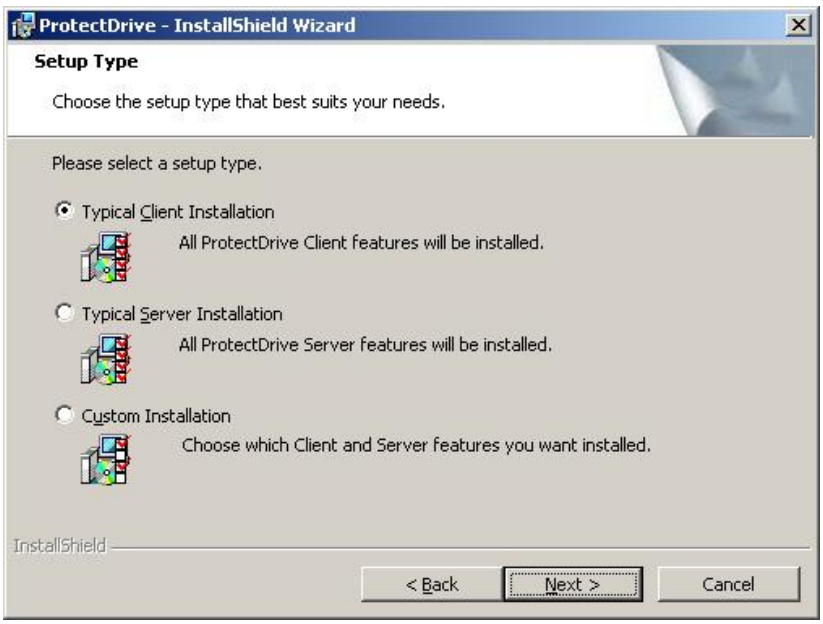
Launching **PROTECTDRIVE.MSI** will results in the ProtectDrive installation wizard. The wizard automatically installs all of the ProtectDrive Client-Side components with minimal user interaction as follows:

Please note that in addition to the installer files listed below Eracom may also place a custom graphics file (named **ACSGIF)** the (below) installer directory. This is a custom graphics file created by Eracom and includes the customer-specific artwork that will appear as part of the various ProtectDrive preboot authentication and/or system recovery display screens. If this file is there the ProtectDrive installer will automatically include this file as part of the Client-Side Component installation.

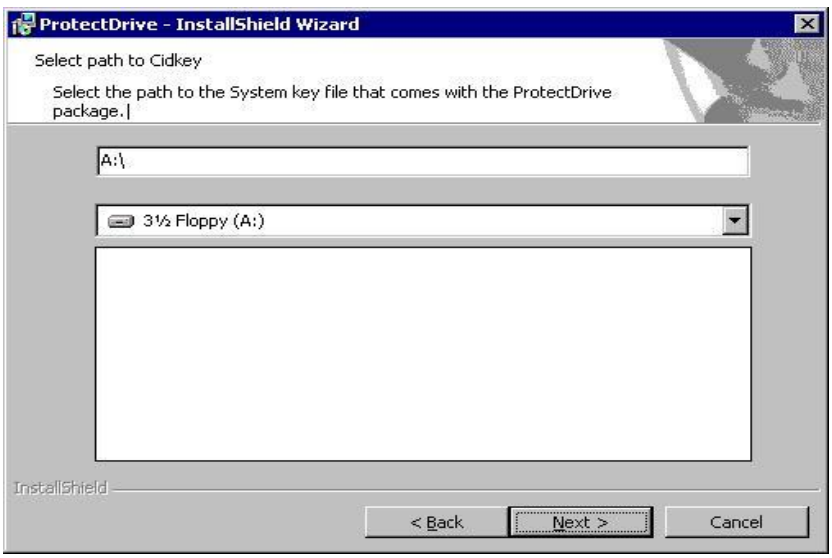


Launch the **`PROTECTDRIVE.MSI`**

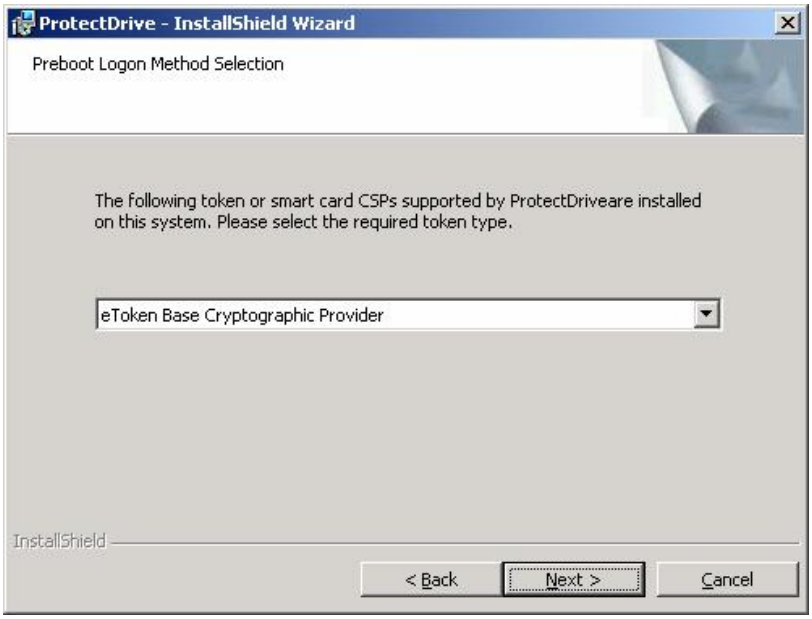
Select **Client** in the wizard and follow the prompts.



ProtectDrive will require a **`SYSKEY.CID`** file prepared prior to the install. Specify the location of this file for the installer.



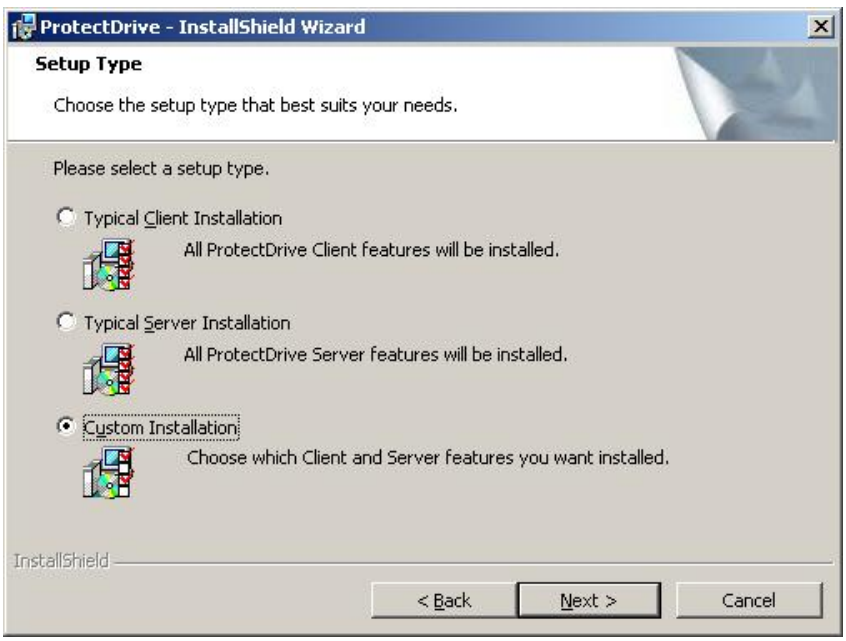
ProtectDrive will automatically detect all installed Token Runtime Environments and will prompt the installer to select the one that will be associated with ProtectDrive.



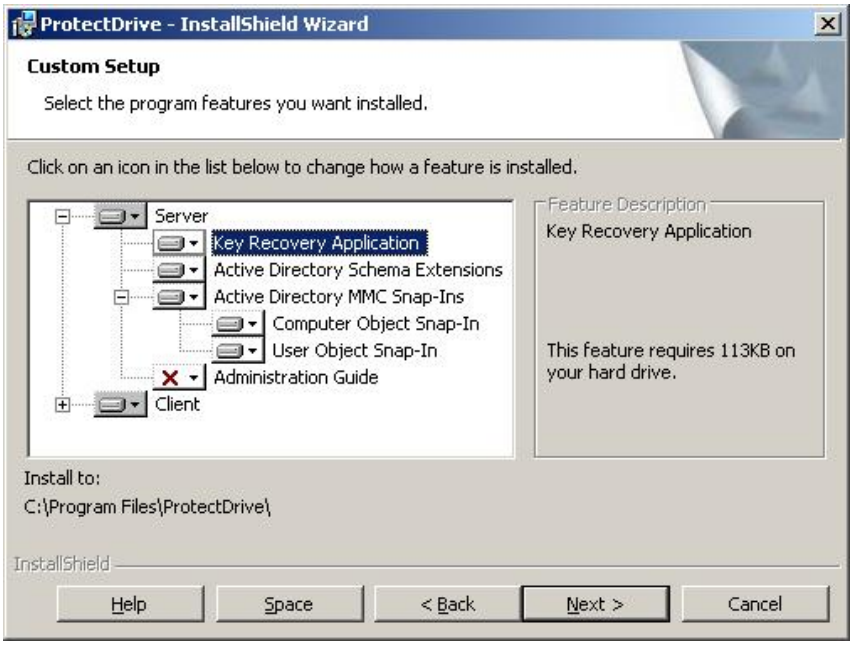
Custom Installation

In addition to the above mentioned Server and Client components install ProtectDrive provides the ability to custom select the install components.

Select **Custom Installation**



Select the **Server** and/or **Client** components that you wish to install.

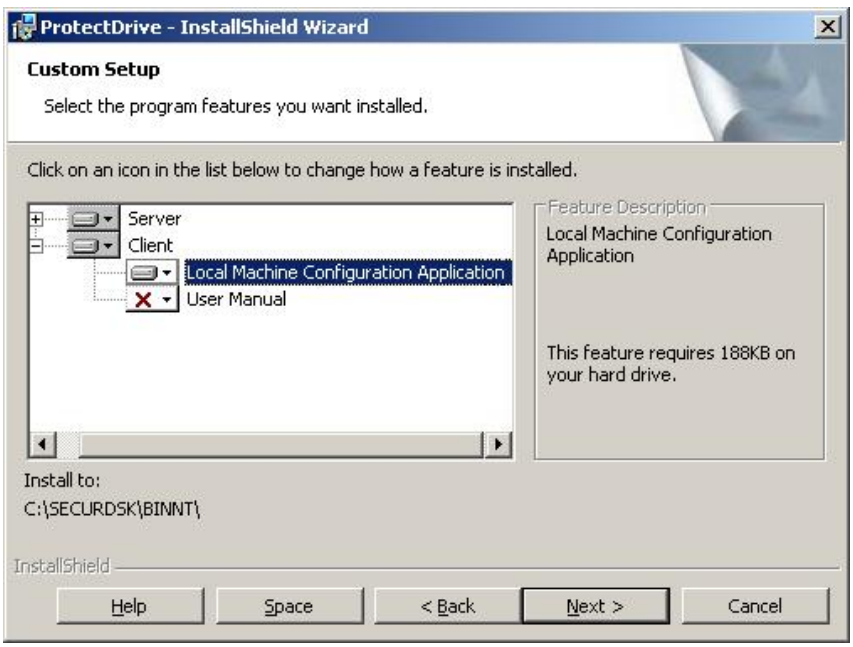


Key Recovery Application — this installs **`RPADMIN.EXE`.** See Chapter 9 - Extraordinary Authentication Scenarios for additional information.

Active Directory Schema Extensions — This applies the AD Schema Extensions.

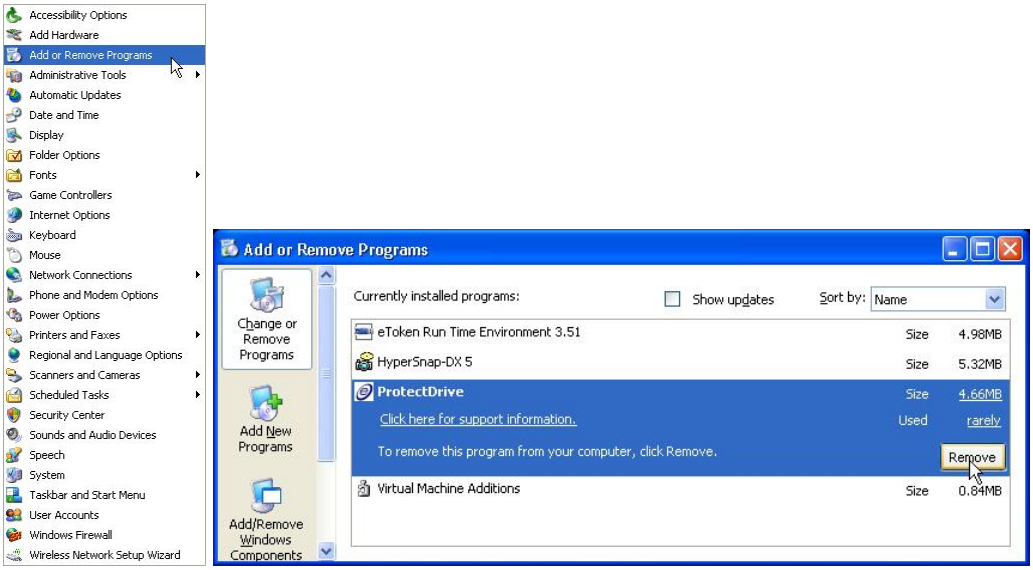
Active Directory MMC Snap-ins — This installs all the MMC snap-ins required to manage ProtectDrive System and User policy from the server.

Administration Guide — This installs this document.



Removing ProtectDrive

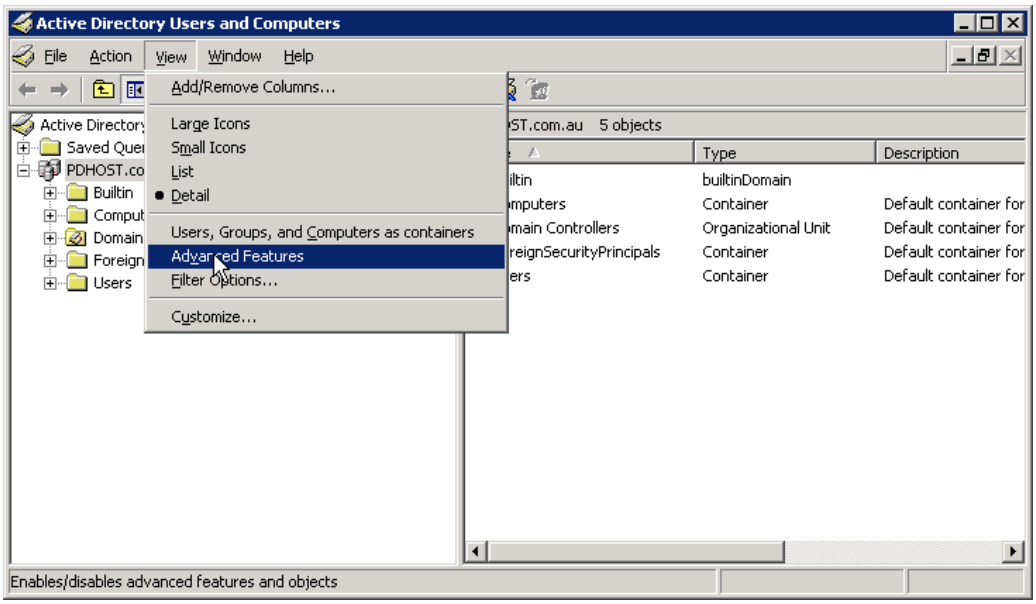
Make sure that all partitions are decrypted. Navigate to **Add or Remove Programs** in the Windows Control Panel. Select ProtectDrive and click **`Remove`**.



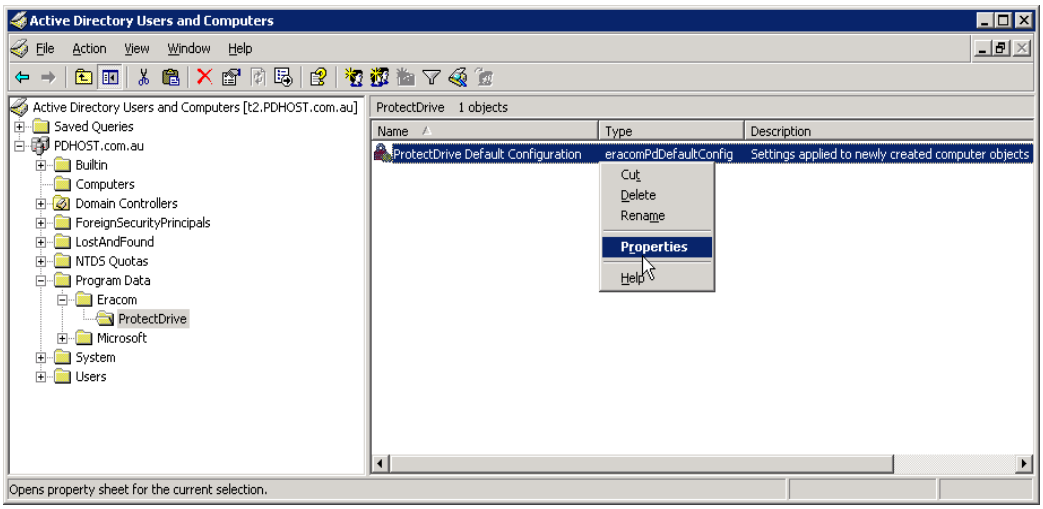
Chapter 6
Configuring Default System and User Policy

ProtectDrive will store an instance of a Default System and User Policy in the Active Directory. Every time a new computer account is created in the Windows Domain these stored default settings will automatically apply.

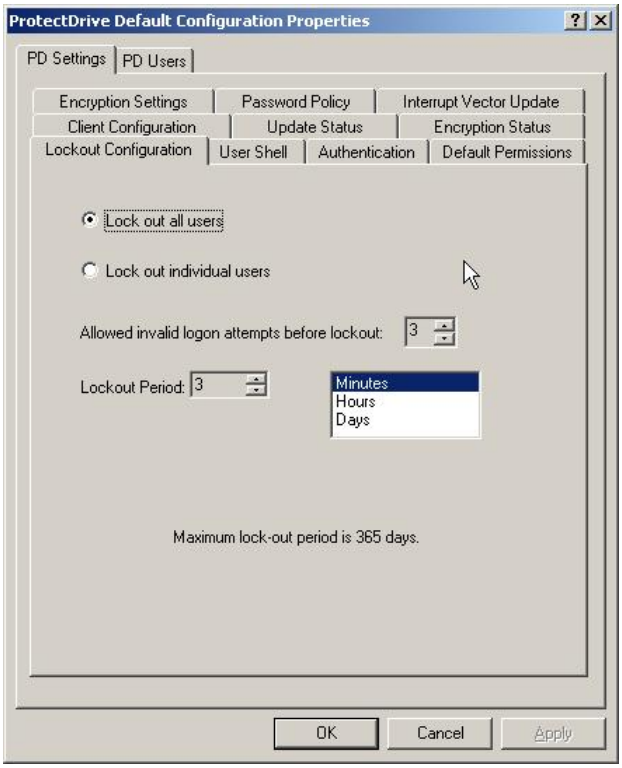
Display **Advanced Features** in the **MMC Active Directory Users and Computers Snap-in**.



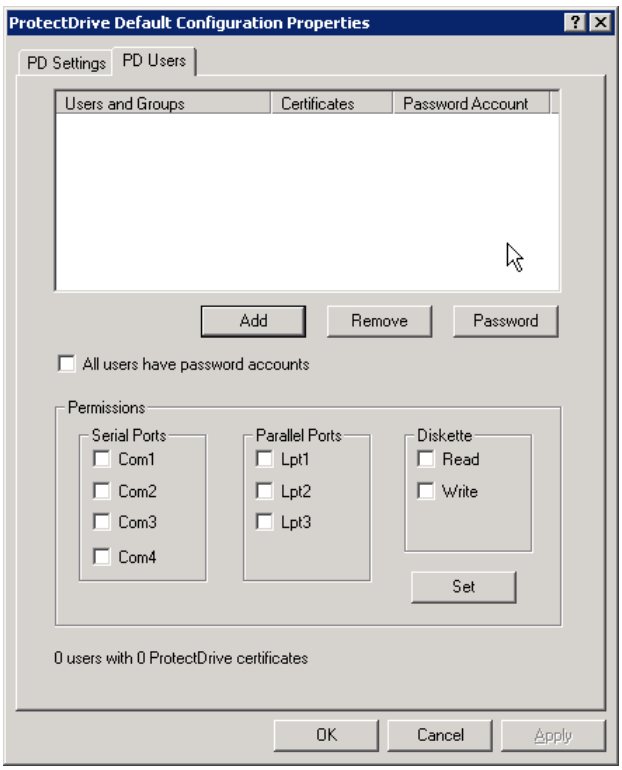
Navigate to **Program Data | Eracom | ProtectDrive | ProtectDrive Default Configuration** and select **Properties**.



