

The background of the page is a white canvas with several thick, vibrant orange brushstrokes that sweep across the page from the top left towards the bottom right. These strokes vary in thickness and direction, creating a sense of dynamic movement and energy.

ProtectDrive

Network Installation Guide

Document Revision A6

Copyright

No part of this manual may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of:

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

National (07) 5593-4911
International +61 75593-4911
FAX (07) 5593-4388
website:www.eracon-tech.com

Copyright © Eracom Technologies 2004, All rights reserved

All trademarks are acknowledged as the property of their respective owners.

Disclaimer

Eracom makes no representations or warranties with respect to the contents of this manual 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 on Eracom to notify any person or organisation of such revision or changes.

Publication Improvements

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

Revision Incorporation Certificate

Revision	Release Date	Description
A0	June 2002	Initial Release
A1	20 September 2002	Rev A1
A2	July 2003	Review for ProtectDrive 6.0 release
A3	December 2003	ProtectDrive 7.0
A4	January 2004	ProtectDrive 7.0.1 Response File
A5	January 2004	ProtectDrive 7.0.1 Response Files
A6	March 2004	ProtectDrive 7.0.2 Functionality

Additional Reading

This Network Installation Guide should be read in conjunction with the ProtectDrive User Manual, including the section on Restrictions and Considerations. Those users wishing to use ProtectDrive in its evaluated configuration should especially familiarize themselves with Chapter 2 of the User Manual, and follow the directions therein.

Table of Contents

C H A P T E R 1 Installation Requirements.....	7
<i>Minimum Requirements.....</i>	<i>7</i>
Network Installation.....	9
<i>Preparing for Network Installation</i>	<i>9</i>
<i>Remote Installation.....</i>	<i>9</i>
<i>Network Installation Preparation Program</i>	<i>10</i>
<i>Network Installation: Interactive.....</i>	<i>13</i>
<i>Network Installation: Automated.....</i>	<i>13</i>
<i>Network Installation: RIS.....</i>	<i>14</i>
<i>Installation Key Files</i>	<i>14</i>
<i>Configuration Response Files</i>	<i>15</i>
Appendix A. Sample Response Files.....	16
<i>Configuration Response Files</i>	<i>16</i>
<i>Crydisk Response File</i>	<i>22</i>
Technical Support	23

This Page Intentionally Left Blank

CHAPTER 1

Installation Requirements

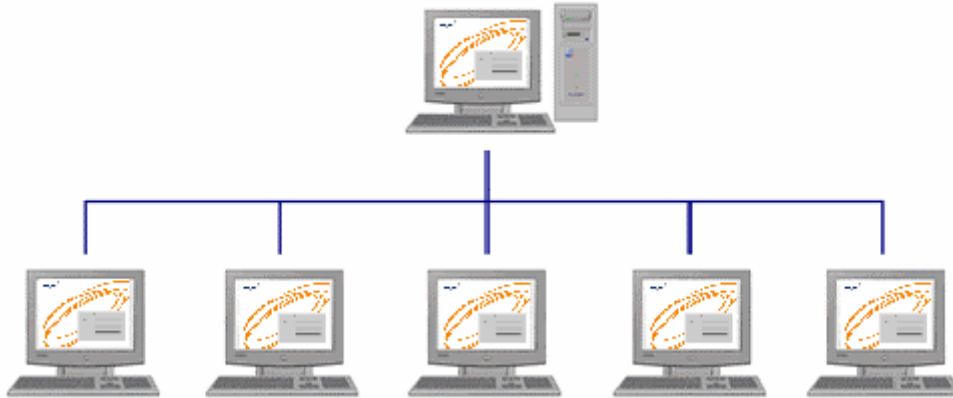
Minimum Requirements

The following are the minimum requirements:

