

# PC/DACS for Windows 95

Version 4.2B

July 21, 1997

Please note that the information disclosed herein is confidential. The intent of this document is to inform Administrators of the new features and the enhanced functions of PC/DACS for Windows 95, version 4.2B. Users may be able to take the information in this document and use it to circumvent PC/DACS security.

This document is divided into three sections:

PERCEPTIBLE CHANGES  
COMPATIBILITY ISSUES  
INFORMATION SECTION

## PERCEPTIBLE CHANGES

This section describes areas of the product that differ in functionality from previous versions of PC/DACS for Windows 95.

### IMPORTANT NOTICE for Release 4.2B:

This version, 4.2B, is an upgrade to version 4.2. This release contains the following two changes for compatibility with new hardware and operating system software.

1. *File system corruption after installing PC/DACS on new PCs with Windows 95 OSR2*

This problem has been reported on the Compaq Armada 7000 Series and the HP Vectra XM4 that have Service Release 2 (OSR2) of Windows 95 installed. This version now supports these environments.

2. *Added support for PCs that use INT 13 Extensions (XE) for large hard drive access.*

Some newer PCs use the Western Digital standard "INT 13 Extensions" to access large hard drives. Previous versions of PC/DACS did not support this standard. When you enabled boot protection, you would get a "Boot Protection Integrity Error" message upon rebooting and the system would lock up.

Version 4.2B now supports this new standard; allowing boot protection and boot protection encryption.

### Logon:

#### *Support Network Group Policy Download*

Version 4.2 supports the downloading of system policies and profiles from the primary network provider, using Group Policy DLL (Grouppol.dll). Version 4.2 supports Group Policies using the following network clients:

Client for Microsoft Networks  
Novell Client 32 for Netware.

### *Improved Interaction with the defined Primary Network Provider.*

PC/DACS installs itself as the Primary Network Provider in order to be the first point of authentication during startup. Previous versions would treat the user's defined Primary Network Provider as a secondary authentication service. This caused certain attributes of a primary network provider to be ignored. The policy setting "Require Validation by Network for Windows Access" in the Local Computer Properties setting is one such primary network provider setting.

Version 4.2 will restore the defined primary network provider after the PC/DACS logon.

### **Boot Protection:**

*Boot Protection will not be Enabled if a WIF is Specified, but is Not Available*

If you specify a WIF as one of your External Unlock options, Boot Protection enablement will not proceed unless the WIF is available. Previous versions would allow boot protection to be enabled if a secondary External Unlock option was available (e.g., Firmware Password, Challenge/Response).

### *Single Step Boot Protection Can Be Done at the End of Product Installation*

Using site implementation procedures, Version 4.2 allows you to enable boot protection at the end of the PC/DACS installation without requiring a reboot before enabling boot protection. PC/DACS requires a VXD (BLKPROT.VXD) to be loaded and active before you can enable boot protection. With 4.2, you can use software distribution tools (SMS, network logon batch files,...) to download the boot protection VXD to workstations ahead of time; it can reside on the system by itself. Then, when you install PC/DACS, Setup will detect that Bklprot.vxd is active and allow you to enable boot protection at the end of installation.

### *Boot Protection Extends and Enhances the Lockdown of the Keyboard during Bootup*

When Boot Protection is enabled, PC/DACS will disable most keyboard input during the bootup process. This prevents users from using F5 & F8 key combinations to enter Safe mode. On certain computer systems, you could bypass the normal startup by repeatedly pressing F5 during boot up. Version 4.2 extends the lock down period to prevent this. It also makes additional keys available to allow you to use specific tools, such as the Compaq Diagnostic partition. You can use number keys, cursor keys, F10, ESC, and ENTER to allow you to access and navigate in the Diagnostic partition.

### **\$LOGOFF Has Expanded Rights**

If you do a new installation of PC/DACS version 4.2, the newly created security database will grant the \$LOGOFF user ID "Full System Access" rights in addition to "Full Configuration Access." This was done to prevent access control violations during the boot up process. This is especially useful for applications such as Microsoft Office/95 that launch programs before the PC/DACS Logon.

You can modify the access rights for \$LOGOFF using the Administration program if you wish to tailor the settings for your security standards.