Use the **PD Settings Tab** to configure Default System Policy.

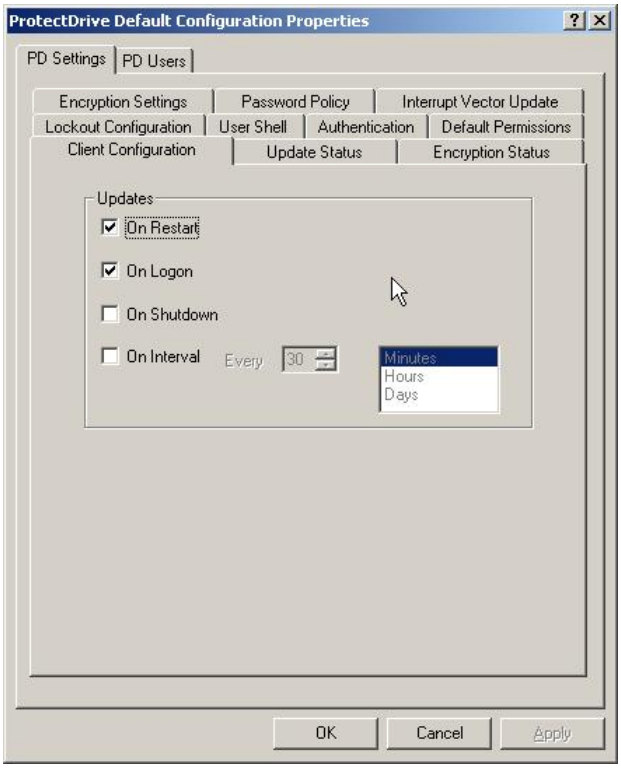


Use the **PD Users Tab** to assign users to the systems by default and also to configure these users' Device Access Permissions to COM/LPT ports and the FDD drive resources. Note following setting **Permissions** you need to press Set. Neither OK nor Apply will save the **Permissions** settings.



PD Settings Tab - Default System Policy

Client Configuration Policy Tab



This tab configures how the ProtectDrive client retrieves System and User Policy data from Active Directory. It also allows the client to be configured locally as well as store the local configuration changes in Active Directory

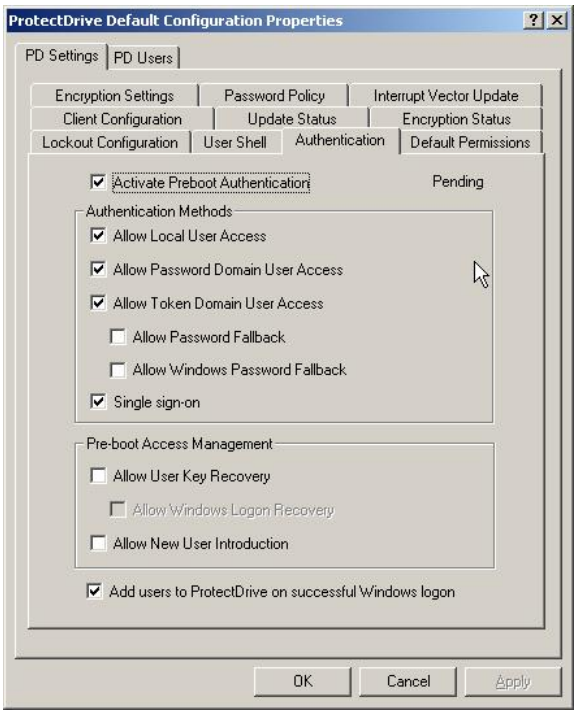
On Restart The ProtectDrive client pulls policy data from the Active Directory service on system boot.

On Logon The ProtectDrive client pulls policy data from the Active Directory service on user login.

On Shutdown The ProtectDrive client pulls policy data from the Active Directory service on system shutdown. Note, if using Windows Certificate Auto-Enrollment (Smartcard/Token users only) this option needs to be selected so a new entry in the ProtectDrive Preboot User dB can be created for the newly issued certificate.

On Interval The ProtectDrive client pulls policy data from the Active Directory service based on the specified period.

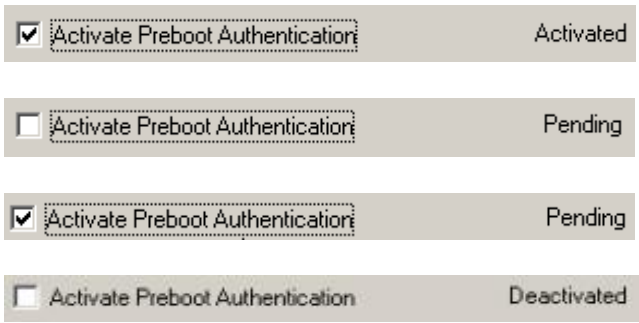
Authentication Policy Tab



Activate Preboot Authentication

This activates the Preboot Authentication. If disabled, all aspects of ProtectDrive including disk encryption will be disabled.

Activated/Pending/Deactivated Indicator



The **Activated/Pending/Deactivated Indicator** indicates whether the Preboot Authentication is currently Active (ON), Pending (the server is waiting for the client to update to the state currently set on the server), or Deactivated (OFF).

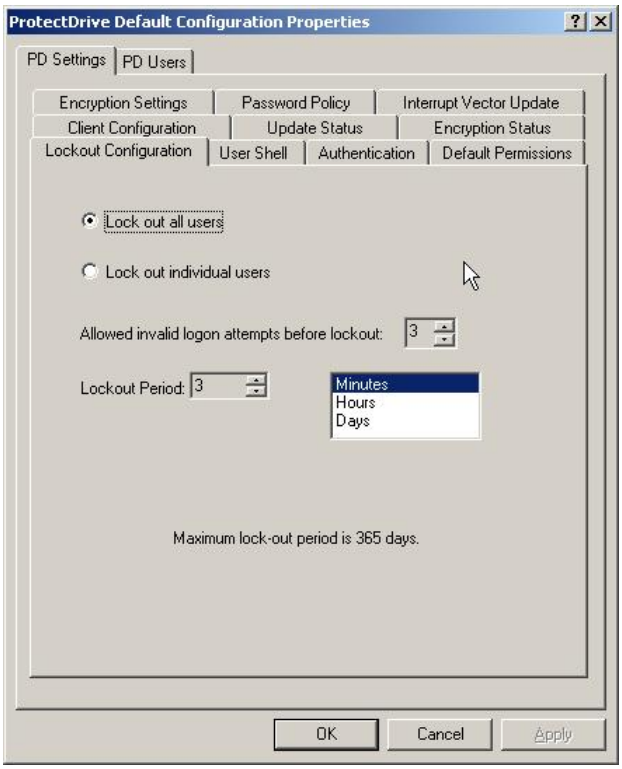
	Note that deactivating Preboot Authentication will remove **all** users from the client system's ProtectDrive Preboot User dB. The Windows Domain users will be re-added automatically when Preboot Authentication is reactivated. Local Windows users however will not be automatically re-added and will not be able to perform preboot authentication. Add Local Windows users manually once the Preboot Authentication is reactivated.
Allow Local User Access	Enabled by default this option allows the Local Windows users to authenticate into the system at preboot using their Local Windows Username, Password, and Local System Name. Local Windows users can only be added using **Local Machine Configuration Utility** or via a Windows Logon when **Add users to ProtectDrive on successful Windows Logon** is set in the **Authentication Tab**. Local Windows users can **not** be added to the client system's Preboot user dB from the server.
Allow Password Domain User Access	This option is permanently enabled. It allows the Windows Domain users to authenticate into the system at preboot using their Windows Domain Username, Password, and Domain Name.
Allow Token Domain Access	Enabled by default on Windows Domains systems with Token Runtime Environment(s), this option enables Windows Domain users to employ Smartcard/Token/PIN for preboot authentication.
Allow Password Fallback	This option is disabled by default. If enabled Smartcard/Token users who have misplaced their tokens or forgotten their PIN are permitted to invoke the Token User Preboot Password Fallback Procedure. This procedure allows for a one-time-only preboot access to the system using the user's Windows Domain Password.

Allow Windows Password Fallback	This feature is disabled by default. If enabled the user who has successfully exercised the Token User Preboot Password Fallback Procedure will be automatically authenticated into Windows. By necessity this will override all authentication restrictions imposed by the potentially disabled setting of the **Allow Local User Access** and/or the **Allow Password Domain Access options**. Please note that enabling this option will permanently force ProtectDrive into the Single Sign-On mode.
Single Sign-On	Enabled by default this option turns the Single Sign-On mode **ON**.
Allow User Key Recovery	This option is disabled by default. If enabled this option allows the user to invoke the User Preboot Password Recovery Procedure. It is used in cases where the user has forgotten their Windows (Domain) Password. It allows for one-time-only preboot access to the system.
Allow Windows Logon Recovery	This option is disabled by default. If enabled, this option allows the user to automatically authenticate postboot into Windows immediately following successful exercise of the User Preboot Password Recovery Procedure.
Allow New User Introduction	This option is disabled by default. This option is only used in conjunction with the ProtectDrive **Allow Local User Access** and/or the **Allow Password Domain User Access** authentication options. If enabled newly created Windows Domain or Local Windows users may invoke the New User Preboot Introduction Procedure. This allows for one-time-only preboot access to the system for all users who do not yet have a ProtectDrive Preboot user account.

Add users to ProtectDrive on successful Windows logon	This will create a new ProtectDrive pre-boot user account, if it does not exist for the user currently attempting to log onto Windows. This functionality is dependent on **Allow Local User Access** or **Allow Domain User Access** or **Allow Token User Access** settings. An entry will be created for the user in the ProtectDrive Preboot User dB only if setting that corresponds with the 'type' of Windows Logon being performed is set.

Note: Caution needs to be taken if **Allow Token Domain Access** is the only enabled authentication policy option. If the **Allow Local User Access, Allow Password Domain User Access, Allow Password Fallback,** and **Allow New User Introduction** are all disabled; then Smartcards/Tokens are the only means of authentication into the system at preboot. If any problems with the Smartcards/Tokens are encountered, the system may be rendered inaccessible. For this reason it may be a good idea to temporarily enable the **Allow Local User Access,** and/or the **Allow Password Fallback**, and/or the **Allow New User Introduction**. This will allow for at least one alternative method of preboot authentication until the Smartcards/Tokens proven to be reliable and properly setup for use with ProtectDrive.

Lockout Policy Tab



Lockout All Users / Individual Users

By default all users are locked out for the specified **Lockout Period** after the specified **Allowed Invalid Logon Attempts Before Lockout**

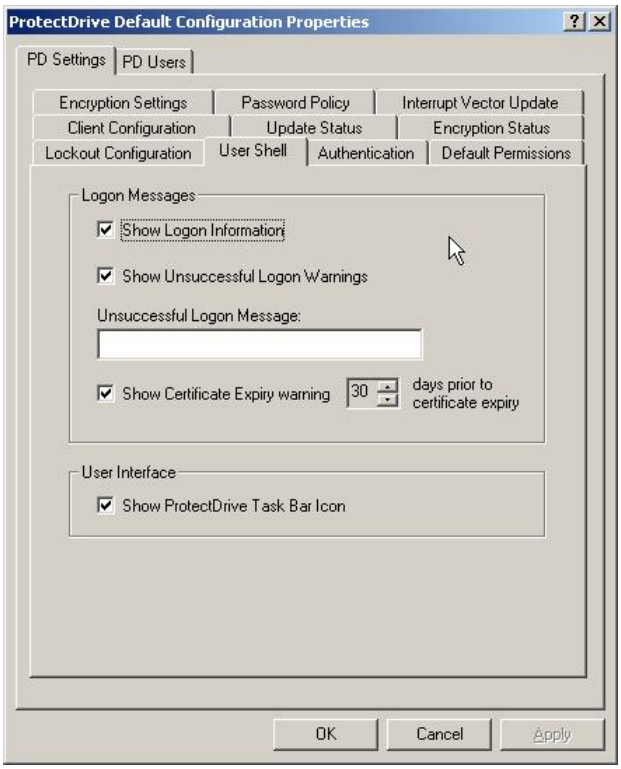
Allowed Invalid Logon Attempts Before Lockout

By default three (3) unsuccessful preboot authentication attempts lead to system lockout.

Lockout Period

By default the system is locked out for three (3) minutes. Please note that the maximum Lockout Period is 365 days.

User Shell Policy Tab



Show Logon Information

By default the ProtectDrive Authentication Information Dialog is displayed immediately preceding the loading of the Windows Explorer Shell.

Show Unsuccessful Logon Warnings

By default a warning message is displayed if previous unsuccessful preboot authentication attempts have occurred. This warning is displayed immediately preceding the loading of the Windows Explorer Shell.

Unsuccessful Logon message

An optional, custom unsuccessful preboot warning message can be specified for display purposes.

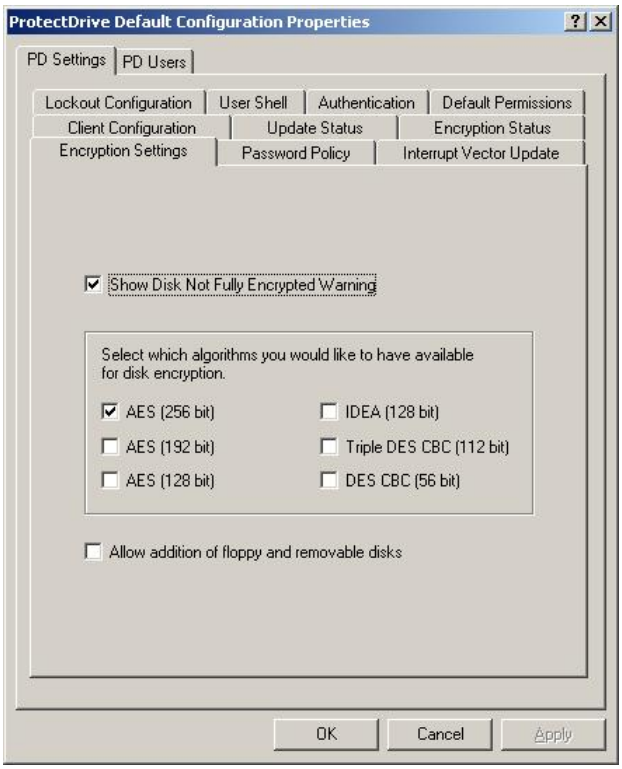
Show Certificate Expiry warning

Smartcard/Token users will see a warning the specified number of days before their certificate expires.

Show Task Bar Icon

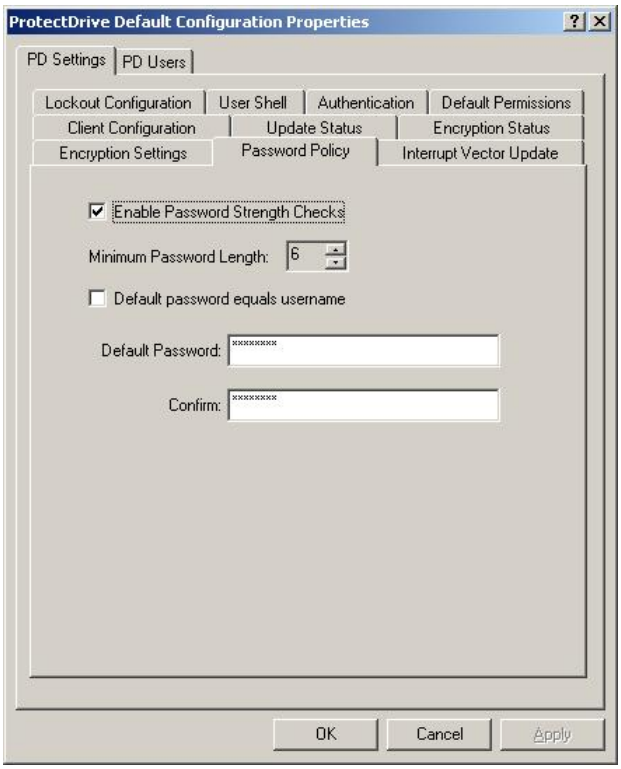
By default a small key icon () is placed in the task bar tray. The system can be locked by **DOUBLE-CLICKING** on this icon.

Encryption Settings Policy Tab



Show Disk Not Fully Encrypted Warning	Enabled by default this option displays a warning message to all users informing them of an incomplete disk encryption status. This ProtectDrive warning message is displayed immediately following the loading of the Windows Explorer Shell.
Selecting the Encryption Algorithm(s)	All encryption algorithms selected here will be made available to users during ProtectDrive encryption operation.
Allow Addition of floppy and removable disks	Only addition/removal of floppy disk drives is supported at this point. Changes to this setting will apply only **after** a reboot.

Password Policy Tab



Enable Password Strength Checks

If enabled, ProtectDrive will monitor the specified **Minimum Password Length** for all Windows (Domain) Passwords. ProtectDrive will also ensure that the password is not the same as the username, and that there is no more than two (2) consecutive repeating characters.

Minimum Password Length

ProtectDrive will impose this restriction to all Windows (Domain) Passwords. Windows Password Policy may impose more stringent limits which will override this setting.

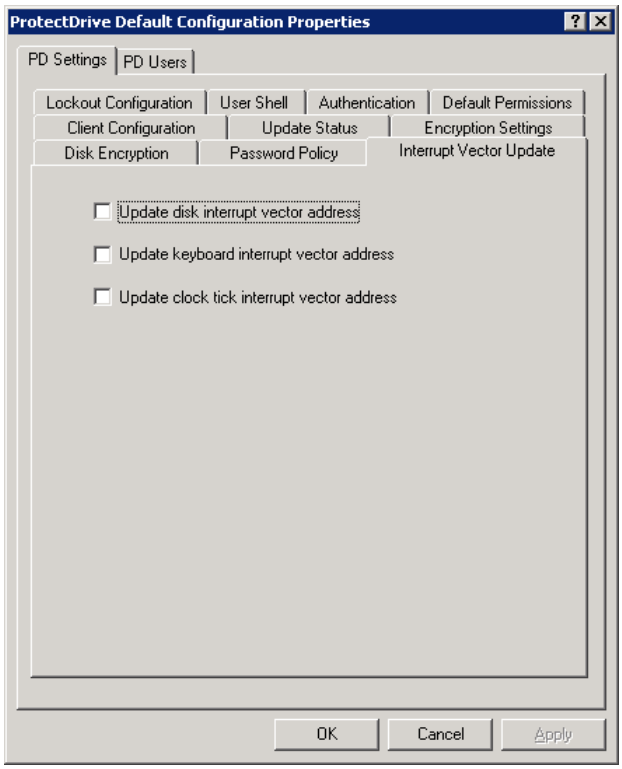
Default password equals username

This is an alternative to specifying the Default Password. Please note that in this case the users still need to type in their password (which is their Windows Username). Note that if **Enable Password Strength Checks** is set, users given a password of their user name will fail to be added to the ProtectDrive dB.

Default Password

Newly added Windows (Domain) users may be instructed to use this default password for their initial (first-time-ever) preboot authentication. Once the user authenticates into Windows using their *Actual Windows (Domain) Password*, the user's *Actual Windows (Domain) Password* replaces the Default Password in the ProtectDrive Preboot User dB. The default password is pre-set to "**password**" by ProtectDrive.

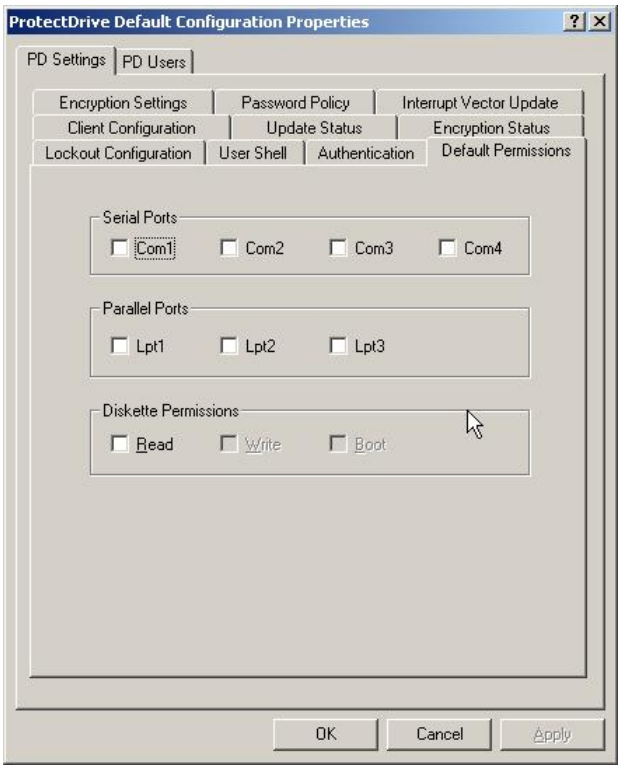
Interrupt Vector Address Update Policy Tab



ProtectDrive maintains a store of the BIOS interrupt vector addresses. This allows ProtectDrive to detect potential attacks mounted by the changing of the interrupt vector address. When ProtectDrive detects a difference between the BIOS interrupt vector address and the copy held by ProtectDrive an error message is displayed.