- IBM PC or 100 % compatible, with a Pentium CPU.
- Memory: At least 32 MB system memory
- CD ROM Drive
- Diskette Drive: At least one 3.5" diskette drive for uninstallation purposes.
- Hard Disk Space: ProtectDrive Setup Program requires 20 megabytes of free disk space on drive C. On exit, Setup will free most of this space and ProtectDrive will then take up only 4 Megabytes.
- Operating System:
 - Microsoft Windows 2000 Professional Edition with Service Pack 2.
 - Microsoft Windows XP Build 2600 Activated

CHAPTER 2

Network Installation



Preparing for Network Installation

Windows 2000 servers have the capability to remotely install operating systems along with whatever utilities are required. The "model" system is downloaded following a request from a client with an appropriately prepared boot disk, or a suitable Network Identification Card (NIC). ProtectDrive can now be installed this way.

The traditional method of installing ProtectDrive over a network (Win NT or Win 2000 server) is to use the "Network Install" option. The ProtectDrive network installation allows multiple workstations to be installed from the same network directory. This requires a directory be created on a network drive, which can be accessed from the workstations onto which ProtectDrive is to be installed. When this is done ProtectDrive is setup using the Automated or Interactive install procedure.

Caution

The workstation version of ProtectDrive is not suitable for installation on Win NT/2000 servers. Separate Eracom products are available for both NT Server and the Windows 2000 and Advanced Server.

Remote Installation

The following information may facilitate remote deployment of ProtectDrive. It is not prescriptive as network environments and upgrade requirements will be site specific.

The fundamental feature of Microsoft Windows 2000 called Remote Installation Services (RIS) has to be installed on the Server together with DNS Server, DHCP Server, and Active Directory. For an overview of this, see Microsoft KBD Q298750 “HOW TO: Set Up and Configure Remote Installation Services”. For an overview of the design of RIS see the Microsoft Support WebCast “Windows 2000 Remote Installation Services”.

To install ProtectDrive on a minimal Windows 2000 client it is only necessary to prepare a Windows 2000 installation disk with Service Pack 2 added. The RIS server can then be used to make an installation image to reside on the Windows 2000 Server. ProtectDrive is installed on the Windows 2000 Server in the usual way by selecting the menu option “Prepare for Network Install” in the autorun application of the ProtectDrive CD.

Installation of ProtectDrive will be effected by the usual *setup.exe* command automatically delivered by RIS after Windows 2000 has been installed. How to modify the RIS setup files is covered in Chapter 25 of the *Windows 2000 Server Deployment Planning Guide* (www.microsoft.com/Windows2000/). Actual initiation of an upgrade at the client can be effected by the preparation of a client RIS boot floppy or by using a PXE-enabled Network Interface Card that supports network boot.

Obviously, network administrators are likely to want to install more complexly tailored Model Systems and the procedures for doing this are described in the above *Deployment Planning Guide*. Issues concerning hard disk partitioning and such parameters that have to be set *before* ProtectDrive is installed are described in the publication *Microsoft Windows 2000 Guide to Unattended Setup* which is included on the Windows 2000 installation disk.

As the RIS environment is complex, users may find useful the book *Using Windows 2000 Server* by Roger Jennings, QUE Special Edition (www.quepublishing.com), since it contains stepwise procedures and screen shots for nearly all of the preliminary set up tasks. It also provides a utility for establishing a non-trivial database of users in Active Directory, which may be found useful in pre-testing the Enterprise environment.

Network Installation Preparation Program

The ProtectDrive Network Installation Preparation program can be run to perform the steps necessary to prepare for a network installation. To run the Network Installation Preparation program, insert the setup CD into your CD-ROM drive and wait for the auto-run menu screen to

appear. If the setup menu does not start automatically, you can start it by executing `autorun.exe` from the setup CD.

Select the "Prepare for Network Installation" option from the menu.

The ProtectDrive Network Installation Preparation program will take a few moments to load.