### **Time Out Support for Hibernation Mode:**

The Time Out feature of Version 4.2 includes improved support for Hibernation Mode on Laptops. Previous versions would disable Time Out after you returned from Hibernation.

### **Migration Disk:**

The Migration Disk is not included in the standard disk set. The Migration Disk contains a utility to allow you to store PC/DACS for DOS security database settings in a temporary file and incorporate those settings into a PC/DACS for Windows 95 security database during installation.

The Migration Disk is still available upon request.

## **COMPATIBILITY ISSUES**

Utimaco Safeware has identified the following compatibility issues in the current release of PC/DACS for Windows 95.

### *Device-Drive Hard Drives Not Displaying in Boot Protection Encryption List Box*

In certain situations, the Standalone Administration program will not display a secondary hard drive in the drive list of the Boot Protection Encryption page of Global Security. One example is a software device-driven Adaptec SCSI secondary drive on a system with an IDE primary drive. If it does not display in the drive list, you cannot boot protect it.

In limited cases, it is possible to make a change to your Windows' configuration to allow you to see the drive in the list and then boot protect it. CALL UTIMACO SAFEWARE'S TECHNICAL SUPPORT DEPARTMENT BEFORE TRYING TO RECONFIGURE A HARD DRIVE AND ATTEMPT BOOT PROTECTION.

We strongly recommend that you back up that secondary drive before attempting boot protection. Due to the non-standard configuration, boot protection could make the drive inaccessible.

### *Norton Anti-Virus*

If you specify VOLUME Labels for floppy disks in the PC/DACS Manage Drives Table, do not use Norton Anti-Virus's "Check Floppies for Boot Viruses Upon Access" feature. This feature is in the Auto-Protect Advanced Settings Page. The PC/DACS Drive Table setting of DRIVE LETTER is the default.

## **INFORMATION SECTION**

This section describes functionality that has been added to PC/DACS for Windows 95, but that has not been included in the printed or on-line documentation.

1. Remote Administration
2. New Logon Procedure
3. Integrated Audit Report Generation
4. Boot Protection Enhancements
5. Resource Encryption Enhancements

## 6. Silent and Monitor Install Commands

### 1. Remote Administration

PC/DACS for Windows 95 version 4.2 contains a remote administration feature that allows other PC/DACS protected machines to be administered remotely using Windows 95 remote administration capabilities.

Remote administration uses remote file sharing to access the target PC's security database, and remote registry functionality to access the target PC's registry.

You must configure the following functionality to perform remote administration.

1. A local area network connection between the two machines.
  - 
  - 2. Both machines must use the same network protocol (i.e., IPX, Netbeui, TCP/IP).
  - 
  - 3. Microsoft Remote Registry service must be installed in the Network section of the Control Panel on both machines.
  - 
  - 4. User-level access control enabled in the Network section of the Control Panel on the target machine (in network control panel)
  - 
  - 5. Install Remote administration in the Password section of the Control Panel on the target machine and add the administrator's network user ID to the list of users allowed to administrate remotely.
  - 
  - 
  - 6. The PC/DACS administrator must be in the PC/DACS security database on the target machine. The administrative privileges granted to the administrator in the remote database will be in affect while administering the remote machine.

Remote administration is accessed using the "Open Machine" menu pick on the File pull-down menu in the Standalone Administratio program. Choosing "Open Machine" results in a select computer dialog. Enter the machine name of the PC/DACS protected machine (found in the "Computer name" field of the "Identification" page of the Network control panel) that you wish to administer. You may also choose browse to select from available machines. There is some delay between the selection of Browse and the display of the machine list dialog. Choose "Close Machine" on the "File" menu to close the remote machine connection and return to administering the local machine.

Note: You cannot administer boot protection remotely.

### 2. New Logon Procedure

The logon procedure has been modified to better integrate with the Windows' unified logon. With version 4.2, you will see the following changes:

1. *The PC/DACS Prompt for a Windows 95 ID and password has been removed.*

After you sign on to the PC/DACS Logon screen, Windows will prompt for a User Id and password. PC/DACS will store what you enter in the PC/DACS database for subsequent logons.

Whatever is in the PC/DACS database for the user's Windows ID and password are passed onto Windows. If the values are not defined then null strings are passed on. One of four things can occur at this point.