When interrupt vector addresses change (e.g. updating the BIOS) this error message is still displayed. The Interrupt Vector Address Update Policy Tab provides a mechanism to accept a legitimate change by updating ProtectDrive's copy of the disk, keyboard and clock tick interrupt vector address.

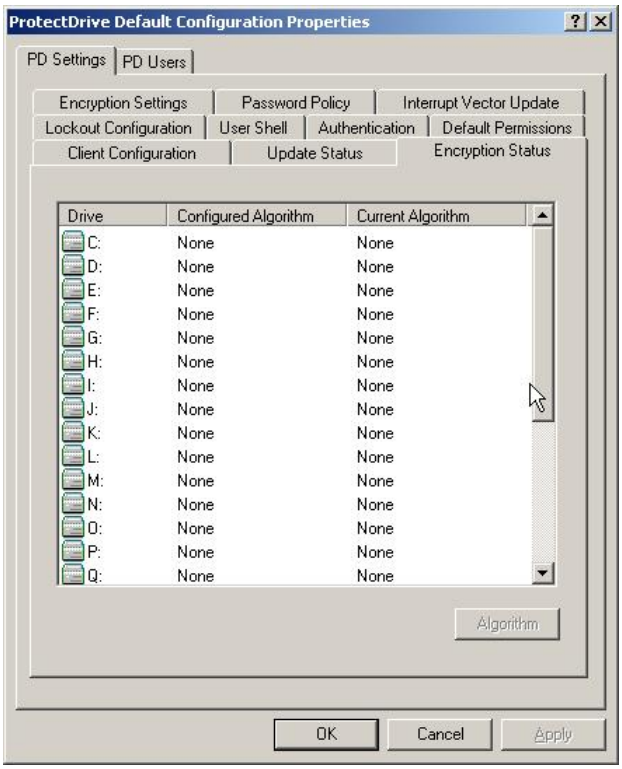
Default Devices Access Permissions Policy Tab



The Default Device Access Permissions only apply to users whose individual User Policy has not yet been defined explicitly (see **PD Users Tab**). In fact individual User Policy settings (once defined in the **PD Users Tab**) will override these defaults.

For example, a user may be added to the ProtectDrive preboot user dB following a successful Windows log-in (see "**Add users to ProtectDrive on successful Windows logon**" in **Authentication Policy Tab**. If this user was not explicitly added to the system using the PD Users Tab, then their device access permissions to the systems resources will be governed by the settings of the Default Device Access Permissions Policy Tab.

Encryption Status Policy Tab



This tab allows for default configuration and automatic execution of disk encryption on the remote client system. Any partitions configured for encryption here will be automatically encrypted by default on all newly added (to the Windows Domain) systems.

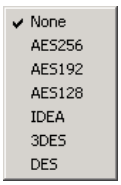
Drive

Lists all possible partitions for the client system. Note that this list does not accurately portray the partition allocation table on the client system. Since this information is not readily available in Active Directory, ProtectDrive lists all possible partitions between A and Z. The number of actual partitions allocated on the client may be lower. Configuring default encryption on a partition letter that does not actually exist on a particular client will result in **no** negative consequence.

Configured Algorithm

This column lists the algorithm selected for the encryption of the given partition. If **None** is shown; then the partition is either not configured for encryption or (if already encrypted see the **Current Algorithm** column) it is slotted for decryption.

Press 

and select 

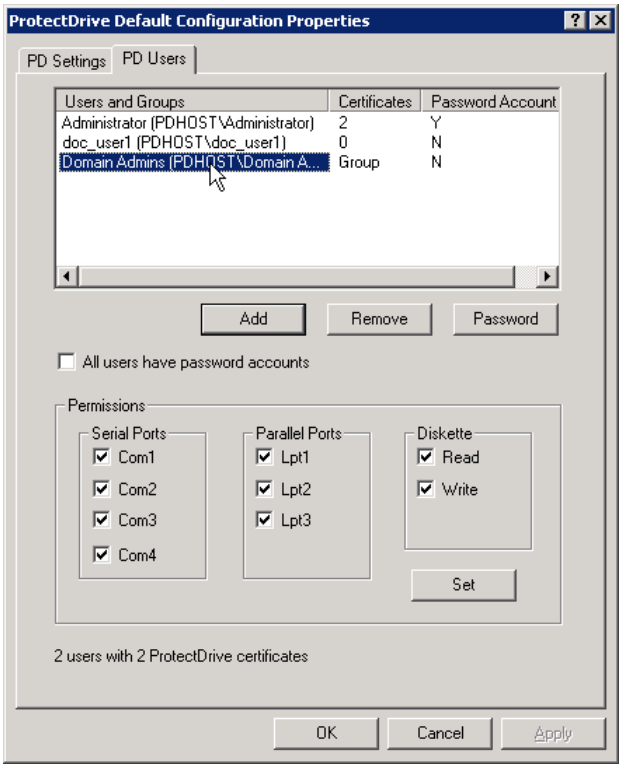
the desired algorithms for each partition that you wish to encrypt by default.

Current Algorithm

This has no effect on the default configuration. In general this column represents the encryption status of the partition. If **None** is shown then the partition is not currently encrypted.

PD Users Tab – Default User Policy

Using this tab certain Windows Domain users can be automatically assigned to newly created computer objects. These users' access permissions to the COM/LPT ports and the FDD drives can be configured here as well.



Users and Groups

Lists individual domain users and groups of users which will be automatically assigned to all newly created computer objects in the given domain. Press Add or Remove to populate this column from Active Directory.

Certificates

Lists the number of Smartcard/Token certificates each user possesses in the given domain. Users with certificates are able to log into ProtectDrive using their Smartcard/Token. Note that the total number of assigned certificates is also listed at the bottom of this tab. A ProtectDrive User account is created for each Smartcard/Token certificate. Including any accounts created for password users the total number of accounts on each client system can not exceed **200**..

Password Account

Indicates whether a user or group of users possess password accounts for login into ProtectDrive. Press Password to configure individual user (or group-wide) password accounts. The number of password users and Smartcard/Token certificate users should not exceed **200**.

All users have password accounts

Selecting this will create a password account for all users listed in this tab. The password will be set to the Default Password configured in the Password Policy Tab described earlier in this chapter. the number of password users and certificate users should not exceed **200**.

Permissions

Default Access Permissions to the client COM/LPT ports as well as the FDD are configured here for each user (or group) listed in this tab. Please note that you need to press Set in order for these settings to be saved in the Active Directory. Pressing Add or Remove will **not** save these settings in the Active Directory.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 7
System and User Management

ProtectDrive clients are managed centrally from the server with the System and User Policy data stored in and replicated from Active Directory. **MMC Active Directory Users and Computers Snap-in** is amended with the **PD Settings** and **PD Users Tabs.**

Alternatively, **Local Machine Configuration Utility** may be used to manage clients locally. Local configuration may be saved in the Active Directory. Finally, each client reports policy data update status back to the server.

Note: In the current release of ProtectDrive the **Local Machine Configuration Utility** is **read-only**. Configuration data may be viewed but not changed.

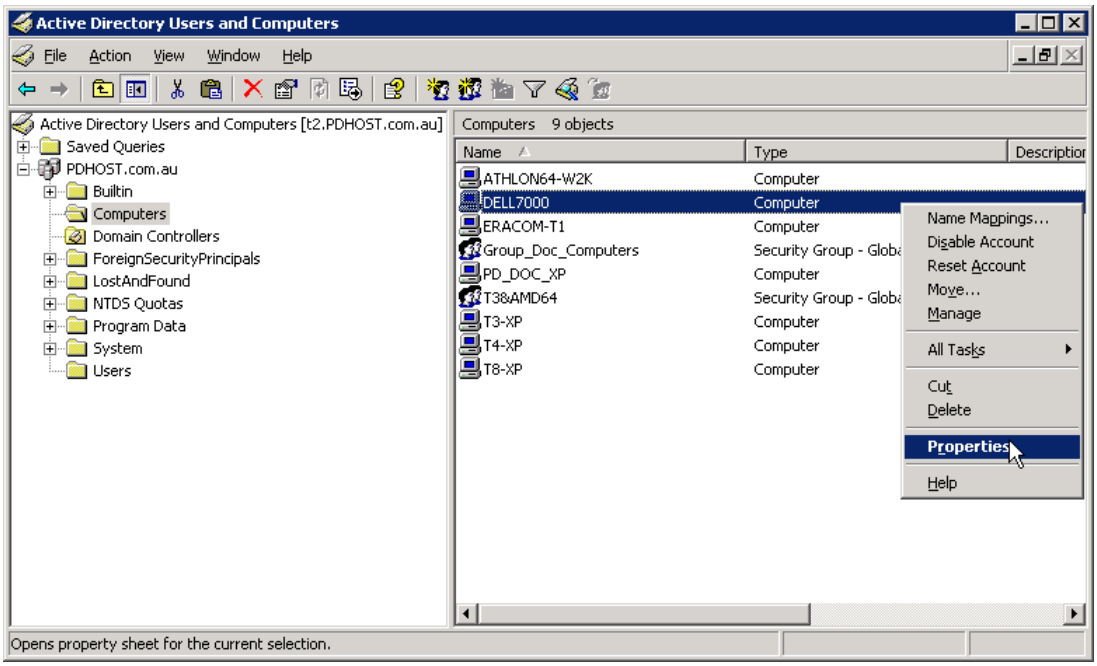
Before You Begin

Enabling Clients to Store ProtectDrive Policy Data in the Active Directory

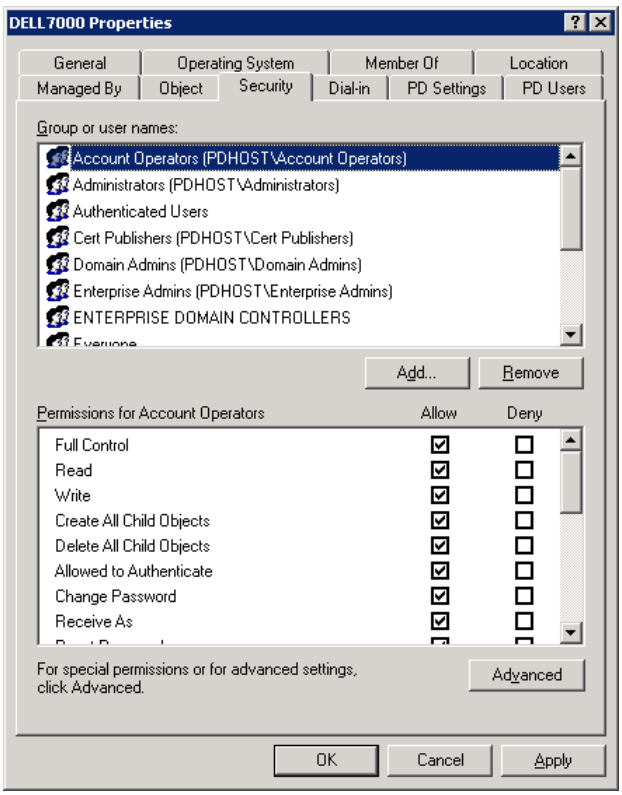
In order to enable client systems to save data in Active Directory and to report policy data update status back to the server it is important to configure each client computer object security configuration to allow writing ProtectDrive policy data to Active Directory.

To do this for a system called DELL7000 for example:

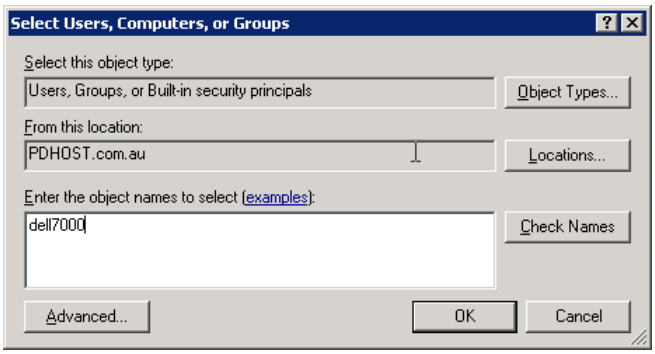
Select **Properties** for the DELL7000 system



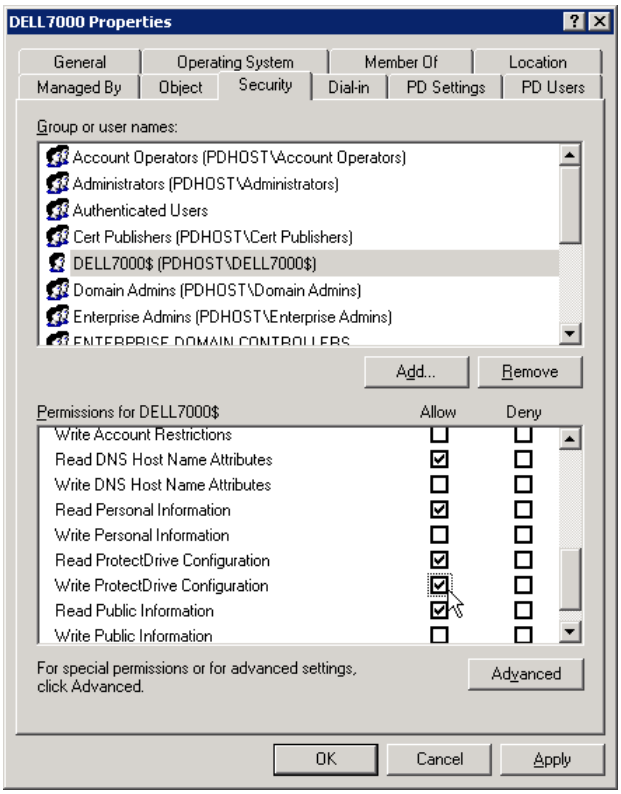
Click **Security Tab**



Click Add and add the DELL7000 computer object, press OK



Click on DELL7000$ and select **Write ProtectDrive Configuration** under the **Allow** column. Press OK

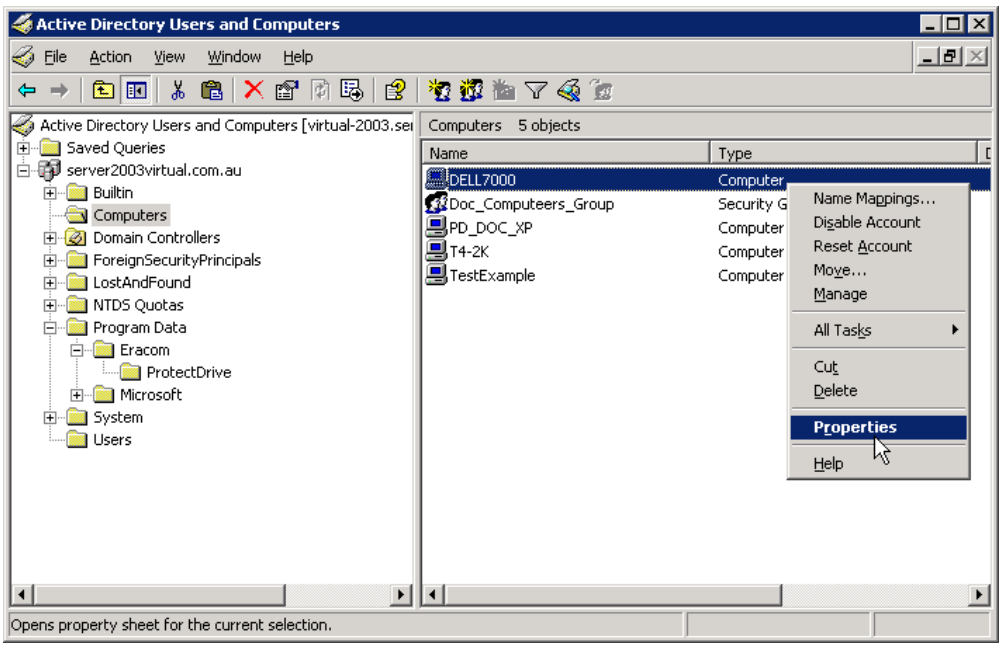


Managing System Policy from the Server

Before configuring System and User Policy review the contents of Chapter 6 Configuring Default System and User Policy. This will familiarize you with the fields contained in the **PD Settings Tab**. This tab is used to configure ProtectDrive System Policy.

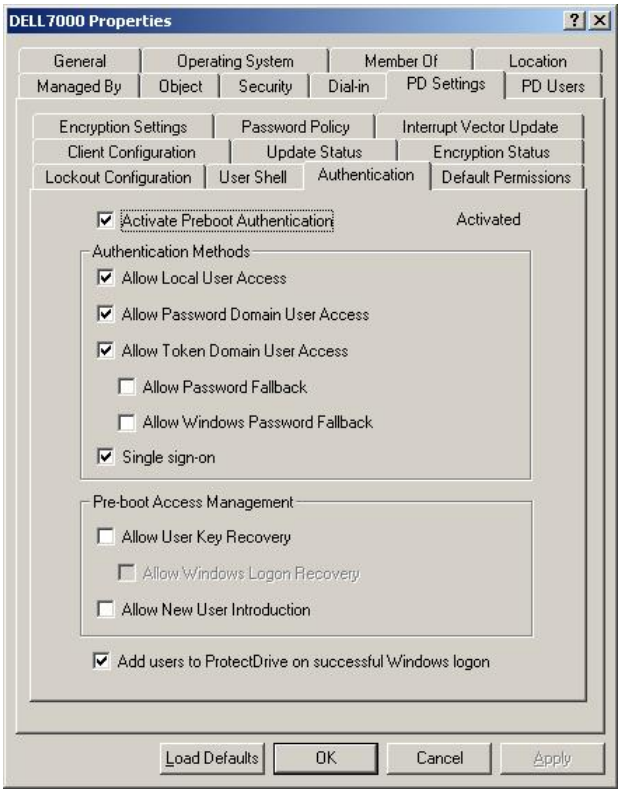
All systems in a Windows Domain can be managed remotely with the use of the **PD Settings** and **PD Users** tabs in the **MMC Active Directory Users and Computers Snap-in**. All the configuration settings in these tabs are stored in Active Directory and are replicated (this is configurable) to the client systems. System Policy settings applied on the server can also be viewed and modified locally on the client systems with the use of the **ProtectDrive Local Machine Configuration** utility. System Policy can be configured to allow local system management with the use of this utility. Any local System Policy changes made inside the **Local Machine Configuration** utility can be (this is also configurable) stored in the Active Directory and made available for view and/or change on the server.

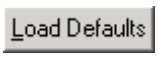
Let's for example take a client system named DELL7000. In the **MMC Active Directory Users and Computers Snap-in** select **Properties** for the DELL7000.



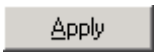
Select **PD Settings Tab** and use all the displayed tabs to set the desired ProtectDrive System Policy.

Go through all the ProtectDrive tabs and set DELL7000 System Policy accordingly. Pay particular attention to the settings outlined below.





If ProtectDrive System and User Policy Defaults have been previously defined for this particular Windows Domain as outlined in Chapter 6; then pressing this button will apply these defaults to all the members of this computer group.