1. The first window to be displayed allows you to select whether you require it to be an automated network installation or an interactive network installation.
2. The next window allows you to select the directory from which the network installation will be run from. All workstations that wish to run the network installation must have read access to this directory.
3. If you selected an automated network installation, the next window allows you to select the directory in which the log file (`INSTALL.LOG`) will be written. As every workstation writes the log file to `INSTALL.LOG`, it is recommended that this directory be on the workstation's local hard disk rather than on a common network drive. If all workstations wrote to the same network hosted log file, the only way to distinguish the logged events from one workstation to another is by the time stamps of the logged events.
4. All necessary files are now copied from the source (CDROM or hard disk) to the directory specified in step 2
5. If you selected an interactive network installation, the next screen will ask if you wish to create a file containing the system key in encrypted form (`SYSKEY.CID`). Creating a `SYSKEY.CID` (i.e. using Installation Key Files) will enable the interactive network installations to run without requiring the diagnostic diskette to be inserted. If you do not create a `SYSKEY.CID` now, the diagnostic diskette will need to be used during each installation.
6. If you selected an automated network installation or an interactive network installation using `SYSKEY.CID`, the next screen prompts you to insert the diagnostic diskette that will be used to create the `SYSKEY.CID` file.
If you inserted a valid registered diagnostic diskette, the information box `CIDKEY` file '`<directory specified in step 2>\syskey.cid`' successfully created, will be shown.
Click "OK" to continue.
7. If you selected an interactive network installation, the next screen will ask: "Would you like to use a response file?" If you use a response file, configuration specifications will be specified in the

Configuration Response File rather than relying on the user selecting the settings during installation.

8. If you selected an interactive network installation without using response files, the Preparation Complete screen will now be displayed. Click FINISH to exit the program.
9. If you selected an automated network installation or an interactive network installation using response files, the Finalise Network Install preparation screen informs you that you must now edit the response file(s). Click FINISH to continue – the response files will be opened using notepad ready for you to edit them.
10. Edit the response files. Once you have finished editing the response files, a message containing the locations of the response files will be displayed in case you decide to change them later.
11. Click OK to finish.

Network Installation: Interactive

This is an interactive installation requiring user inputs similar to a normal CD-ROM installation.

Installation Key Files can be used to optionally enable the installation to run without prompting for a diagnostic diskette at each workstation.

The Configuration Response File can also be used as an option to minimize user interaction during an installation.

The ProtectDrive Built-in Administrator's name and password will be set to that of the currently logged on user at the workstation onto which ProtectDrive is being installed. This user must be a member of the Windows 2000/XP Administrators Group.

To initialize this type of installation the client is requested to run `setup.exe` from the location specified during the Network Preparation.

Network Installation: Automated

This type of installation allows ProtectDrive to be installed without input from the user other than the interactions associated with the obligatory operating system shutdowns. The contents of the response files must be carefully prepared beforehand.

No user input is required at the workstation other than starting the Setup Program. The Setup Program is in itself not visible, and is driven automatically by Response Files and Installation Key Files, which enable the installation process to run without prompting for a diagnostic diskette.

Automated Disk Encryption can also be performed as part of an automated network installation. Log Files for pre-installation, installation and Automated Disk Encryption are created allowing for installation and disk encryption verification.

Unlike interactive installation options, the ProtectDrive built in administrator name and password is taken from the Configuration Response File, as such, this file should be handled securely by the administrator because it presents a level of risk. Both the user who starts the setup program and the built in administrator listed in the configuration response file must be members of the Windows 2000/XP Administration Groups with access to the directory from which setup will be run.

Both the pre-installation and installation phases of an automated network install run invisibly. The second phase (installation) may require more than five minutes to complete. Observe hard disk activity to determine if the process is running - if there is no disk activity, view the INSTALL.LOG file to see if an error has occurred.

For the reboot between the pre-installation and installation phases, the logon module will silently log on the Built-in Administrator specified in the Configuration Response File. The Automated Disk Encryption process will run visibly so that progress can be observed in the normal manner.