- If both the user ID and password are correct then the user will be logged onto that windows account.
- If only the user ID is valid then the logon will be displayed with the user ID field initialized.
- If there was no user ID then the standard Windows logon dialog will be displayed.
- If there was a user ID but it did not match an account then the account will be created in Windows and a password confirmation dialog will be displayed.

2. *Password changes now occur before the Windows logon.*

PC/DACS password changes will occur after the Last Logon Date and Time dialog box, but before the Windows logon.

3. *A password change menu item has been added to the PC/DACS tray icon.*

You can change your PC/DACS password by right-clicking the mouse on the DACSMENU icon in the system tray. Note that the menu item is grayed if the user does not have rights to change their password.

4. *PCDACS/Windows 95 password synchronization is only imposed during logon and after DACS password change.*

After the user has logged onto Windows the password is compared with their DACS password. If they are the same then synchronization is set. If they are not the same it is switched off. If the user changes their DACS password it is compared to the Windows password in the database. If they are the same then synchronization is switched on. However, if the user changes their Windows password there are no synchronization checks.

5. *Ability to Disable Logon Passthrough to Windows*

Version 4.2 provides the ability to disable the Windows 95' User ID passthrough during Logon. Normally, PC/DACS will send the Win95 ID and password that are stored in the User's Advanced Properties tab in the Administration program.

Do the following steps to disable the passthrough feature.

1. Select the User in the Administration program; select Edit **Properties**.
2. On the User Properties Dialog box, select the **Advanced** button and select the Win95 Tab.
3. Enter a tilde in the ID field. PC/DACS Logon will recognize this as a special ID and prevent the logon passthrough.
4. Enter any value for a password. This password will never be used.
5. Save your changes.

When you logon as that user, you will be prompted to provide a user id and password by Windows or the network provider, depending upon your Primary Logon configuration.

### **3. Integrated Audit Report Generation**

The audit report functionality is now integrated into the PC/DACS administration program. It is accessed through the File menu under "Audit Report". The "Reset Audit Log" menu selection is also found here.

### **4. Boot Protection Enhancements**

#### *1. Single-step install of Boot Protection.*

Boot protection (with or without encryption) may now be enabled at product installation time. This option is only available on "fresh" installs (not updates). The functionality allows you to boot protect and select a single type of encryption to be applied to all disks/drives. The actual boot protection process takes place following the re-boot and after logon, unless the BKLPROT.VXD driver is loaded and active.

You must logon as a user that has the "Enable Boot Protection" and the "Boot Protection Encryption" administration privilege.

#### *2. Boot Protection Now Supports Drive Partitions Setup with FAT32.*

OEM versions of Windows 95 include support for 32-bit File Allocation Tables (FATs) which allows Windows to support hard drivers larger than 2 Gig, and use smaller cluster sizes. This version of PC/DACS supports boot protection of 32-bit FAT hard drives.

#### *3. Real-Mode Drives Can Be Boot Protected and Encrypted in a Single Process.*

PC/DACS version 4.0 required that boot protection first be applied, the machine re-booted and then encryption applied on PCs with real-mode, INT 13 drives. Protected-mode drives could be boot protected and encrypted in a single process. This limitation has been removed in version 4.1, boot protection and encryption may be applied in a single step.

### **5. Resource Encryption Enhancements**

#### *1. Resource Encryption Supports Network Drives*

Resource encryption may now be applied to network drives locations that are mapped with a drive letter. To support resource encryption for a mapped network drive, the drive must be in the drive table (accessed using the "Drives" menu pick on the "Manage" menu) and have the "Resource Encryption Supported" check box selected.

#### Limitations:

PC/DACS does not support network drives accessed though universal naming convention.

#### *2. Resource Encryption Rules Can be Applied to Populated Directories*

Resource encryption may now be applied to and removed from directories that are not empty. Version 4.0 required that directories (or file specs) be empty prior to application of or removal of a resource encryption "rule". This is no longer true. To remove the product though, there must be

no resource encrypted directories or all resource encrypted directories must be empty. When creating or removing resource encrypted directories on a remote machine (using peer administration), PC/DACS will require that the directories be empty.