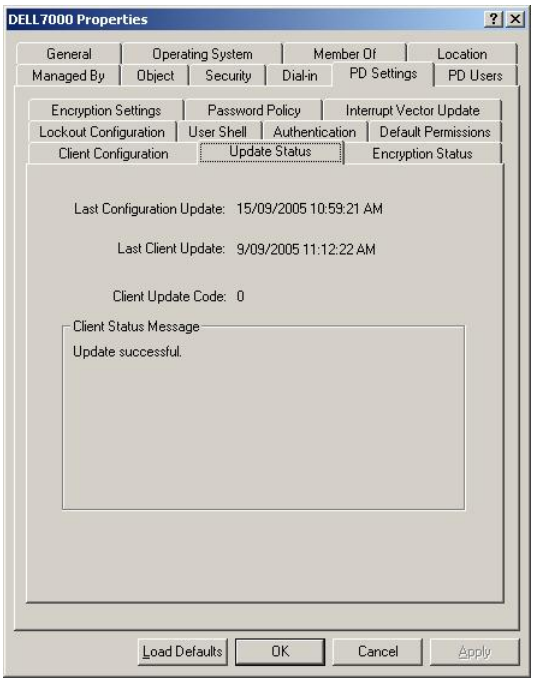


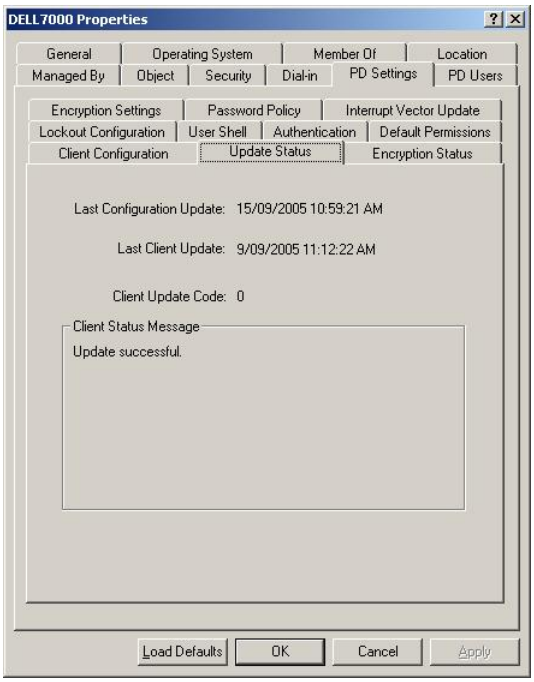
Pressing these buttons will store the System and User Policy data in Active Directory and time stamp it in preparation for eventual replication to the client system(s). Replication of the configuration changes to the client(s) will take place in accordance with the **Updates** settings located on the **Client Configuration Tab**.

In the **Authentication Tab** pay attention to the **Activated/Pending/Deactivated Indicator**. Note that this indicates the current status of the client's ProtectDrive Preboot Authentication. ProtectDrive client **Activated/Deactivated** state gets updated in accordance with the settings of the **Update Interval Tab**. When setting of the **Activate Preboot Authentication** checkbox changes the ProtectDrive client goes through a delayed transitionary period (indicated by **Pending**) before the actual **Activated (or Deactivated)** state takes effect.

In the above example the indicator tells us that although the preboot authentication is activated (check box is checked) no preboot users have replicated to the client **yet**. Therefore, for the time being all ProtectDrive features are disabled on DELL7000. This may be the case when ProtectDrive is first installed on DELL7000, and the System Policy has not yet propagated to it from Active Directory. Alternatively, the same effect will be achieved if no users have been assigned to DELL7000. In short, the **Pending** status will prevail until DELL7000 is properly configured and the policy data successfully replicates from the server.

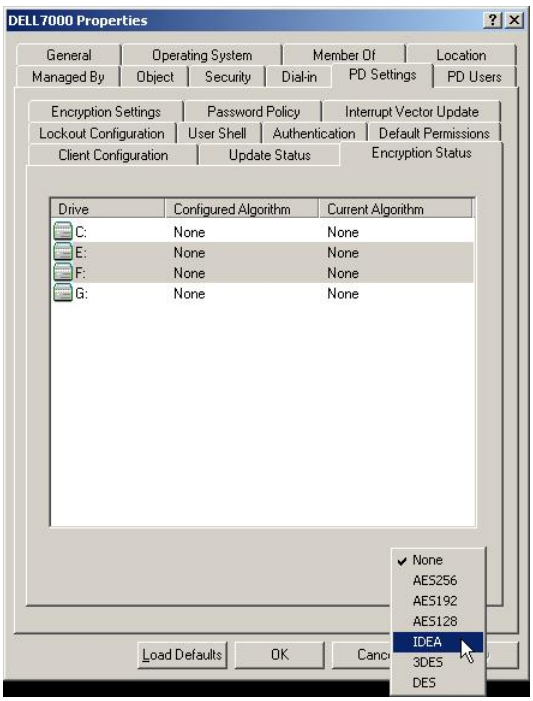
Monitor the **Update Status Tab** for indication of the time of the most recent policy data change and client update. If the **Last Client Update** is chronologically later than the **Last Configuration Update**, then the policy data has successfully replicated to the client. In the following example DELL7000 has successfully updated policy data from the server (snapshot on the left). In the snapshot on the right the client is still awaiting the next update.

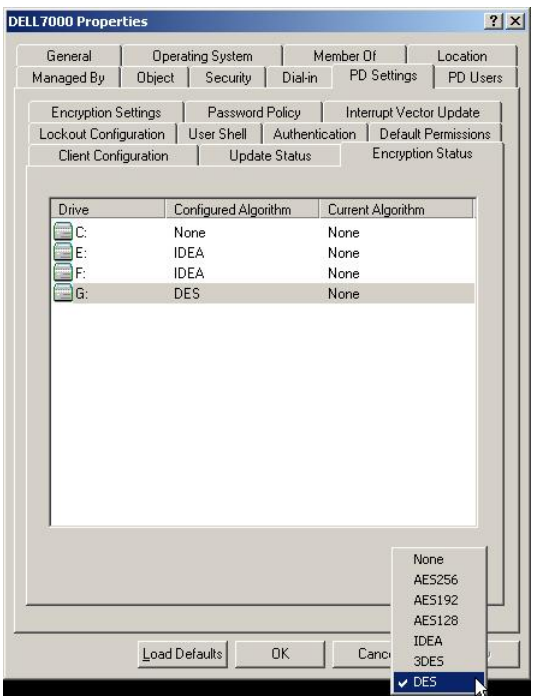




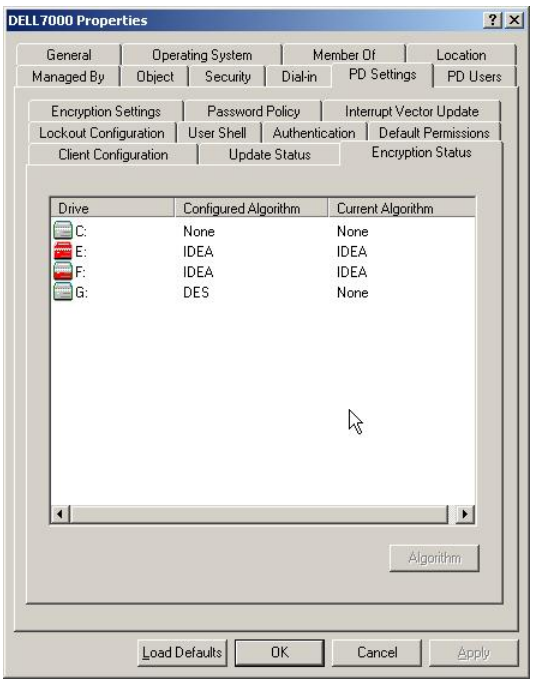
Use the 

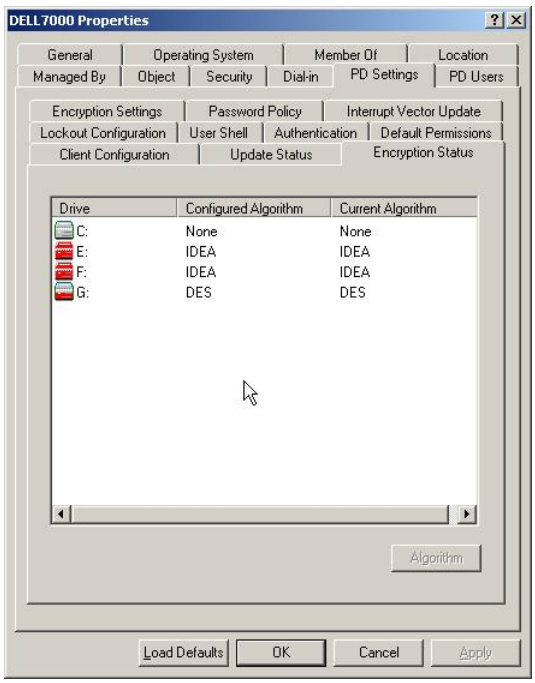
button on the **Encryption Status Tab** to specify which partitions on the client will be encrypted.



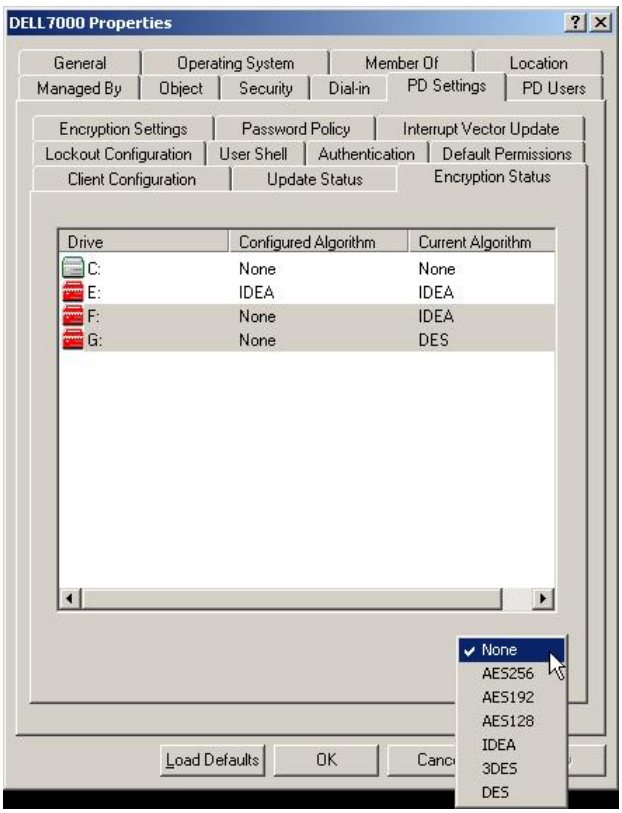


Ongoing encryption progress will be indicated in half-shaded disk drive icons as follows (drive F on the left and drive G on the right).





If you wish to decrypt any of the encrypted partitions set the **Configured Algorithm** to **None**. In the following example drives E and F are configured for decryption, which will take place as soon as the policy data replicates to the client in accordance with the **Updates** settings in the **Client Configuration Tab.**

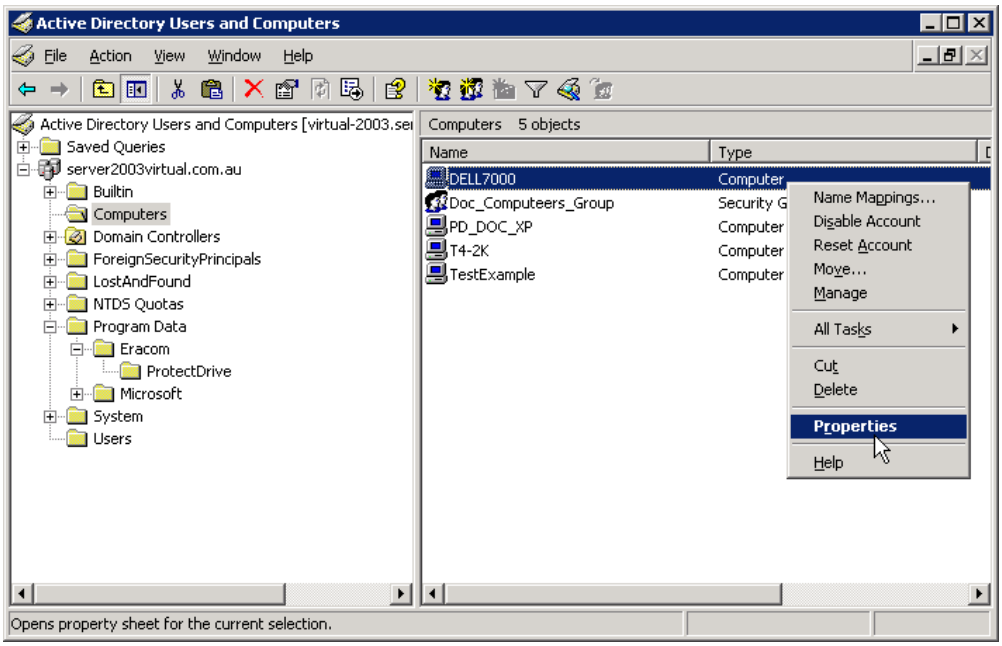


Managing User Policy from the Server

Assigning Users to Clients and Managing User Policy via the Computer Object

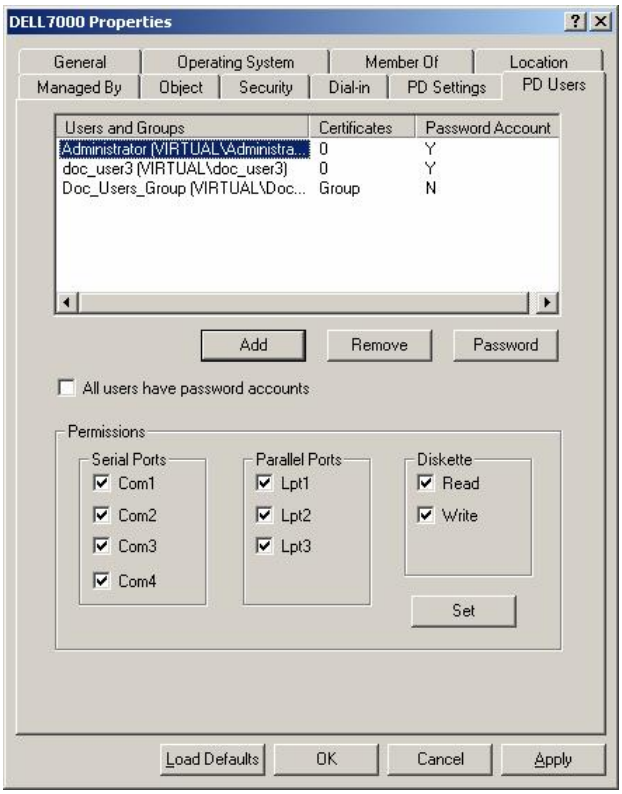
Before configuring User Policy review the contents of Chapter 6 Configuring Default System and User Policy. This will familiarize you with the fields contained in the **PD Users Tab**. This tab is used to configure ProtectDrive User Policy.

Let's for example take a client system named DELL7000. In the **MMC Active Directory Users and Computers Snap-in** select **Properties** for the DELL7000.



Select **PD Users Tab**. Add all Windows Domain users and groups you would like to give preboot access to this on client system. For each user or group use Set to set their device access permissions. Note that changes to device access permissions for any user or group apply across the entire Windows Domain. Changing permissions here will make the change for all client systems where this user or group is listed.

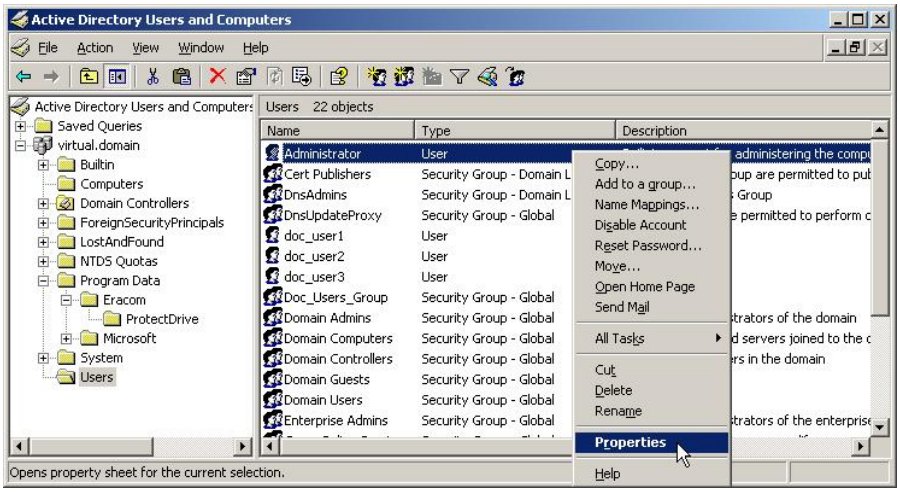
Enabling **All users have password accounts** will allow all users listed here preboot access with the use of the password defined in the **Default Password (System Policy) Tab**.



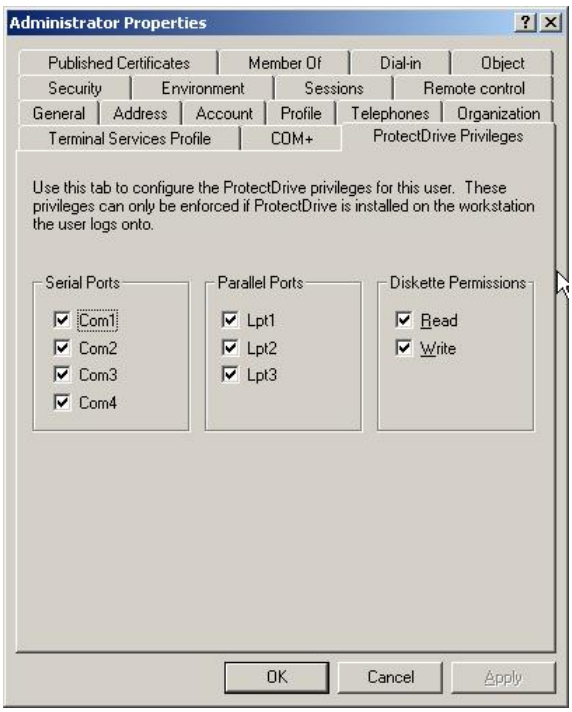
Managing User Policy via the User Object

ProtectDrive device access permissions for individual Windows Domain users can be set using the **ProtectDrive Privileges Tab** in the **MMC Active Directory Users and Computers Snap-in**.

Select **Properties** for a Windows Domain user.



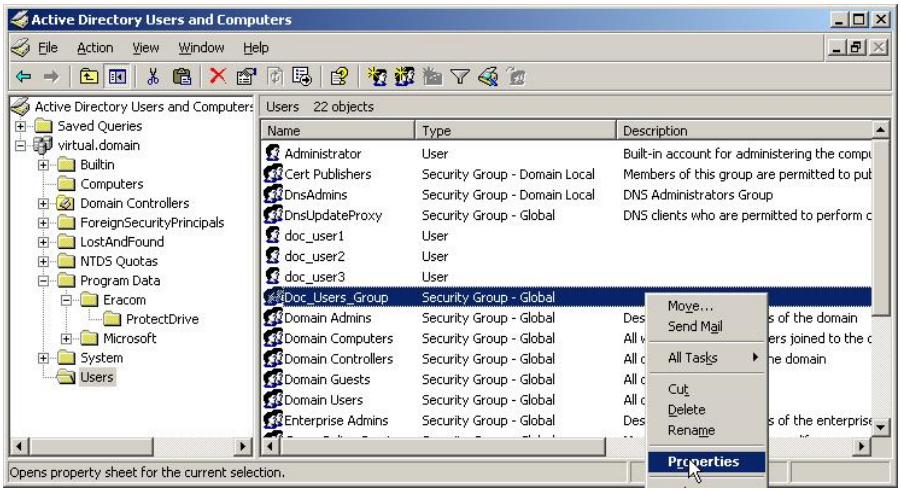
Click the **ProtectDrive Privileges Tab** and set the device access permissions as appropriate. Note that these settings will apply across the entire Windows Domain and will be picked up by all clients where this Windows Domain User is listed.



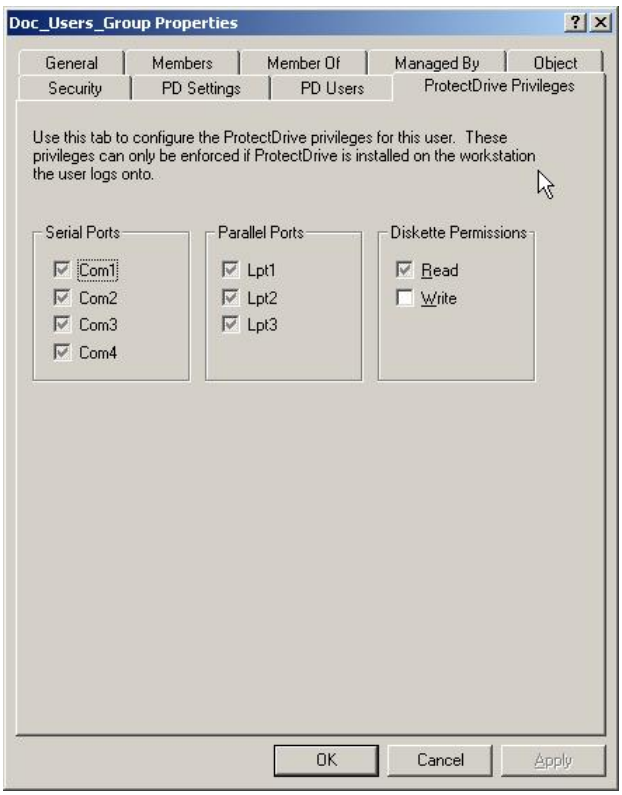
Managing User Policy via the Group Object

ProtectDrive device access permissions for groups of Windows Domain users can be set using the **ProtectDrive Privileges Tab** in the **MMC Active Directory Users and Computers Snap-in**.