See the section Preparing for Network Installation for details on running the ProtectDrive setup program to perform the steps necessary to create the network directory from which an automated network installation can be run.

Network Installation: RIS

ProtectDrive for Windows 2000/XP can be installed on remote client machines over a network either as an upgrade from Windows NT or as a new installation of Windows 2000, using Microsoft Remote Installation Service (RIS) techniques.

This has been demonstrated in a test network environment using a Server on which Windows 2000 Advanced Server had been installed. Windows 2000 Server is sufficient but Windows NT server is not.

Installation Key Files

Installation Key Files can be used by all methods of installation. During normal installation, ProtectDrive requires the SYSKEY.BIN file from the diagnostic diskette to obtain the keys to be used for the installation. During a network-based installation, all required files are copied to an image directory on the server. In the case of ProtectDrive this is less than desirable since access to the server would then imply access to a facility that could be used to create a ProtectDrive diagnostic diskette. The possession of the ProtectDrive diagnostic diskette would allow an attacker to uninstall a ProtectDrive system.

To overcome this, the ProtectDrive Setup Program can install a system from a SYSKEY.BIN variant called SYSKEY.CID. This alternate file, SYSKEY.CID, is a cryptographically altered form of SYSKEY.BIN that can only be used for installation processes. It cannot be used for an uninstall operation and therefore is of no benefit to any would be attacker who obtains this file from the server.

The CIDKEY utility, which can be found in the root directory of the ProtectDrive CDROM, is used to cryptographically transform a SYSKEY.BIN to a SYSKEY.CID file.

Note: CIDKEY can only be run using a SYSKEY.BIN from a previously registered diagnostic diskette. CIDKEY requires that the correct Registration.txt file exists in the same directory as SYSKEY.BIN.

Configuration Response Files

Examples of Configuration Response files are shown in Appendix A

The file INSTALL.RSP is used to establish initial system settings and to add users.

The file CRYPDISK.RSP can optionally be used to selectively encrypt drives.

A sample configuration response file is provided with ProtectDrive and should be edited as necessary when preparing for network installation. This file is optional for Interactive Network Installations but mandatory for Automated Network Installations. (See Appendix A for a sample file)

For Interactive Network Installations it is used to provide configuration specifications other than the defaults, as well as to add users to ProtectDrive, and if they don't already exist, add other users to Windows.

For Automated Network Installations it is used in the same manner, but also provides ProtectDrive 's Built-in Administrator's name and password, as such, this file should be handled securely by the administrator because it presents a level of risk.

Appendix A.

Sample Response Files

WARNING:

If used in the context of a fully automatic installation, the response file below will contain the logon credentials (user name and password) of a user with administrative privilege (Built-in user).

The file can also be used to automatically add users to ProtectDrive with a default password; representing valid logon credentials.

Therefore the response file should be handled securely by the administrator because they present a level of risk.