Resource encryption administration will prompt before encrypting/decrypting existing files when resource encryption rules are being added/removed. Most of the time administrators should select to encrypt/decrypt. An example of when to respond to not encrypt would be when adding a resource encryption rule for a shared directory on a network drive that already is being accessed by another PC/DACS protected machine and has files that are already encrypted.

## 6. Silent and Monitor Install Commands

In version 4.2, setup.exe has been enhanced to simplify the command line paths required to perform a silent or monitored install.

### **Silent Install:**

- a) Follow procedures for editing pcdacs.iss file in the "Getting Started Manual" and copy to PCDACS/95 Disk1.
- b) On Disk1 rename setup.exe to setups.exe
- c) Run setups.exe from Disk1 - make sure the pcdacs.iss file exists in the same directory as setups.exe or install will fail.

### **Monitored Install:**

- a) Follow procedures for editing pcdacs.iss file in the "Getting Started Manual" and copy to PCDACS/95 Disk1.
- b) On Disk1 rename setup.exe to setupm.exe
- c) Run setups.exe from Disk1 - make sure the pcdacs.iss file exists in the same directory as setupm.exe or install will fail.

## Logon and Password Synchronization

### *Synchronizing PC/DACS and Windows' Desktop Password*

The password change sequence for initial logon has been changed to allow you to synchronize your PC/DACS password with the Windows' desktop password. The initial logon, using the one-time password, will take the following steps.

1. Enter your PC/DACS User ID and initial password at the PC/DACS Logon Entry screen and click the Logon button to continue.
2. After you click on the OK button of the optional Last Logon message dialog box, you are prompted to enter a Windows 95 ID and password. The values you enter here are stored by PC/DACS.

PC/DACS will automatically send this ID and password to Windows when requested.

3. Windows will prompt you to confirm this password if this is a new desktop user ID. Reenter your Windows' password and click on OK to continue.

Depending upon your network configuration and current connections, you may be prompted to logon to the default network.

4. PC/DACS prompts you to change your initial password. Enter the same password that you used as your Windows' password in both fields and click on OK. If the password change is accepted by PC/DACS, the logon concludes and your desktop becomes available. If the new password is invalid, you will be prompted to reenter a new password.

If your PC/DACS password matches the Windows desktop password, PC/DACS will add PC/DACS to the Control Panel Password Synchronization field and your PC/DACS password will remain synchronized with the Windows' password.

#### *Current Limitations with Password Synchronization*

In order to synchronize passwords, you must use a Password Change setting of ALL or USER in the User Security Properties of PC/DACS. The SYSTEM and NONE settings, will prevent you from making a password change, which invalidate your password.

#### *Adding Lines of Text in User Address Fields*

To add additional lines of information in the Address field in User Information page of User Security, press the **CONTROL+ENTER** key combination.

#### *Trusted Application Feature is Designed for Windows' Use Only*

The Trusted Application feature only works with Windows' applications launched from the desktop. If you launch a defined trusted application from an MS-DOS box, that application is limited to the logged-on user's access rights.

## **Time Out**

#### *Advanced Power Management Support*

PC/DACS supports Advanced Power Management (APM) in Time Out. A suspend can occur in two ways: the standard energy save and the critical hardware type. If you, or the PC, effect a standard suspend, PC/DACS will trigger a time out before the suspend occurs. When you press the Suspend button, the PC will be timed out. If you effect a hardware suspend, PC/DACS will not time out the PC until after you resume. This can cause a situation where the desktop is briefly visible until Time Out gains control of the screen.

If you encounter compatibility problems with the Suspend/Resume support, you can disable it with the following registry setting:

**SRTIMEOUT** set to 0 (zero) in the key:  
**HKEY\_LOCAL\_MACHINE\Security/PCDACS/Configuration**

#### *PC/DACS Time Out Range Settings Override Windows' Control Panel Display Settings*

PC/DACS will synchronize the Windows' Screen Saver setting with the current PC/DACS user's time out time value. This allows the Windows' screen saver to run when the PC times out. If you set a Maximum Time Out Range value for a user that maximum value will override any changes that user can make to the Control Panel's Screen Saver setting. For example, although your



maximum Time Out setting is 20 minutes, you could change the Windows' value to 30 minutes in Control Panel, because PC/DACS cannot control the Windows' interface. However, PC/DACS will still enforce the 20 minute value and will reset that value when you next logon.