Select **Properties** for a Windows Domain Group.



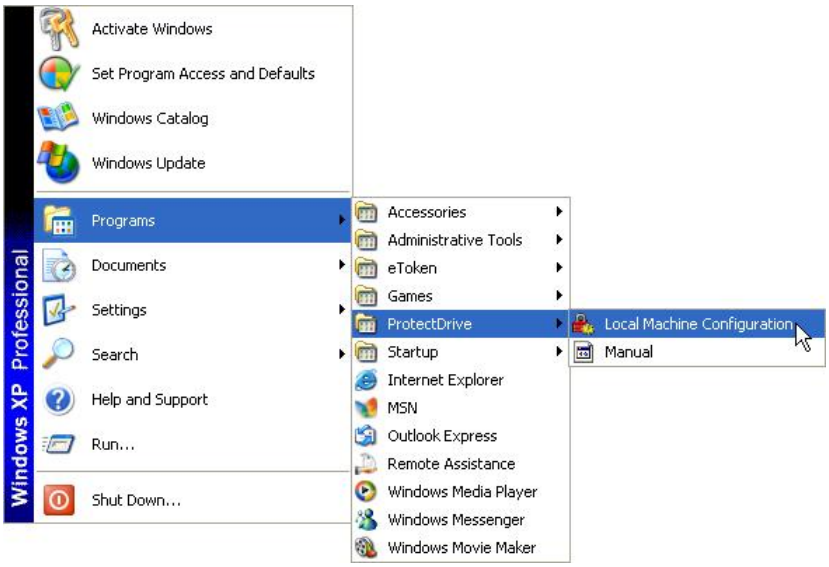
Click the **ProtectDrive Privileges Tab** and set the device access permissions as appropriate. Note that these settings will apply across the entire Windows Domain and will be picked up by all clients where this Windows Domain User Group is listed. Also note that settings that differ for various members of the group will be grayed out indicating conflicting data. Check these settings and set as appropriate.



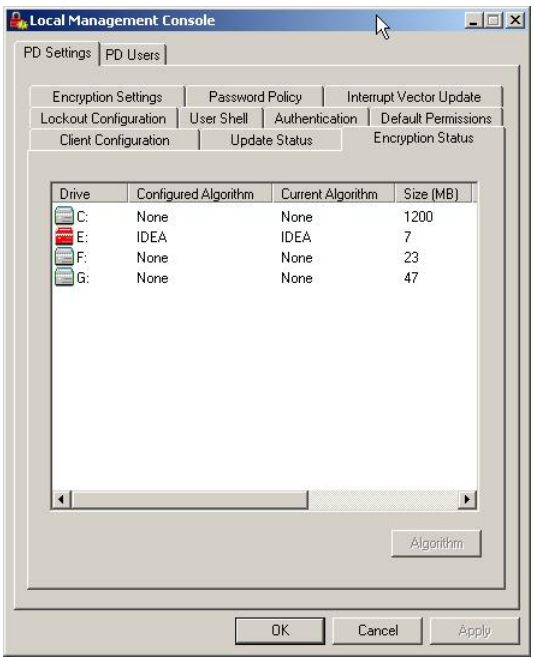
Managing System and User Policy Locally

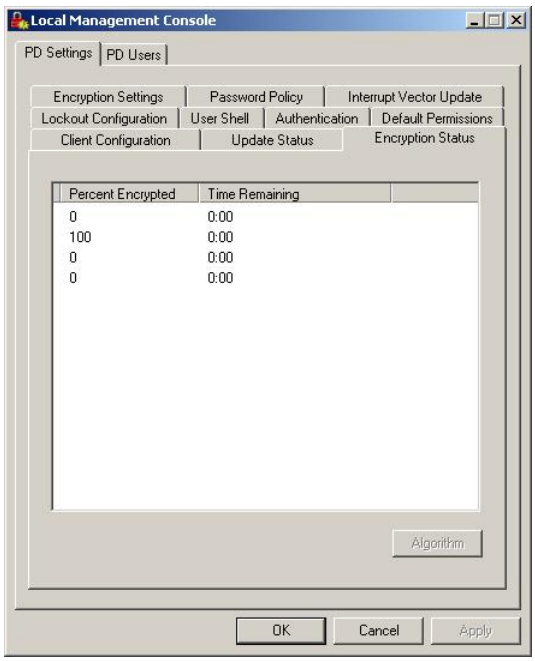
Please note that in the current release of ProtectDrive the Local Machine Configuration Utility operates in read-only mode. All System and User policy changes need to be made on the server. The Local Machine Configuration Utility is used for display-only of the configured System and User policy.

Run the **Local Machine Configuration Utility**.



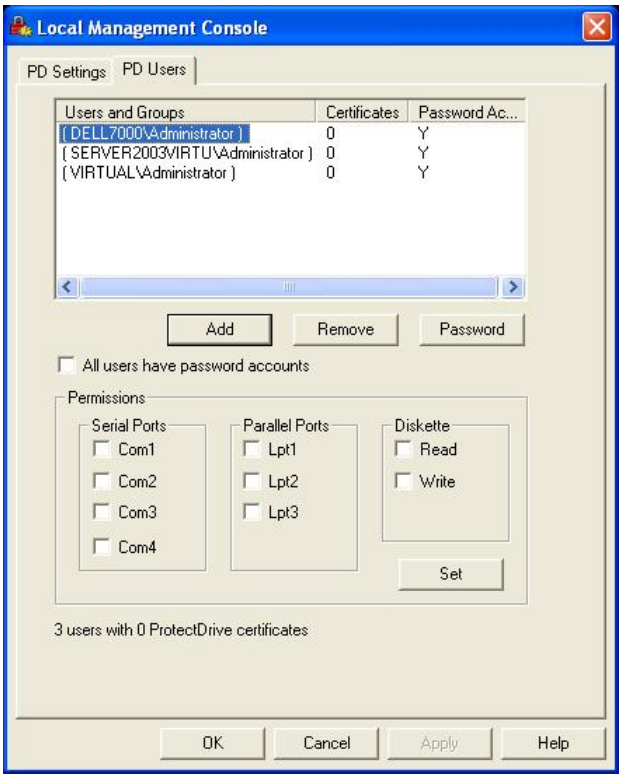
The **PD Settings Tab** is identical to the one used on the server with minor modifications as follows. The **Encryption Status Tab** lists three (3) additional columns





Size (MB)	Indicates the size of the hard drive partition.
Percent Encrypted	Indicates the encryption status of the hard drive partition.
Tine Remaining	Indicates the time remaining to completion while encryption is in progress.

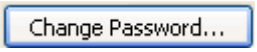
Use the **PD Users Tab** to add Windows Domain users and groups to the client. Note that all existing preboot user accounts are listed here. To add Windows Domain users press Add.



Adding Local Windows Users to the ProtectDrive Preboot User dB

To add local Windows users to the ProtectDrive Preboot User dB log out of your Windows Administrator session on the client PC and have each user log into the local Windows. Once they successfully log in, their preboot user accounts will be automatically created (assuming **Add users to ProtectDrive on successful Windows logon** in the **Authentication Policy Tab** is enabled).

Changing Preboot Passwords

Press **CTRL-ALT-DEL** and select 

Select the appropriate domain in the **Log on to** filed and specify the new password.

For local Windows (see **"this computer"** above) the new password change immediately propagates to the Preboot User dB.

For Windows Domain (below) the user will need to log out of Windows and log back in. This will propagate the new password to the ProtectDrive Preboot User dB. If the user does not follow this procedure, they would have to use their old password at preboot. Once they log into Windows Domain with their new password, this new password is immediately available for use during preboot authentication.

Chapter 8
User Authentication

Note: If System Policy has been configured to disable preboot authentication (see **Activate Preboot Authentication** in the **Authentication Tab**); then none of the material in this chapter applies. In this case the user will be presented with a standard Windows Domain authentication dialog, and normal Windows logon applies.

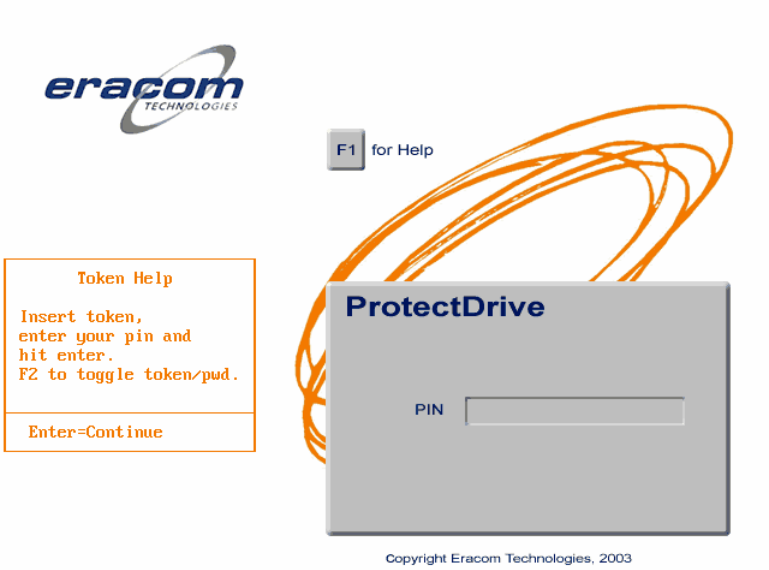
Authenticating with Smartcard/Token and PIN

Preboot Authentication

Please refer to Appendix A for a detailed diagram of the Smartcard/Token/PIN Preboot Authentication logic flow.

If the ProtectDrive **Allow Token Domain User Access** Authentication Policy option is set; then the preboot authentication screen will be as shown below. Furthermore, if either (or both) of the **Allow Local User Access** or the **Allow Password Domain User Access** Authentication Policy option is set, then pressing **[F2]** in the below screen will cause it to toggle with the Domain Password Preboot Authentication Screen.

At this point the user can authenticate into the system by using either their Smartcard/Token/PIN or their Windows Username/Password/Domain Name. Please note that in the case of consecutive failed preboot authentication attempts the Lockout Policy will be enforced to prevent PIN guessing.



Authentication into Windows

Note: Every time a user successfully logs into Windows their most current Windows Password propagates to the ProtectDrive preboot user dB.

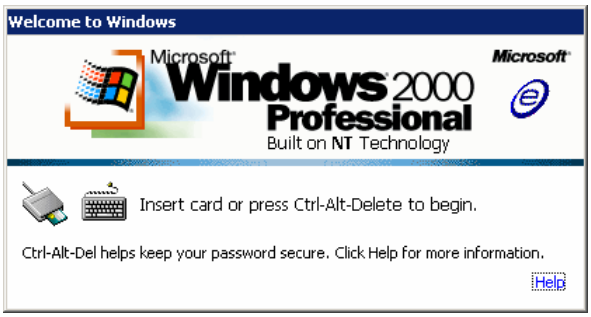
Please refer to Appendix C for a detailed diagram of the Windows (Domain) authentication logic flow.

Automatic - Single Sign-On Mode is ON

Assuming the ProtectDrive Single Sign-On mode is ON; the user is then automatically authenticated into their relevant Windows Domain.

Manual - Single Sign-On Mode is OFF

In the case of no Single Sign-On the following standard Windows Domain authentication screen will display.



Inserting the Smartcard/Token into the reader will result in the following standard Windows Domain PIN authentication screen. At this point the user enters their PIN.

Alternatively, assuming that either the **Allow Local User Access** or the **Allow Password Domain User Access** Authentication Policy option is set; then the user may press **`CTRL-ALT-DEL`** to invoke the standard Windows Domain Log On Screen.

Token Removal Policy

Computers using Smartcards/Tokens for Windows Domain authentication can be configured to automatically lock the system when the token is removed.

This behavior is controlled by the "Smart card removal behavior" policy in the MMC Local Security Settings Snap-in. By default this policy is set to "No action" or "Not defined".

Eracom recommends setting this policy to "Lock Workstation". This setting will require the user to re-insert their token and enter their PIN upon returning to the workstation

Authenticating with Username, Password, and Domain Name

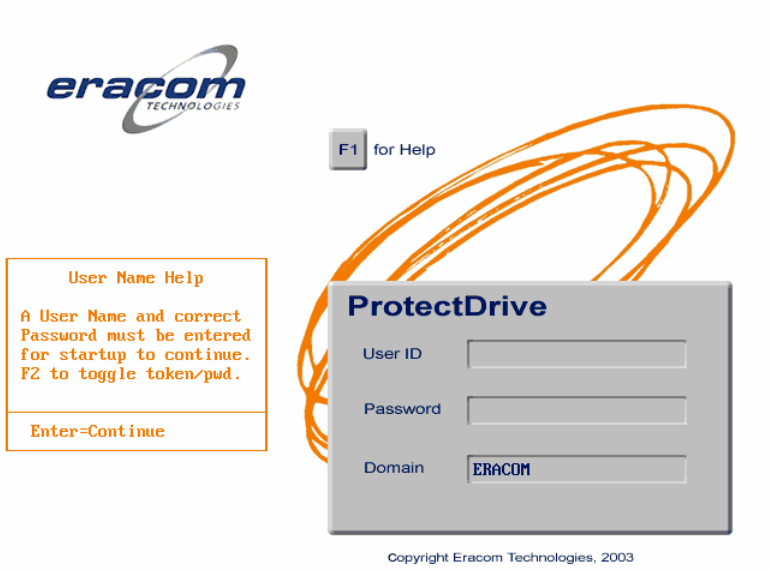
Preboot Authentication

Please refer to Appendix B for a detailed diagram of the Username/Password/Domain Name preboot authentication logic flow.

If either the **Allow Local User Access** or the **Allow Password Domain User Access** Authentication Policy option is set, the ProtectDrive preboot authentication screen will be as shown below.

The **"Domain"** field lists all the relevant Windows Domains available on the system. Assuming the **Allow Local User Access** Authentication Policy option is enabled; then the *Local System Name* will also be listed in the **"Domain"** field of the following Protect Dive preboot authentication screen.

[UP-ARROW] and **[DOWN-ARROW]** are used to navigate the list of available domain names.



Please note that in the case of consecutive failed preboot authentication attempts the Lockout Policy will be enforced to prevent password guessing.

Windows Authentication

Note: Every time a user successfully logs into Windows their most current Windows Password propagates to the ProtectDrive preboot user dB.

ProtectDrive Single Sign-On Mode is ON

Assuming the ProtectDrive Single Sign-On mode is ON; the user is then automatically authenticated into their relevant Windows (Domain) following successful preboot authentication.

ProtectDrive Single Sign-On Mode is OFF

In the case of no Single Sign-on the following standard Windows Domain authentication screen will display.

The following standard Windows Domain authentication screen will display upon the pressing of the **CTRL+ALT+DEL**. The relevant Windows Domain Usernames and Passwords apply.

Chapter 9
Extraordinary Authentication Scenarios

Note: If System Policy has been configured to disable preboot authentication (see **Activate Preboot Authentication** in the **Authentication Tab**); then none of the material in this chapter applies. In this case the user will be presented with a standard Windows Domain authentication dialog, and normal Windows logon applies.

In addition to normal preboot user authentication System Policy can be configured to accommodate the following extraordinary circumstances:

- Token User Preboot Password Fallback Procedure – this is used when a Token User misplaces their Smartcard/Token or forgets their PIN. This procedure allows for one-time preboot access to the system with some help from the System Administrator.

- User Preboot Password Recovery Procedure – this is used to accommodate a Windows Domain or Local Windows user who has forgotten his/her Windows Password. Preboot access to the system can be achieved with some help from the System Administrator.

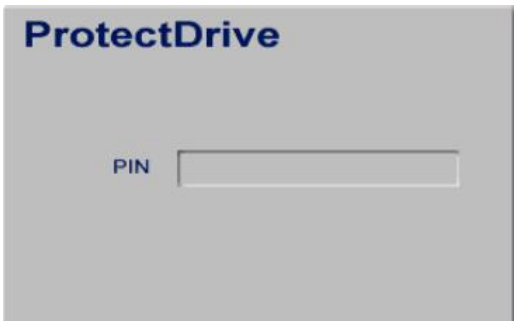
- New User Preboot Introduction Procedure- this is used to introduce newly added Windows Domain or Local Windows users to the client system's Preboot User dB. For example, this method of new user introduction would be appropriate in situations where the Active Directory User Policy has not yet replicated to the client system prior to the user's initial preboot authentication. Once the user executes this procedure and then authenticates into Windows, an account is created for him/her in the local system's Preboot User dB.

- Unattended Reboot with Automatic Preboot Authentication – if an unattended reboot followed by an automatic preboot authentication is needed by the System Administrator; then a special Preboot User account needs to be created. This function is **not** controlled by System Policy. Instead, the System Registry must be amended as described later in this chapter.

Token User Preboot Password Fallback Procedure

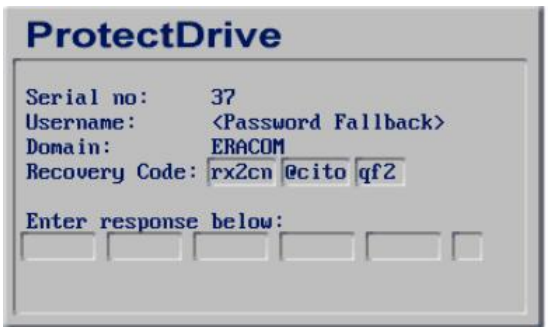
End-User Instruction

If a Smartcard/Token/PIN user misplaces their Smartcard/Token or forgets their PIN, access to the system may be achieved by exercising the ProtectDrive Preboot Password Fallback Procedure as follows:



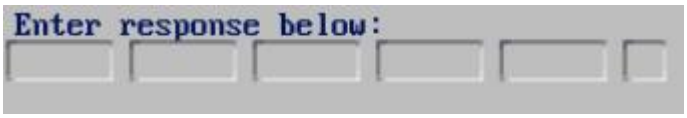
Press **[SHIFT-F9]** while the cursor is placed into the **"PIN"** field of the Smartcard/Token/PIN Preboot Log On Screen shown above.

The ProtectDrive Password Fallback Challenge/Response Screen displays.



Contact your System Administrator (either in person or by phone) and communicate to them the displayed Recovery Code (Challenge). Please note the code shown below is just an example.

In return the Administrator will communicate to you to the Response Code. Enter this code into the **"Enter response below:"** field shown below.

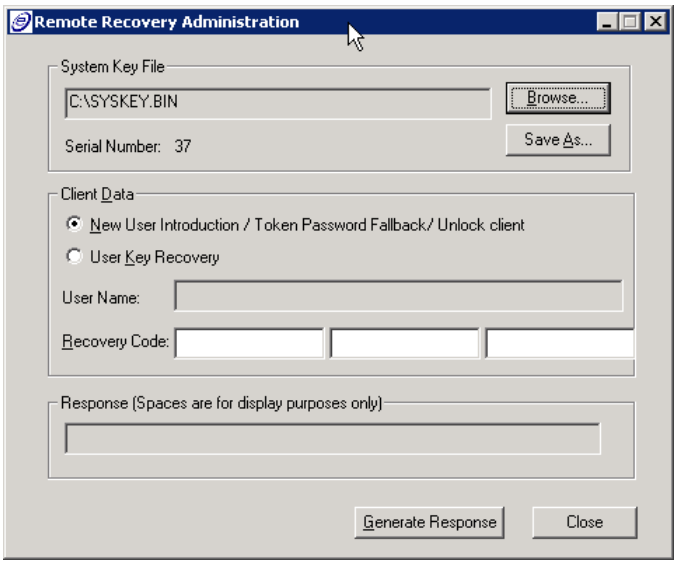


At this point Windows will proceed to load normally and will either log the user on automatically or manually depending on how the System Administrator configured ProtectDrive.

System Administrator Instruction

For user administration purposes the Preboot Password Fallback Procedure is as follows:

Run **RPADMIN.EXE** located in **\Program Files\ProtectDrive** on the server. This will result in the display of the ProtectDrive Remote Recovery Administration window shown below.



Provide the system with the Registration Disk originally used during the ProtectDrive install. The **SYSKEY.BIN** file will be used for this procedure. Alternatively, if you created a custom **SYSKEY.SKE** as described in **Creating a Custom SYSKEY.SKE** later in this chapter, then point the system to that file.

Select Token Password Fallback in the Remote Recovery Administration window.