Configuration Response Files

INSTALL.RSP

Below is an example of the Configuration Response File.

```
#####
# ProtectDrive Installation and Upgrade
# Sample Configuration Response File.
#
# When is it necessary to use this file?
#   Automated Network Installation
#   Automated Upgrade
#
# NOTE: For Automated Network Installation ensure SuperName and
# SuperPassword are correct. This must be a Windows user who is
# a member of the Administrators group.
#
# NOTE: For Automated Network Update only some sections of the
# response file will be used, the rest will be ignored.
#
# Syntax
# Comments begin with a #
# Keywords must begin at first column
# Blank lines are ignored
#
# Not all fields need to be present as the system will automatically
# use predefined defaults
#
#####

#####
# Installation Only Configuration Options
#####

# AllowAdditionOfRemovableDrives=(Y,N)
# Allow Removable Drives to be added after installation.
# Default is N
# By default (N) only drives present during installation can be
# accessed.
# Options
AllowAdditionOfRemovableDrives=N

# DiskEncAlgorithmGroup=(1,2)
# Disk Encryption Algorithm Group 1 = DES CBC + Triple DES CBC
```

```
#                                     2 = IDEA CBC
# Only one of the following groups of algorithms can be used.
# Select which group of algorithms you require.
# This selection cannot be altered after installation.
# Default is 1
DiskEncAlgorithmGroup=1

#####
# Installation Only Advanced Configuration Options
#####

# Show logon window after system boot (Y,N)
# By default ProtectDrive will automatically logon to Windows using
# the username and password entered at pre-boot ProtectDrive logon.
# If this option is set to Y, the user will need to log on twice
# after the system has been restarted, once at pre-boot time
# and once for Windows.
# Automatic logon to Windows can also be overridden by holding down a
# Shift key when the Windows logon window would normally be
# displayed.
# Default is N
ShowWindowsLogonAfterBoot=N

# After each logon ProtectDrive will display a window reporting
# logon information eg: Number of logons, password last changed
# etc...(Y,N)
# Default=Y
ShowLogonInfo=Y

# ProtectDrive will display an icon in the task bar notification area
# which provides a quick mechanism to lock the system. (Y,N)
# Default=Y
ShowTaskBarIcon=Y

# After each logon ProtectDrive will check to see if there have been
# any unsuccessful logon attempts. If there have been, a
# window will be displayed providing this information. (Y,N)
# Default=Y
ShowUnsuccessfulLogonWarning=Y

# If ShowUnsuccessfulLogonWarning is set to Y a custom string
# can be displayed when the user is informed that unsuccessful
# logon attempts have been made.
# Default= ( blank )
InvalidLogonMsg=

# After each logon, Display a warning (to Administrators only)
# if one or more disks have not been fully encrypted. (Y,N)
# Default=Y
DisplayUnencDiskWarning=Y

#####
# Installation Only Built-in Administrator (Supervisor) Setup
# This field is ignored unless Automated Network Installation.
#
# Ensure that the user name and password is a valid Windows
# user and a member of the Windows Administrators group.
#
#
#####

# SuperName=(string) Supervisor Name - Max 20 characters (Case
sensitive)
SuperName=Admin

# SuperDomain=(string) Supervisor Domain Name - Max 80 characters
(Case sensitive)
# Default is the local machine
#SuperDomain=DOMAIN

# SuperPassword=(string) Supervisor password Max 20 characters,
# Min 6
SuperPassword=password

# SuperTokenUser=(Y,N) Supervisor is a token user. Active Directory
```

```
# will be queried for this users information when they are added to
# ProtectDrive
# Default is N
SuperTokenUser=N

# SuperDisketteBoot=(Y,N) Supervisor can perform maintenance boot
from
# Diskette
# Default is Y
SuperDisketteBoot=Y

# SuperDisketteRead=(Y,N) Supervisor can read diskette
# Default is Y
SuperDisketteRead=Y

# SuperDisketteWrite=(Y,N) Supervisor can write diskette
# Default is Y
SuperDisketteWrite=Y

#####
# Installation and Updgrade Authentication Methods
#
#
#####
# Authentication Method Options are:
#
# AllowLocalUsersPasswordAccess
# AllowDomainUsersPasswordAccess
# AllowTokenAccess - ProtectDrive currently supports eToken Pro's
# that have been initialised as a Microsoft
# Windows logon token.
# SynchroniseLocalWindowsUserAccounts - by default ProtectDrive
# will add all members of the Windows local
# database to the ProtectDrive database
# during installation.
#
#
# If 'AllowLocalUsersPasswordAccess' is set to Y, users from
# the local machine may be added via the response file
# Default=Y
AllowLocalUsersPasswordAccess=Y

# If 'SynchroniseLocalWindowsUserAccounts' is set to Y, the local
# Windows users will be added to the ProtectDrive database during
# installation.
# Only valid if local password access is allowed.
# Default=N
SynchroniseLocalWindowsUserAccounts=N

# If 'SynchroniseLocalWindowsUserAccounts' is set to Y, existing
# local Windows users will need to use this password in the
# ProtectDrive preboot logon
# just for the first time. As soon as the user logs into Windows
# ProtectDrive will synchronise the ProtectDrive and Windows password
# to the Windows password.
# Only valid if local password access is allowed and
# 'SynchroniseLocalWindowsUserAccounts'
# is set to Y
# Default=password
# Minimum length is 6
LocalUserOneTimePrebootPassword=password