#### *Time Out in a Full Screen DOS Screen Can Cause Display Problems on Some Compaqs*

If PC/DACS times out while your computer is in a full screen MS-DOS window, the video display may be garbled when you relogon to the Time Out dialog box. This was noticed on a Compaq Deskpro with 256 color display set. You can press ALT+TAB twice (to toggle sessions) to restore the display.

## **Trusted Applications**

#### *Trusted Applications on Network Drives Must be Run Through a Mapped Drive Letter*

If you create a trusted application that resides on a network drive, you must launch that application by way of a mapped drive letter. To do this, run My Computer and map a drive letter to the location of the trusted application, then run the application.

Network Neighborhood uses Universal Naming Convention (UNC) filenames which the trusted application feature does not recognize. Trusted applications run from Network Neighborhood retain the logged-on user's access rights.

## **Windows 95 Related Issues**

#### *Single Mode MS-DOS Sessions*

PC/DACS creates a registry entry during installation to disable the single-mode MS-DOS option on the Shutdown menu. The setting is called NoRealMode=00000 and it is located in the key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp.

If you remove PC/DACS, this setting is still in effect, unless you enabled the single-mode MS-DOS value in the Manage Features dialog box. In this case, you can use Regedit or Poedit to restore the setting if you wish.

#### *Restrict User Access to REGEDIT to Increase Security*

PC/DACS does not put restrictions on a user's ability to change Registry settings with the exception of PC/DACS entries. While this prevents users from bypassing PC/DACS, misuse of Regedit could cause other system problems. Depending upon your security and systems management needs, you may want to use Windows' profiles and policies to restrict user's ability to use Regedit.

#### *Saving a Boot Protection WIF File to a Resource Encrypted Floppy Makes the WIF Unusable.*

If you specify Drive A:\ as a Resource Encrypted drive and use that drive as the location for creating a WIF file while enabling boot protection, the WIF file gets encrypted, making it unusable.

### *Disallowing Resource Encryption Passthrough Does Not Work in an MS-DOS Box*

The User Security setting to disallow Resource Encryption passthrough does not work inside of an MS-DOS box.

### *A Volume Label Must Exist for Drives Specified By Volume Label in the Manage Drives Table*

If you set a drive to use a Volume Label for Pathnames in Manage Drives screen, you must ensure that those drives actually have volume names assigned.

### *Printer Port Access is Tied to the Windows Session, Not the PC/DACS Logon Session*

Local Printer port access is tied to Windows' SPOOL32 which stays in effect while Windows is running. The problem is due to the inherent single-user, unsecured nature of Windows 95. SPOOL32 is started as needed (the first time anyone starts a print job) and remains running until the machine is shutdown. SPOOL32 is associated with the initial user's security credentials when it is started. This remains in place for the life of SPOOL32 and is what makes background print jobs possible (regardless of the security credentials of the foreground user). If one PC/DACS user logs on to the workstation with LPTx port access, and begins a print job, subsequent PC/DACS users who logon will also be able to print to that port, even if their Access Control settings deny LPT port access.

This only applies to LPTx port access. COMx port access is tied to the current user.

### *Workgroup File Sharing with PC/DACS Uses Shared Drive's Access Control*

Only Administrators, or users with the Full System Access attribute (FSA) enabled are allowed to set up file sharing on a PC/DACS-protected PC. However, once a Share is setup, it stays in effect, even if the administrator logs off and a User with limited access rights logs on afterwards. In this case, a remote user who attaches to the shared drive has full access to the shared drive, while the local logged-on user has limited access. This allows network administrators the ability to configure remote administration capabilities while preventing workstation users from accessing resources needed for remote administration.

### *PC/DACS Accepts Leading and Trailing Spaces in Password*

Windows 95 allows leading and trailing spaces as well as only spaces in desktop passwords. PC/DACS for Windows 95 has added this functionality to PC/DACS passwords in order to allow password synchronization between PC/DACS and Windows 95.

The space character has been grouped among the "special" characters for Password Restrictions in Organizational Security.

Boot Protection's Firmware Unlock is also case-sensitive.

=====END OF README.TXT=====

Utimaco Safeware, Inc.

7 Waterside Crossing  
Windsor, CT 06095

860-688-4454