Enter the user provided Recovery Code (a.k.a. Challenge) and press 

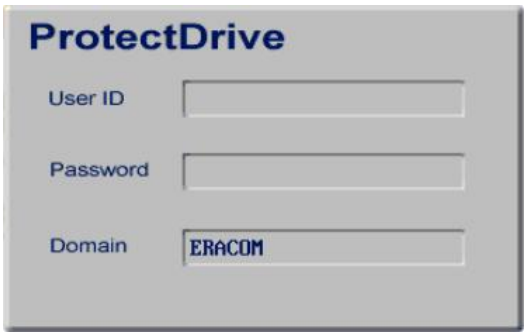
Provide the user with the automatically generated Response and instruct them to enter it into their ProtectDrive Token User Challenge/Response Screen. At this point the user will be granted one-time preboot access to the system.

Domain User Preboot Password Recovery Procedure

Note: This procedure does **not** create new preboot user accounts for newly added Windows (Domain) users. New User Preboot Introduction Procedure should be used instead.

End-User Instruction

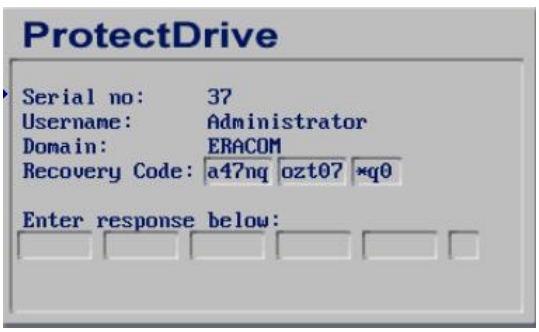
If a Username/Password/Domain Name user forgets their Password, the Preboot Password Recovery Procedure can be used to gain access to the system as follows:



Enter your Username into the **"User ID"** field shown above.

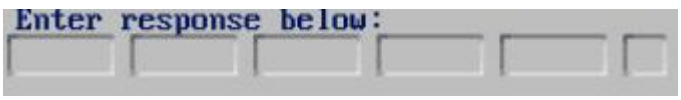
Next place the cursor into the **"Password"** field and press **SHIFT-F10**

The Password Recovery Challenge/Response Screen displays.



Contact your System Administrator (either in person or on the phone) and communicate to them the displayed Recovery Code (Challenge) along with your Username. Please note the code displayed below is just an example.

The Administrator in turn will communicate to you the appropriate Response Code. Enter the Response Code into the **"Enter response below:"** field.

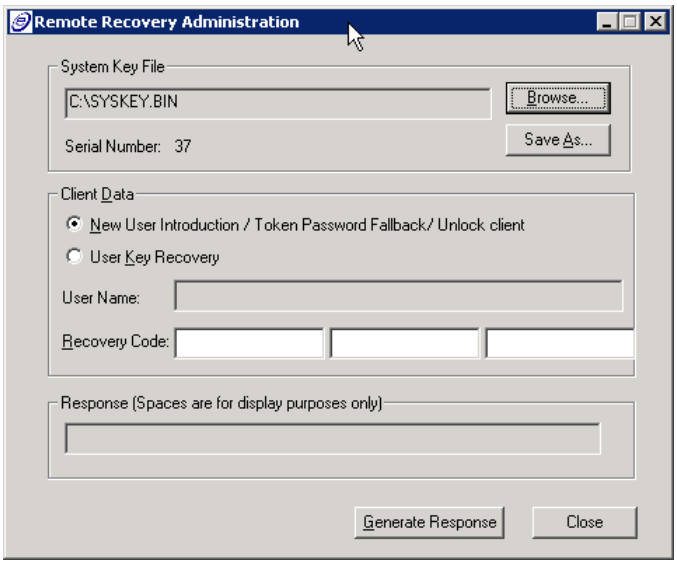


At this point Windows will proceed to load normally and will either log you on automatically or manually depending on how the System Administrator configured ProtectDrive.

System Administrator Instruction

For System Administration purposes the Preboot Password Fallback Procedure is as follows:

Run **RPADMIN.EXE** located in **\Program Files\ProtectDrive** on the server. This will result in the display of the ProtectDrive Remote Recovery Administration window shown below.



Provide the system with the Registration Disk originally used during the ProtectDrive install. The **SYSKEY.BIN** file will be used for this procedure. Alternatively, if you created a custom **SYSKEY.SKE** as described in **Creating a Custom SYSKEY.SKE** later in this chapter, then point the system to that file.

Select User Key Recovery in the above window.

Enter the user provided Username and Recovery Code (a.k.a. Challenge) and press Generate Response.

Instruct the user to enter the automatically generated Response into their respective ProtectDrive User Key Recovery Challenge/Response Screen.
At this point the user will be granted one-time preboot access to the system.

For security purposes instruct the user to change their Windows (Domain) Password as soon as they log on to Windows.

New User Preboot Introduction Procedure

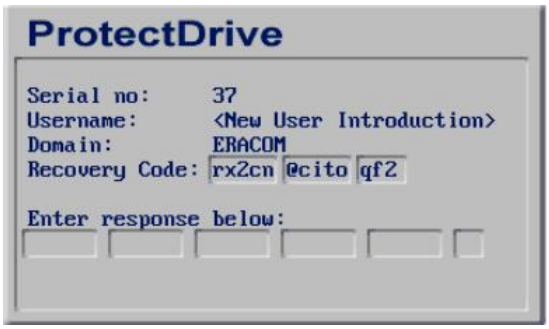
Note: This procedure does **not** apply to the Smartcard/Token/PIN users.

End-User Instruction

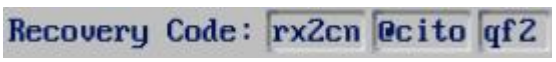
Place the cursor into the **"User ID"** field of the Username/Password/Domain Name Log On Screen (below). Note: ERACOM domain is just an example.

Press **SHIFT** and the **F9** function key while the cursor is placed into the **"User ID"** field

The New User Introduction Challenge/Response Screen displays.

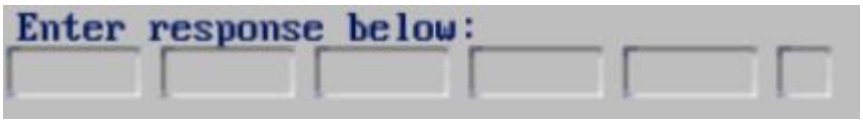


Contact your System Administrator (either in person or phone) and communicate to them the displayed Recovery Code (Challenge). Note: the code listed below is just an example.



In turn the System Administrator will communicate to you the appropriate Response Code.

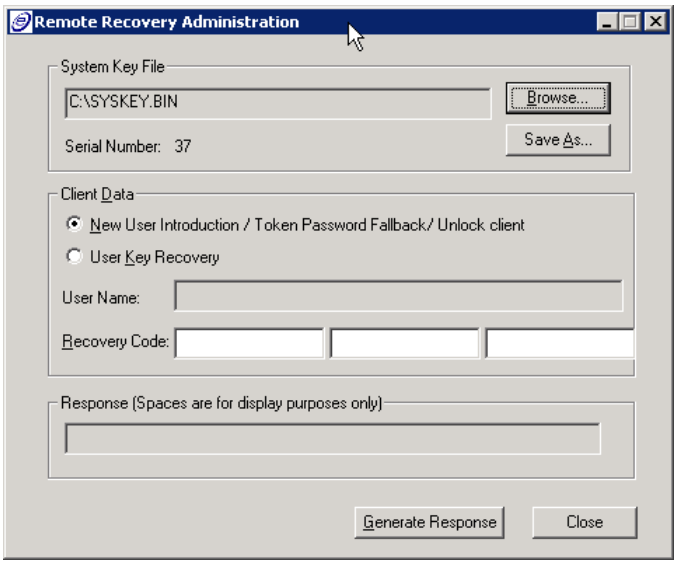
Enter the Response Code into the **"Enter response below:"** field and one-time-only preboot access to the system is granted. The user then proceeds to normal Windows log-in.



System Administrator Instruction

For System Administration purposes the New User Introduction Preboot Procedure is as follows:

Run **RPADMIN.EXE** located in **\Program Files\ProtectDrive** on the server. This will result in the display of the ProtectDrive Remote Recovery Administration window shown below.



Provide the system with the Registration Disk originally used during the ProtectDrive install. The **SYSKEY.BIN** file will be used for this procedure. Alternatively, if you created a custom **SYSKEY.SKE** as described in **Creating a Custom SYSKEY.SKE** later in this chapter, then point the system to that file.

Select New User Introduction in the Remote Recovery Administration window shown above.

Enter the user provided Recovery Code (a.k.a. Challenge) and press 

.

Instruct the user to enter the automatically generated Response into their respective ProtectDrive New User Introduction Challenge/Response Screen.

At this point the user will be granted one-time preboot access to the system. Once the user successfully completes their postboot Windows authentication a new preboot user account is created for them in the local system's ProtectDrive Preboot User dB.

Unattended Reboot and Automatic Preboot Authentication

Certain system administration tasks require unattended system reboots and automatic loading of the operating system. For these purposes ProtectDrive is provisioned for creation of the Dummy Preboot User account. Creation of this account combined with the following additions to the Windows Registry allows for the automatic, unattended pre-boot system authentication. Note that the unattended preboot will disable Single Sign-On independent of the System Policy setting. The system will automatically log in at preboot, load Windows and stop at the Windows (Domain) Log On screen.

The Unattended Preboot Authentication setup procedure is as follows:

Create a new preboot user account with **any unique** Username and Password. One way to do this is to use the **`PDUSERDB.EXE`** (see Chapter 10)

Amend the Windows Registry as shown below

`HKLM\SOFTWARE\`
`\ERACOM TECHNOLOGIES AUSTRALIA PTY. LTD\PROTECTDRIVE\`

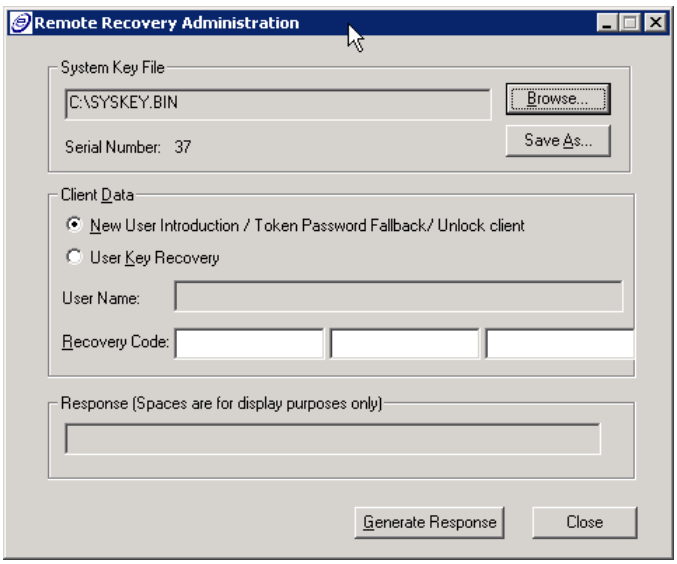
`APB_COUNT`	`REG_DWORD` **`0`**`, >0`	Set to zero (0) by default it allows no automatic pre-boot authentication. Maximum number of automatic preboot authentications allowed. If any one of the automatic preboot authentications attempts fails this value is reset back to zero (0). If set to a value greater than 0 (N>0), then N number of automatic preboot authentications is allowed.
`APB_USERNAME`	`REG_SZ`	Username.
`APB_PASSWORD`	`REG_SZ`	User Preboot Password.
`APB_DOMAIN`	`REG_SZ`	Domain Name for the User.

APB_RESETINTV	REG_DWORD **0**,1	The default value is 0 causing no change in the normal ProtectDrive operation. When set to one (1) this option will suppress the standard ProtectDrive warning message displayed when any system tampering is detected. This can be useful when performing a BIOS upgrade, which potentially changes the interrupt vector addresses, as part of automated system maintenance.

Creating a Custom SYSBIN.SKE for Use with RPADMIN.EXE

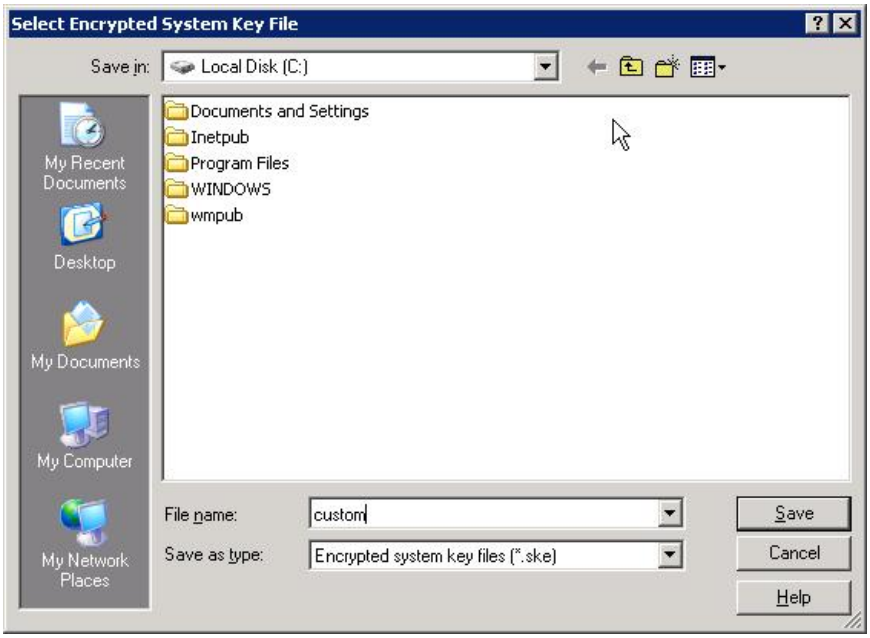
When using **RPADMIN.EXE** it is possible to create an encrypted **SYSKEY.SKE** file to be used in place of the **SYSKEY.BIN** originally used during ProtectDrive deployment.

This will provide protection for the sensitive key files, if they are not kept physically secure. Follow this procedure to achieve this.

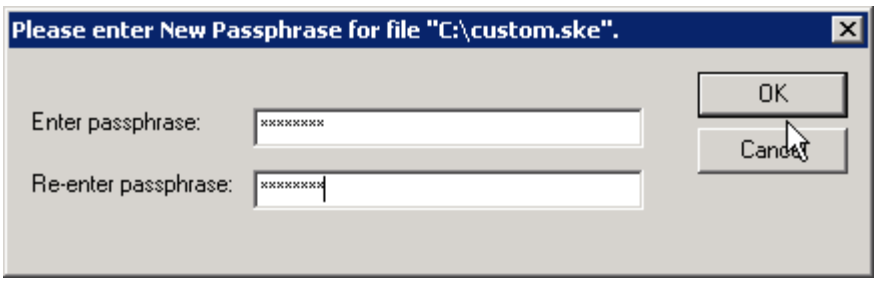


Click on 

and point to a location for saving the **SYSKEY.SKE**



Provide RPADMIN with a Pass Phrase. Use this Pass Phrase every time you use RPADMIN with this **SYSKEY.SKE** file.



Chapter 10
Disaster Recovery Tools

BACKUP.EXE – Creating ProtectDrive Recovery Files

In preparation for disaster recovery the command prompt utility **`BACKUP.EXE`** must be used following each disk encryption status change. Note that you can also run this utility as a scheduled administrative task.

`Usage:` **`BACKUP.EXE [options]`**

Options	Description	Default
`/? | -usage`	Displays usage help	
`/v | -ver`	Displays utility version	
`/t | -tgt`	Specifies target directory for backed up **Recovery Files**	Current directory. Note that it may be good practice to store the Recovery Files off the client system. This will ensure their availability in cases when the client system is rendered inoperable.
`/n | -noverchk`	No ProtectDrive version compatibility check is performed	

If for some reason the ProtectDrive secured system becomes inaccessible (due to data corruption for example) the System Administrator can use the following disaster recovery tools to perform system diagnosis, decrypt the hard disk(s), manipulate the MBR, and administer the Preboot User dB. The following tools are included in the **\RECOVERY** directory of the ProtectDrive distribution CD. These tools along with the original *Registration Disk* and the Recovery Files provide enough functionality to recover any inoperable ProtectDrive system.

DISPEFS.EXE – ProtectDrive Diagnostic Utility

This diagnostic tool displays contents of the ProtectDrive system files. ProtectDrive stores system data in a number of files contained in the embedded file system.

Usage: **DISPEFS.EXE [options] [>output_text_file]**

Options	Description
/? | -usage	Displays usage help
/a | -all	Displays contents of all ProtectDrive system files
/d | -dtes	Displays drive table entries
/c | -cfg	Displays configuration data
/k | -dky	Displays key data
/x | -ex	Displays exchange data
/u | -user	Displays the Preboot User dB.
/r | -rec	Displays data from Recovery Files
/rp | -recpath	Specifies the path to the Recovery Files
No Arguments	Displays all system files

DECDISK.EXE - Disk Decryption Utility

This is a 16-bit MS-DOS command prompt disk decryption utility. It should be used only when access to the GUI-based decryption mechanism is not available for use.

Usage: **DECDISK.EXE [options]**

Options	Description	Default
/? | -usage	Displays usage help	
/v | -ver	Displays utility version	
/kp | -keypath	Specifies the *Recovery Disk* path	Current directory
/t | -recover	Uses *Recovery Files* for the decryption operation	
/r | -recpath	Specifies the path to the *Recovery Files*	Current directory
/a | -all	Decrypts all encrypted partitions	User specified
/e | -est	Specifies the hard disk sectors corresponding to the region intended for decryption	

DECDISK will initially display partition information for all known hard disks. The output will be similar to that below.

```
Partition Information

Disk    Start Sector    End Sector     Megabytes      Type....
1       63              16771859       8189           Primary (Boot)
1       16771923        78140159       29964          Logical
2       63              417689         203            Primary
2       417690          10217339       4784           Primary
2       10217403        12498569       1113           Logical

Area  Disk  Start Sector      End Sector     Algorithm      Megabytes      %     Enc'ed
        Type
1.    1     63                16771859       3DES CBC       8189           100.00
        Primary
2.    2     6771923           78140159       3DES CBC       29964          100.00
        Logical
3.    2     63                417689         3DES CBC       203            100.00
        Primary
4.    2     417690            10217339       3DES CBC       4784           100.00
        Primary
5     2     10217403          12498569       3DES CBC       1113           100.00
        Logical

Select encrypted area to decrypt. (Ctrl-C to exit) _
```

In the above example **DECDISK** displays information regarding all known hard disk partitions. Disk is the physical disk number. Start Sector and End Sector are relative to the start of the physical disk. **DECDISK** also displays information regarding encryption status of the above partitions. Start Sector and End Sector show the extent of the encryption. The value in Area is used to select which area to decrypt.

The information above portrays two physical disks. First disk has primary and extended partitions containing one logical drive. The second disk contains two primary partitions and an extended partition containing one logical drive. All partitions on these disks are fully encrypted with triple DES.

The user is required to select one of the encrypted areas to decrypt. As the decryption progresses the user is informed of the percentage of the encrypted area still to be decrypted and approximately how long the decryption will take as follows:

```
75.10%      3hrs:15mins remaining (Press Ctrl-C to stop)
```

Once the decryption is complete, the list of encrypted areas will be refreshed. When there are no more encrypted areas the following will message will display:

```
No encrypted areas found.
```

Using Recovery Files

In case of serious system corruption, the ProtectDrive system files may not be accessible. In this case **DECDISK.EXE** requires the backed up **Recovery Files**. These files are produced using **BACKUP.EXE** during normal ProtectDrive operation.

The following command line syntax example allows the user to select partitions for decryption.

```
decdisk –kp l:\pd\key –r –rp l:\pd\recover
```

Manually Specifying Decryption Area (`/e | -est option`)

DECDISK decrypts disk areas selectable by sector number. User manually provides the Start and End Disk Sectors and the Algorithm as follows:

```
Partition Information
Disk    Start Sector   End Sector     Megabytes      Type....
1       63             16771859       8189           Primary (Boot)

Enter disk number 1
Enter start sector 63
Enter end sector 16771859
Enter Alg (1=DES, 2 = 3DES, 3 = Idea) 3

----------------------
Area Disk Start Sector   End Sector    Algorithm     Megabytes % Enc'ed
1.    1     63           16771859     3DES CBC      8189       100.00

Select encrypted area to decrypt. (Ctrl-C to exit)
```


RMBR.EXE – MBR Recovery Utility

The ProtectDrive Boot Manager/Master Boot Loader is the very first utility that runs after the system BIOS is loaded. ProtectDrive modifies part of the MBR during installation. This is done to enable ProtectDrive to locate its embedded file system upon system boot and prior to all other disk access. If the MBR is altered, replaced or corrupt after the ProtectDrive install the **RMBR.EXE** is used to recover it.

Restoring the ProtectDrive MBR requires a sector by sector search of the embedded file system located on the boot partition. Once the embedded file system is located, the ProtectDrive MBR can be restored. Reverting to the original system MBR in existence prior to the ProtectDrive install is done using the **fdisk /mbr** command.