# If 'AllowDomainUsersPasswordAccess' is set to Y, users from
# the domain may be added via the response file or when logging
# into Windows.
# Default=Y
AllowDomainUsersPasswordAccess=Y

# If 'AllowTokenAccess' is set to Y, users from
# the domain's Active Directory may be added via the response file
# or user interface
# Default=N
AllowTokenAccess=N
```

```
#####
# Installation and Updgrade Pre-Boot Access Management
#####
#
# Pre-Boot Access Management options for password access are:
#
# AllowRemotePasswordRecovery - Domain or local password access must
be allowed
# AllowNewUserIntroduction - Domain or local password access must be
# allowed
# AllowPasswordFallback - Token Access must be allowed
#
# If 'AllowRemotePasswordRecovery' is set to Y, it will cause
# password recovery information to be generated by Protectdrive the
# first time a # user logs through into Windows.
# Only valid if local or domain password access is allowed.
# Default=N
AllowRemotePasswordRecovery=N

# If 'AllowNewUserIntroduction' is set to Y, it will cause
# password recovery information to be generated by Protectdrive
# during installation. This information will enable the new user
# introduction functionality.
# Only valid if local or domain password access is set.
# Default=N
AllowNewUserIntroduction=N

#
# Pre-Boot Access Management options for Token Access
#
# If 'AllowPasswordFallback' is set to Y, domain token users will be
# allowed to log on using a username, password and domain.
# This option is only valid if domain users are able to logon
# using a supported Microsoft Windows
# logon token.
# Default=N
AllowPasswordFallback=N

#####
# Default Disk/Port Permissions.
# These permissions are assigned to users when they are created.
# They can be re-assigned by User Manager, for local users, or
# Active Directory ProtectDrive snap-in for domain users.
# By default users have no disk or port permissions.
#####
DefaultDisketteBoot=N
DefaultDisketteRead=N
DefaultDisketteWrite=N
DefaultAccessCOM1=N
DefaultAccessCOM2=N
DefaultAccessCOM3=N
DefaultAccessCOM4=N
DefaultAccessLPT1=N
DefaultAccessLPT2=N
DefaultAccessLPT3=N

#####
# Users Setup - Token users will be added on Update.
#
#####
#
# Use this section to automatically add specific users to the
# ProtectDrive database.
#
# All users specified in this section are expected to be members of a
# Windows user database.#
#
#
# NOTE: If the password specified here is not the correct Windows
# password the user will need to use the password specified here to
# logon to ProtectDrive pre-boot. ProtectDrive will then update the
# users password with the Windows password when the user performs a
# Windows logon.
#
```

```
# The ProtectDrive permissions for users that have
# TokenUser set to Y will be specified on the domain server
# via the ProtectDrive snapin to the Active Directory Users
# and Computers application.
#
# NOTE: The number of TokenUsers plus the number of users
# in TokenGroups is limited to the maximum number of
# ProtectDrive users. Please consult the ProtectDrive user
# manual for this figure.
#
# To add users make a copy of the Example User and remove the # from
# the beginning of the line.
#

#
# All users default to :
#
#UserX.Name= INVALID NOTE: If name is not specified then user is
invalid
#UserX.TokenUser=N NOTE: If this is set to Y the remaining
fields are not required
#UserX.Password= NOTE: This does not have to be specified if the user
is a token user
#UserX.Domain= NOTE: If not specified, will default to the local
machine
#UserX.UseDefaultPermissions=Y NOTE: If Y, then the following
permissions will be ignored.
#UserX.DisketteBoot=N
#UserX.DisketteRead=N
#UserX.DisketteWrite=N
#UserX.AccessCOM1=N
#UserX.AccessCOM2=N
#UserX.AccessCOM3=N NOTE: Permissions will be ignored for domain
users
# as these will be taken from Active
Directory
#UserX.AccessCOM4=N
#UserX.AccessLPT1=N
#UserX.AccessLPT2=N
#UserX.AccessLPT3=N
#
#
#####
# Example User
#####

#
# User1 setup
#
#User1.Name=Local or Domain User
#User1.TokenUser=N
#User1.Password=password1
#User1.Domain=domain1
#User1.UseDefaultPermissions=Y
#User1.DisketteBoot=N
#User1.DisketteRead=N
#User1.DisketteWrite=N
#User1.AccessCOM1=N
#User1.AccessCOM2=N
#User1.AccessCOM3=N
#User1.AccessCOM4=N
#User1.AccessLPT1=N
#User1.AccessLPT2=N
#User1.AccessLPT3=N

#####
# Installation and Upgrade Token Groups Setup
#####
#
# This section allows all users that have a smart card logon
# certificate in a domain group to be added to ProtectDrive.
# The maximum number of groups that can be specified is 20. The
# maximum length of a group name is 256.
#
```

```
# The number of TokenUsers plus the number of users
# in TokenGroups is limited to the maximum number of
# ProtectDrive users. Please consult the ProtectDrive user
# manual for this figure.
#
# The permissions for these users will be specified on the domain
# server via the ProtectDrive snapin to the Active Directory
# Users and Computers program.
#
#
# To add group make a copy of a line below and remove the # from
# the beginning of the line.

#####
# Example Groups
#####

#
#TokenGroup1.Name=Domain Admins
#TokenGroup2.Name=Domain Users
#TokenGroup20.Name=Last Group
```