Usage: **PDUSEDB.EXE [options]**

Options	Description
/? | -usage	Displays usage help
/v | -ver	Displays utility version
/p | -pd	Recover the ProtectDrive MBR
/o | -original	Recover the original system MBR. This is same as fdisk /mbr.
/r | -recovery	Use the ProtectDrive Recovery Files to perform any of the above operations.

RMBR Initial Status Check

Prior to performing any MBR recovery **RMBR** will display the current MBR status. If the ProtectDrive MBR has been unaltered since the install, the following message display:

Current MBR is the ProtectDrive MBR

However, if RMBR detects any alteration to the ProtectDrive MBR, the following message will display:

Current MBR is not the ProtectDrive MBR

RMBR Version Compatibility Check

RMBR will attempt to verify that it is working with the correct version of the ProtectDrive system. If the version is incorrect the following message will display:

```
Incompatible versions
ProtectDrive Version: 7.1.0 (example)
RMBR.EXE Version: X.X.X (example)
```

Note: Depending on the level of system data corruption it is not always possible to determine the version of the currently installed ProtectDrive system.

Restoring the ProtectDrive MBR (RMBR /p)

RMBR will initially display the list of all ProtectDrive partitions. Select the partition you wish to recover the ProtectDrive MBR for.

```
Disk    Start Sector    End Sector      Megabytes       Type...
1       63              16771859        8189            Primary (Boot)
(ProtectDrive)

Select partition to recovery. (Ctrl-C to exit) _
Current MBR is not the ProtectDrive MBR
Searching for super block from sector 63 to sector 20487599
99.99% and 3hrs 20mins remaining. (Press Ctrl C to stop)
```

RMBR.EXE will search the disk sector by sector looking for the ProtectDrive super-block corresponding to the start of the ProtectDrive embedded file system. It is possible that remnants of previously installed ProtectDrive systems may exist on the disk. If a super-block is found, but it is not correspond to the current ProtectDrive installation, the following message will display:

```
Found super block at sector 1893443
Incorrect super block. Continuing search ..
```

If a valid super block is located RMBR will display the version and ask the user for verification, as shown below.

```
Found super block at sector 1893443
ProtectDrive v7.1.0
Is this the correct version of ProtectDrive? [Y/N]
```

If the version is not correct enter **N** and **RMBR** will continue. If the version is correct enter **Y** and the following will be displayed.

```
ProtectDrive MBR restored.
Current MBR is the ProtectDrive MBR.
```

Restoring the Original MBR (RMBR /o)

This option replaces the current MBR with the original system MBR which ProtectDrive saved during installation. This is only supported if there are no currently encrypted drives present on the system. Otherwise decrypt before proceeding.

PDUSERDB.EXE – Preboot User dB. Administration Utility

This command line MS_DOS tool manipulates the ProtectDrive pre-boot user dB allowing the ProtectDrive Administrator to:

- List the names of users authorized to perform ProtectDrive pre-boot authentication.
- Remove Local and Domain (including Token/PIN user account) user accounts from the ProtectDrive pre-boot user dB.
- Add Local and Domain user (including Token/PIN user account) accounts to the ProtectDrive user dB.

`Usage:` **`PDUSEDB.EXE [options]`**

Options	Description
`/? | -usage`	Displays usage help
`/l | -list`	Displays a list of all existing pre-boot users
`/r | -remove`	Removes a user from pre-boot dB.
`/a | -add`	Adds a user to the pre-boot dB.
`/c | -change`	Change Password for a ProtectDrive user
`/d | -domain`	Windows Domain the newly added user is a member of. This defaults to the *Local System Name*.
`/f | -file`	Specifies filename of a file containing user certificate.
`/n | -name`	Username to add to the pre-boot dB.
`/p | -password`	Password of the newly added user

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 11
Troubleshooting

Disk Encryption Warning

If **Show Disk Not Fully Encrypted Warning** option on the **Disk Encryption (System Policy) Tab** is set, and any of the drives are found to be unencrypted or partially encrypted; then the following warning message will display right after the loading of the Windows Explorer Shell.

ProtectDrive User Authentication Activity Tracking

If **Show Logon Information** and/or the **Show Unsuccessful Logon Warnings** options on the **User Shell (System Policy) Tab** are set; then after successful Windows authentication and right before the loading of the Windows Explorer Shell the following two (2) ProtectDrive information dialogs will display alerting the user to all of their ProtectDrive preboot authentication activity to date.

Incorrect Preboot Username and/or Password

Lockout Policy defines the maximum number of failed preboot authentication attempts along with the lockout period. If this condition occurs, ProtectDrive will display the following **User Lockout Screen**. A count down period will commence for a period defined by Lockout Policy. The system will be inoperable during this time.

Preboot Log On Failure Due to System Inoperability

If any of the ProtectDrive system files and/or encrypted hard drive partitions experience corruption, the user may not be able to authenticate into the system at preboot. In these isolated instances an error screen similar to the one shown below will display. The screen will list an *ACS Error Code*, which the user needs to communicate to the System Administrator. Please note that ACS0301 is just an example. See Appendix D for a complete listing of ACS Error Codes.

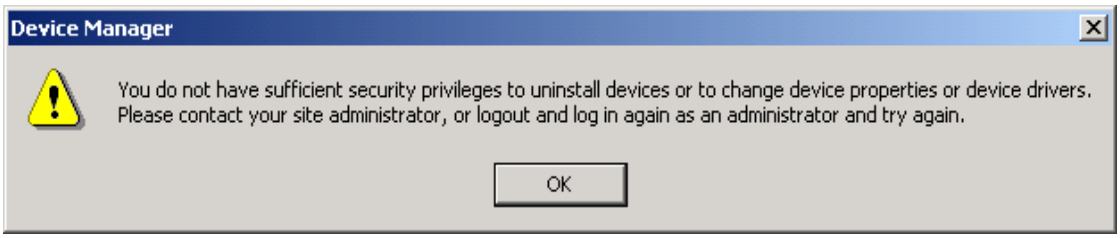
Disallowed Floppy Device Access Error

If System Policy and/or User Policy disables floppy drive access, and the user attempts to access the floppy drive; then the following error will display.

Disallowed COM and LPT Port Access Error

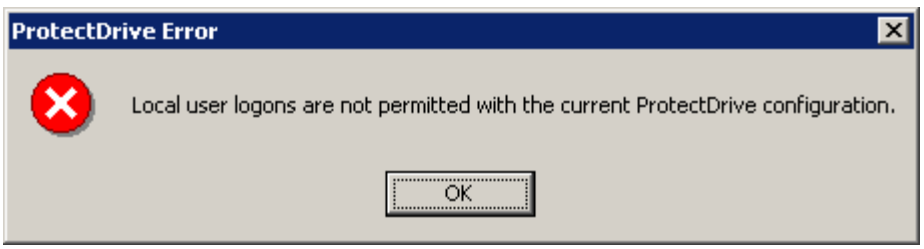
If a user who's ProtectDrive *Device Access Permissions* are disabled attempts to access any of the devices including the COM and LPT ports the an error will occur. This error may be displayed by the actual software application the user is running, through which the device is being accessed. For example while using the Windows HyperTerminal the user may try to use the COM port(s) permissions for which are currently disabled by ProtectDrive. In this case HyperTerminal will display some sort of device access (or read/write) error. In isolated instances ProtectDrive itself will display the following message. In these instances the user is advised to contact their respective system administrator for further assistance.

.



Disallowed Local Windows Authentication Error

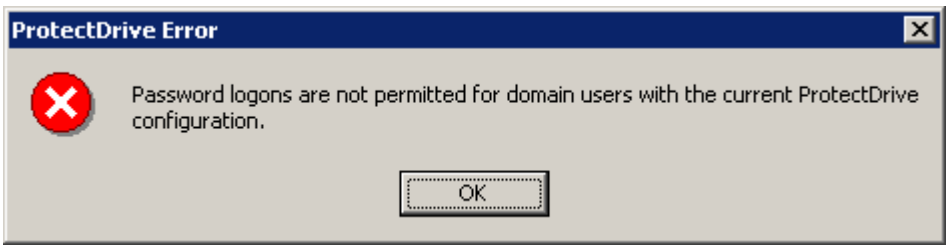
If the **Allow Local User Access** authentication System Policy option is disabled, and the user attempts to authenticate postboot into the Local Windows by specifying *Local System Name* in the "**Domain**" field of the Windows Log On Screen; then the following error will display.



Note that if **Allow Local Password Access** and **Allow Domain Password Access** are both disabled then pressing **CTRL-ALT-DEL** will have no effect. Similarly, if **Allow Domain Token Access** is disabled, inserting a Smartcard/Token will have no effect

Disallowed Postboot Windows Domain Authentication Error

If the user attempts to authenticate into the Windows Domain using the Windows Log On Screen, but the Allow Password Domain User Access authentication System Policy option is disabled; then the following error will display.



Invalid Password Format Error

If a user attempts to change their Windows Domain or Local Windows password by specifies a string that falls outside the ProtectDrive defined Password Policy limits; then the following error will display. Please note that as an example the following error was generated on a system where Password Policy requires password strength to be between 7 and 20 characters.

Error Saving Local Configuration Data to Active Directory

The following error may occur when the Local Machine Configuration utility has trouble saving System Policy data in the Active Directory. This may be due to connectivity problems or other reasons for which the Computer Object account can not be reached on the domain controller. This may also occur if the computer object does not have permissions to write ProtectDrive configuration data to the Active Directory. Follow the steps outlined in the section titled Enabling Clients to Store ProtectDrive Policy Data in the Active Directory**.** Finally, this may also happen if the client's Computer Account has been removed from the domain controller. To fix this un-join the Windows Domain on the client system and then rejoin it.

Appendix A
Smartcard/Token/PIN User Authentication

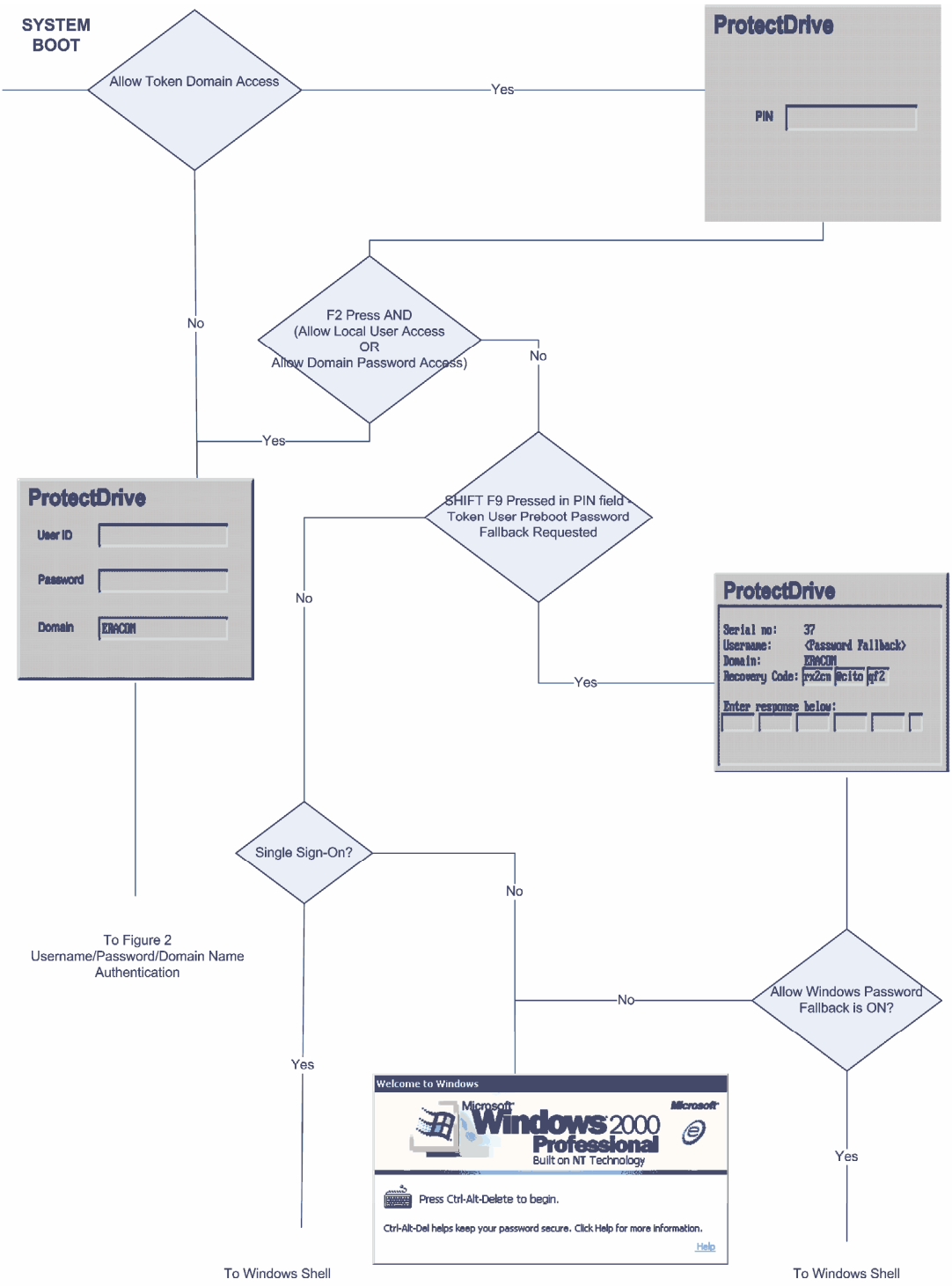


Figure 1
Smartcard/Token/PIN
Preboot Authentication

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix B - Username/Password/Domain Authentication

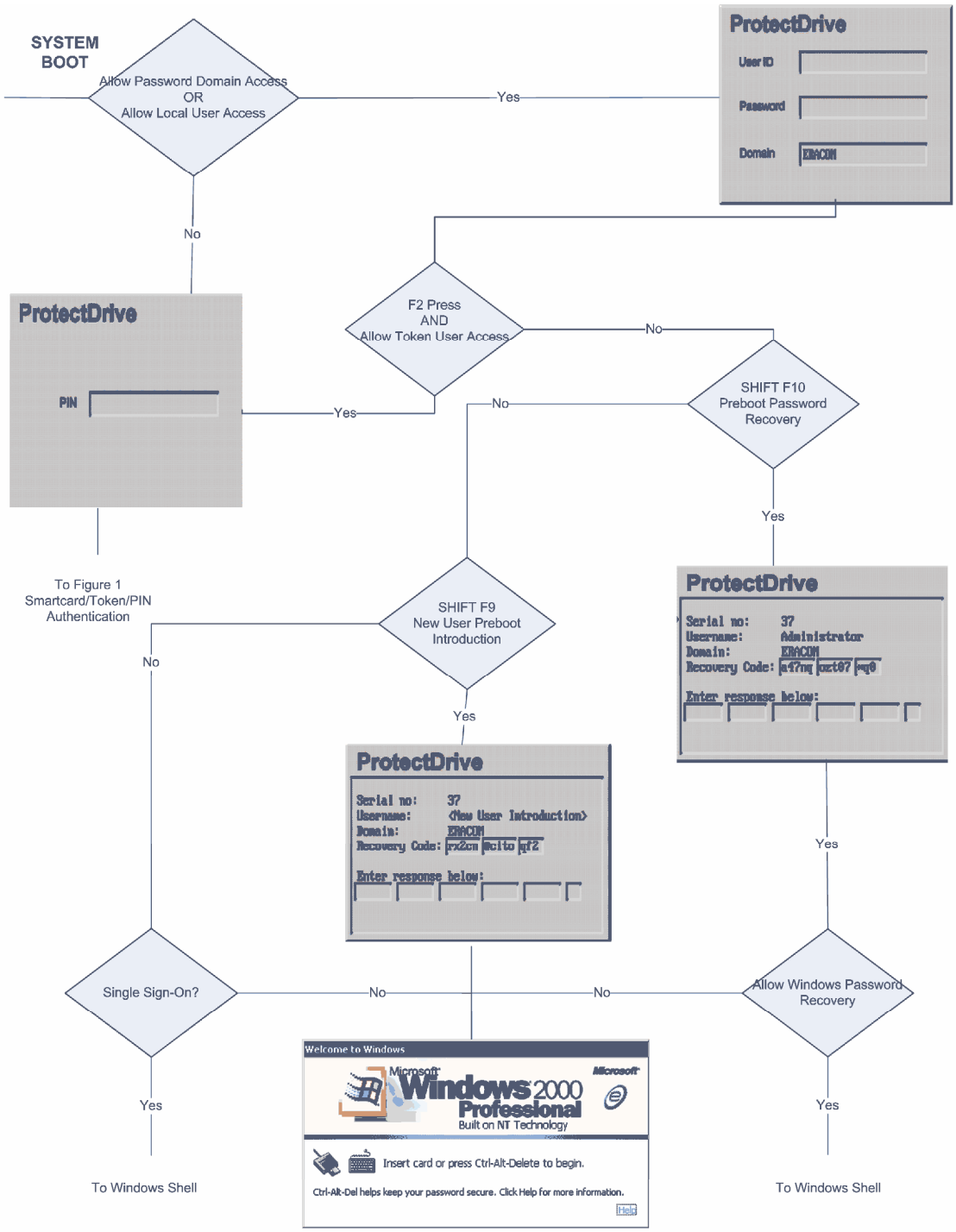


Figure 2
Username/Password/Domain Name
Preboot Authentication

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix C -
Postboot User Authentication into Windows

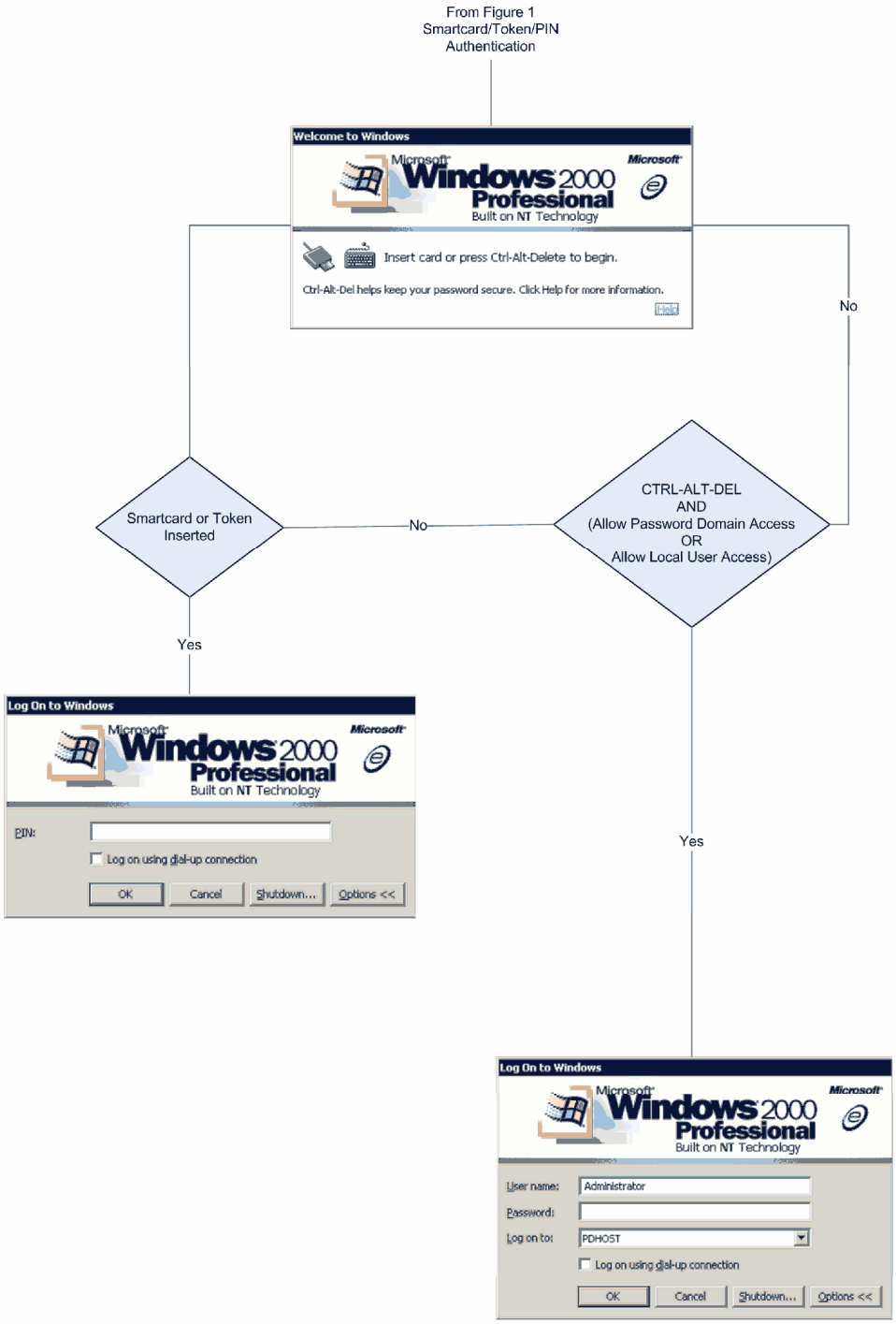


Figure 3
Smartcard/Token/PIN or
Username/Password/Domain
Postboot Authentication

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix D
System Debug and ACS Error Messages

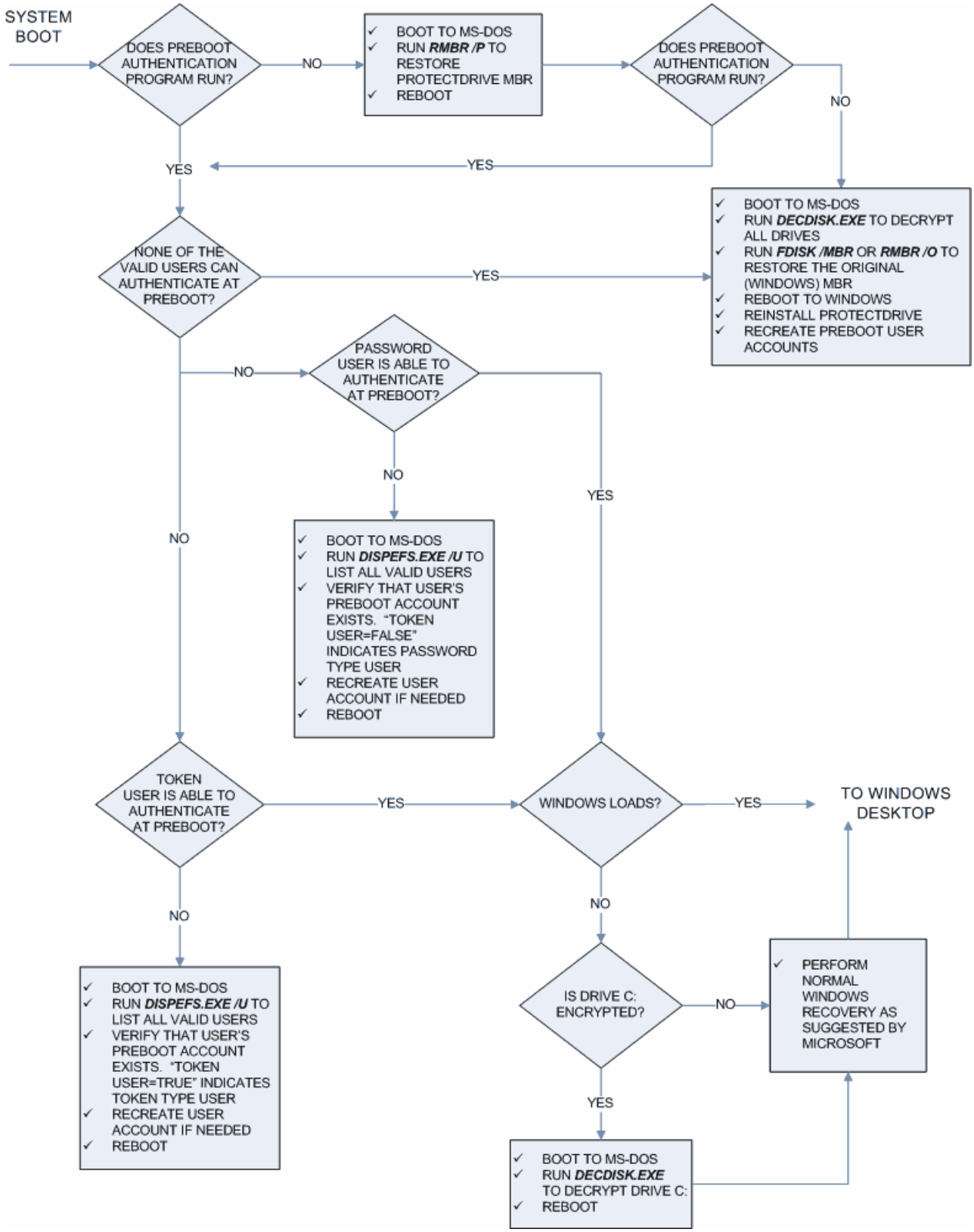
Before proceeding familiarize yourself with the contents of Chapter 10 - Disaster Recovery Tools.

System Debug

Problem	**Fix**
Password type account user can not be authenticated by the ProtectDrive Preboot Authentication program.	Run *Dispefs.exe /u*. This will display a list of all users and their account types. Password type account users are indicated with **Token User = False** setting. If the user is shown to have a Password account type; then it is possible they are entering an invalid password. Passwords are case sensitive. Finally, if the user is positive they are entering the correct password, and no other user is able to log on; then the ProtectDrive files have become corrupt. See below for *ProtectDrive appears to be corrupt.*
Smartcard/Token type account user can not be authenticated by the ProtectDrive Preboot Authentication program.	Run *Dispefs.exe /u*. to list of all existing users and their account types. Smartcard/Token type account users are designated with **Token User = True** setting. Although a user may have one or more token accounts, it is possible that the Certificate contained by the token does not match the Certificate originally used for this user's record creation in the ProtectDrive Preboot User dB. Note that users may have multiple records in the preboot user dB. The "Hash" field displayed by *Dispefs.exe* /u is the same as the "Thumbprint" field displayed when certificate details are viewed in Windows. Finally, if the user is positive they are using a valid token, and no other user is able to log on; then the ProtectDrive files have become corrupt. See below for *ProtectDrive appears to be corrupt*.

User successfully authenticates at Preboot but Windows does not boot.	It's possible that one of the Windows system files is corrupt. If Drive **C** is not encrypted, proceed with normal Windows recovery. If Drive **C** is encrypted, run *Decdisk.exe* to decrypt the system drive and enable Windows Recovery tools access the system drive.
ProtectDrive Preboot Authentication Program does not run.	If *fdisk /mbr* or another utility has replaced the ProtectDrive MBR the Preboot Authentication program will not be run. If the system drive is encrypted the operating system will also fail to load. If the system drive is not encrypted, but other drives are, the operating system will load but access to the encrypted drives will be prevented by the ProtectDrive driver. To recover from this situation run *rmbr /p*.
ProtectDrive appears to be corrupt.	If ProtectDrive is corrupt; then one of the following is possible: 1 Preboot Authentication Program will not run or behaves strangely. 2 Valid users can not be authenticated at preboot. 3 Operating system fails to load. If none of the above sections apply or you failed to restore ProtectDrive to normal working order; then all the encrypted drives will need to be decrypted using *Decdisk.exe.* If *Decdisk.exe* is unable to access the ProtectDrive Embedded File System (EFS); then use the Recovery Files originally created by *Backup.exe*. Once all the drives have been decrypted, run *fdisk /mbr* or *rmbr /o* to restore the ProtectDrive MBR. It is possible to boot the operating system once the system drive has been decrypted. It is not possible to uninstall ProtectDrive until all drives are decrypted.

The following flowchart represents the system debug information listed above. It is included for additional information.



ACS Error Messages

The ProtectDrive Access Control System (ACS) becomes active when a computer with ProtectDrive installed boots up. If an error occurs during its initialization, the system will display an error message composed of an error number and a brief description.

Error numbers are composed of three components:

CTXX where:

C	is the module the error occurred in
T	identifies the type of error and
XX	is the actual error number

Module identifiers are:

0	Master Boot Loader (MBL)
1	VXBIOS
2	Not used
3	VROM

Type identifiers are:

0	Not used
1	Warning
2	Error
3	Fatal

The following table lists all ACS errors together with their possible causes and recommended recovery action.

Note: The Standard Recovery Procedure referred to in the table is described at the end of this chapter.

ACS Error	Component	Description	Possible cause	Recovery action
0301	MBL	Invalid master boot code checksum	MBR corruption MBR Trojan attack	Run RMBR.EXE to recover the ProtectDrive MBR.
0305	MBL	Invalid VXBIOS	Signature, checksum or size verification of the VXBIOS failed possibly caused by disk corruption	Contact Eracom Support
0306	MBL	Invalid master boot record signature	MBR corruption MBR Trojan attack	Run RMBR.EXE to recover the ProtectDrive MBR.
0307	MBL	No ERACOM partition info	Partition table corruption or changeAddition of fixed disk after ProtectDrive installation	Run RMBR.EXE to recover the ProtectDrive MBR.
0313	MBL	Disk i/o error reading sector stack	Disk IO error (Hard disk failure) or partition table corruption	Run RMBR.EXE to recover the ProtectDrive MBR.
0314	MBL	Disk i/o error reading VXBIOS	Disk IO error (Hard disk failure) or partition table corruption	Run RMBR.EXE to recover the ProtectDrive MBR.
1100	VXBIOS	System Not Initialised	System could not load the disk encryption key or the DTE EFS is missing or corrupted.	Standard Recovery Procedure
1204	VXBIOS	VROM load Error	VROM file is missing, has an incorrect size or a read error occurred	Standard Recovery Procedure
1205	VXBIOS	VROM Status Error	VROM signature verification failed or the program loader reported an error.	Standard Recovery Procedure
1300	VXBIOS	Insufficient memory	Failed to allocate memory for the VROM Insufficient memory available	Try to free up resources
1301	VXBIOS	GDA file load error	GDA file is missing or a read error occurred when tying to initialize encryption information	Standard Recovery Procedure
1310	VXBIOS	Cannot Init EFS	EFS corruption	Standard Recovery Procedure

ACS Error	Component	Description	Possible cause	Recovery action
1311	VXBIOS	VROM load Error	VROM file is missing, has an incorrect size or a read error occurred (Displayed after a ACS1204 error)	-
1312	VXBIOS	VXVECT save fail	Failed to store original disk interrupt service routine (ISR) address in the EFS super block EFS corruption	Standard Recovery Procedure
1313	VXBIOS	SBLK get fail	Failed to locate the EFS Super Block	Run RMBR.EXE to attempt to restore the ProtectDrive MBR
1314	VXBIOS	Info open fail	Missing VDX EFS file EFS corruption	Standard Recovery Procedure
1315	VXBIOS	Info write fail	EFS corruption	Standard Recovery Procedure
1316	VXBIOS	VROM EXEC fail	Failed to execute the VROM (Displayed after a ACS1205 error)	-
1317	VXBIOS	Info read fail	EFS corruption	Standard Recovery Procedure
1318	VXBIOS	Diskette boot fail	Master Boot Loader signature verification failed; Missing operating system on floppy disk	Use bootable floppy diskette; Eject floppy diskette from drive and boot from hard disk
1319	VXBIOS	GDA open fail	GDA file is missing when trying to load (and execute) the original MBL.	Standard Recovery Procedure
1320	VXBIOS	GDA read fail	A read error occurred on the GDA file when trying to load (and execute) the original MBL.	Standard Recovery Procedure
1321	VXBIOS	Boot fail	Master Boot Loader signature verification failed.	Standard Recovery Procedure
3301	VROM	Too many logon attempts	Forgotten password Corrupted user database	Log on as other user; Exercise user key recovery; Run DISPEFS.EXE

ACS Error	Component	Description	Possible cause	Recovery action
3302	VROM	I/O error reading disk	Corrupted EFS Hard disk failure	Standard Recovery Procedure
3304	VROM	An unknown error has occurred	Internal program error	Standard Recovery Procedure
3305	VROM	Configuration file has been corrupted	MAC check of configuration file failed Corrupted EFS	Standard Recovery Procedure
3306	VROM	User information has been corrupted	MAC check of user database entry failed Corrupted EFS	Log on as different user at preboot and let failed user log on to Windows. User database entry will be regenerated. Alternatively, exercise user key recovery mechanism.
3308	VROM	ProtectDrive Administrator information has been corrupted	MAC check of ProtectDrive Administrator failed; Corrupted EFS	Log on as different user at preboot and let failed user log on to Windows User database entry will be regenerated. Alternatively, exercise user key recovery mechanism.
3309	VROM	Configuration file has been fatally corrupted	EFS corruption Hard disk failure	Standard Recovery Procedure
3310	VROM	Error occurred initialising the token	The token module could not be initialised and password logons are not allowed.	To diagnose this error further contact Eracom. To get access to the system exercise the token password fallback function.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix E
Additional Guidance Regarding Security

Evaluated Versions of ProtectDrive

This chapter provides important guidance to users of evaluated versions of ProtectDrive. Evaluation of ProtectDrive is based on assumptions contained in a Security Target for the evaluation.

The Security Target describes the basis of the evaluation including:

- Threats that the security claims of ProtectDrive are designed to counter
- Environmental and organizational assumptions required to support the security claims
- Constraints to the configuration of the ProtectDrive required to support the security claims

When relying on an evaluated version of ProtectDrive users should follow the recommendations in this chapter, refer to the evaluation Security Target and refer to the Certification Report for guidance on use of the evaluated version of ProtectDrive.

The Security Target and the Certification Report can be found at the Common Criteria Evaluated Products List (EPL). Both the Security Target and Evaluation Technical Report are available on-line on completion of an evaluation.

This list, for ProtectDrive, may be found at:

`http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html`

Guidance for Users of ProtectDrive

Further Reading Relevant to the CC Certification

The following documents should be read in conjunction with this manual:

- Security Target
- Certification Report
- Release Notes included on the distribution CD
- README.TXT included with the distribution CD

Users are reminded that evaluated versions of ProtectDrive are based on assumptions contained in the evaluation Security Target. In particular the following chapters should be read: Chapter 3 – Assumptions; and Chapter 4 - Security Objectives for the Environment. These chapters describe the responsibility of users and detail requirements needed to ensure that ProtectDrive product is used and administered securely.

Delivery Procedures

Standard commercial practice is used for the packaging and delivery of ProtectDrive. Registered copies of ProtectDrive are distributed in a shrink-wrapped package that comprises:

- a CD-ROM containing the ProtectDrive software, user manual, Release Notes and a **`README.TXT`** notice
- a diagnostic floppy disk holding licence information
- a licence certificate
- a support agreement certificate (if a support agreement has been purchased) and
- a packing list.

On receipt of a delivery you should:

- Check the delivery for any signs of tampering. Eg shrink wrap package open or damaged.
- Check the packing list to ensure all items are correct and that the customer purchase order number and the Eracom Technologies sales order number are consistent with the delivery.

On opening the package you should verify the product identification by checking the product version number which is printed on the CD-ROM, and on the packaging.

If there are any signs of tampering or any inconstancies with the delivery or the product version then you should immediately notify Eracom Technologies.

Product Identification

To ensure that the copy of ProtectDrive you have is authentic and the correct version you should:

Before Installation:

- As noted above, under "Delivery Procedures", if the product or its packaging shows signs of tampering when it is received, you should notify Eracom Technologies for advice before using the product.
- Check the product version number on the CD volume label. You should ensure that the volume label identifies the version as PD x.yy.zz where x.yy.zz is the ProtectDrive version number e.g PD 7.02.02. If you are using an evaluated version of ProtectDrive ensure that the version you are installing matches the version listed in the Evaluated Products List.
- If installing The ProtectDrive from an electronic archive then ensure that the file name is pd_x_yy_zz where x_yy_zz is the version number.
- Ensure that the files README.TXT and Release Note, on the distribution CD-ROM refer to the product version being used.
- All files in the ProtectDrive installation package are electronically signed. The file PD_x_yy_zz.sig contains the signatures of all files contained in the installation package. To verify the integrity of the installation package, download and use the file verify utility from Eracom Technologies Internet site.

  http://www.eracom-tech.com/resources/fileverify

Instruction for using the File Verify utility may be found in the File Verify Technical Bulletin which is available from the same location as the File Verify utility. The File Verify utility may also be obtained by contacting the Eracom Technologies support section.

After Installation

Verify the version number of ProtectDrive after installation by starting the ProtectDrive About application. Navigate to:

Start|Programs|ProtectDrive|About ProtectDrive

Verify that the version number displayed matches the expected version number of the installed software.

Organizational Requirements

Connections to Outside Systems

Those responsible for management of the systems in which ProtectDrive is used must ensure that no connections are provided to outside systems that would undermine the security features of ProtectDrive.

Guidance

Guidance should be provided that details the delivery, installation, configuration, administration and operation of ProtectDrive within an organization.

Tampering

The system on which the product is installed must have features that detect physical tampering and provide a clear indication to users that tampering has occurred. Users must be able to regularly check the system for indications of tampering.

Training

All users of ProtectDrive with administrator privileges must receive sufficient training to enable them to securely administer ProtectDrive.

Users of ProtectDrive with administration privileges are responsible for implementing guidance that ensures ProtectDrive is installed, configured, administered and operated in a secure manner consistent with the evaluated configuration.

Tokens

Smartcards or Tokens used with ProtectDrive, for authentication, must provide an adequate level of security to protect authentication information and perform the functions required by ProtectDrive. This security may be gained though assurance of the Smartcard or Token or a combination of Smartcard or Token assurance combined with organizational procedures.

Users

Users of ProtectDrive must receive sufficient guidance and training to be able to fulfill their duties.

USB and other I/O Devices

I/O devices, such as USB and Firewire ports for example, may pose the risk that protected information could be accidentally sent to a device without adequate protection. If the risk posed by I/O devices is considered unacceptable then an organization policy should be used to specify and restrict the use of these I/O devices. If the risk is considered unacceptable even through procedural policy then the I/O devices should be disabled at the operating system as a part of the system configuration. General users should not have system privileges that would enable them to change the status of an I/O Device.

ProtectDrive currently manages secure use of Floppy Disk, Serial Ports (COM) and Parallel Port (LPT). Future releases of ProtectDrive will provide secure operation of other I/O devices.

Guidance for the Operating System Configuration

General

ProtectDrive provides protection of information through pre-boot authentication and access control of peripheral devices combined with hard disk encryption. Once access is gained to a computer (by correct user authentication) the user is then responsible for ensuring that the computer is treated in accordance with organizational security policies for the level of information available.

Administrators of ProtectDrive are responsible for ensuring that the underlying operating system is correctly configured and complies with organizational security policies.

If the computer on which ProtectDrive is installed is a part of a network domain then the domain security policies must be correctly configured and comply with organizational security policies.

Password Policy

The operating system password policy must be configured in accordance with organisational policies and be consistent with ProtectDrive requirements. The following minimum settings should be used:

Enforce Password History	7 passwords
Maximum Password Age	In accordance with organisational policy
Minimum Password Age	1 day or greater if required by organisational policy
Minimum Password Length	6 characters or greater if required by organisational policy
Passwords Must Meet Complexity Requirements	Enabled
Store Password Using Reversible Encryption	Disabled

Screen Lock Feature

The operating system screen lock feature must be enabled and configured in accordance with organisational requirements. If the screen lock feature is not enabled and configured correctly, ProtectDrive security features may be subverted.

Information Relevant to Administrators of ProtectDrive

Operating Systems

Evaluated versions of ProtectDrive are tested on specific version of operating systems. For example:

- Microsoft Windows 2000 Professional, 5.00.2195 Service Pack 4
- Microsoft Windows XP Professional 5.1.2600 Service Pack 2 Build 2600.

While the product will operate with a wider range of service packs and builds, if you wish to use it in its evaluated configuration you should only use it on those specified above.

Evaluated items

Note that the "Server Edition" of ProtectDrive has not been evaluated, and nor has the "Multiple Boot Manager" functionality. Furthermore, only the "Registered Product" has been evaluated.

The evaluation does allow for the installation of ProtectDrive over a network, so this manual should be read in conjunction with the network installation manual by those administrators that will be performing the installation in that way.

Encryption Algorithm

To comply with Government advice only the AES and Triple-DES encryption algorithms have been evaluated and one these algorithms should be selected during installation. This will ensure that the correct components are installed and the choice of algorithms available for initial encryption will be limited to AES and 3DES.

Show Disk Not Fully Encrypted Warning

It is strongly recommended that this option be set ON in the evaluated configuration so that users are advised if the disk they are working on is not completely encrypted. If this is set to ON, the warnings will be displayed for all users.

Automatic Pre-boot Authentication

This option must be used with caution, and strictly as directed in the relevant chapter of this user guide.

Show Unsuccessful Logon Warnings

This should be set on in the evaluated configuration so that the user is warned of unsuccessful logons.

Access Control

ProtectDrive offers a number of access control options: User ID and Password, Token and PIN and password recovery and fallback options as well as new user introduction.

Evaluated versions of ProtectDrive may not include all access control options. When using an evaluated version of ProtectDrive users should refer to the evaluation Security Target to determine which options form part of the evaluated version. Only those access control options that form a part of the evaluated version of ProtectDrive should be enabled.

END OF DOCUMENT