Crypdisk Response File

The response file is structured as an easy to understand unordered set of command/control strings that are parsed by the utility prior to operation.

A sample response file, CRYPDISK.RSP, is provided with ProtectDrive to instruct the system to carry out a non-interactive encryption. The sample response file should be edited as necessary when preparing for Network Installation.

For CRYPDISK.RSP to be used during an installation the DiskCryp_Auto field in the file must be set to Y

Sample Crypdisk File (This file is on the installation CD-ROM)

```
# DiskCryp_Auto=(Y,N)
# Perform Disk Encryption without prompting and disable all controls.
# e.g. non interactive mode
# Default is N
DiskCryp_Auto=N

# DiskCryp_EncryptionAlg=(3,4,10,11) Disk Encryption Algorithm
# 3 = DEA, 10 = IDEA, 11 = Triple DES
# Default is 11
DiskCryp_EncryptionAlg=11

# DiskCryp_Priority= (1,2,3)
# 1- low, 2=normal 3=high
# Sets the priority of the disk encryption.
# Default is 2.
DiskCryp_Priority=3

# Limited encryption wanted (System Areas Only)
# Default is N
DiskCryp_Limited=N

# Encrypt all possible drives. This option overrides
DiskCryp_EncryptDrives
# Default is N
DiskCryp_EncryptAll=N

# Encrypt specific drives. This option is overridden by
DiskCryp_EncryptAll
# Default is blank
# EG : To encrypt C:,D: and E: - DiskCryp_EncryptDrives=cde
DiskCryp_EncryptDrives=
```

Technical Support

If you encounter a problem while installing, registering or operating ProtectDrive, please make sure that you have read the relevant sections of this manual.

Should you still have problems that cannot be resolved, please contact Eracom support on the following numbers.

Within Australia: 1800 634 796
Outside Australia: + 61 7 5593 4796
email: support@eracom-tech.com

Before contacting Eracom support, please ensure that you have the following information available:

- Version of product
- Support certificate number

End of Document