ProtectDrive 8.4.1
Release Notes

Version: 8.4.1, Build 03
Release Notes Issue Date: July 1, 2008
Updated:

Product Description

ProtectDrive is hard disk encryption software for securing sensitive data. ProtectDrive provides pre-boot authentication, and once installed, it can be configured to encrypt and decrypt data transparently. The pre-boot feature prevents unauthorized users from gaining access to the operating system and sensitive information. ProtectDrive is ideally suited for large scale enterprise deployment as it offers centralized management for token, smart card and password users. For maximized protection, the encryption of removable media such as USB thumb drives is also supported.

Version Summary

This is a feature and maintenance release.

Scope

This version is released for general distribution. Please see **Advisory Notes** and **Known Issues and Workarounds** for limitations and restrictions.

GA	LGA
√	

Release Description

New Features and Enhancements

- **Entrust certificate support**— Standard Microsoft PKI functionality has been expanded to include support for Entrust certificates for authentication and access. This has been implemented in a generic manner, referred to as “Allowed Certificate Usages,”’ to add much greater flexibility with certificates.
- **Borderless security compression support**—Borderless security compression support allows for compressed certificates on SafeNet 330 smart cards. ProtectDrive will now also cater to multiple certificates on a smart card or token.
- **SafeNet 330 G3 support**—SafeNet 330 G3 smart cards are now supported at ProtectDrive pre-boot authentication (with and without compression).
- **Precise biometric keyboard reader support**—Precise biometric 200 MC and 250 MC keyboard readers can be used for ProtectDrive pre-boot authentication. Note that this support is based on the card reader.
- **Token auto pre-boot support (including iKey 1000)**—ProtectDrive can be configured to allow for auto pre-boot authentication with smart cards and tokens. The support will handle sudden power loss and will include iKey 1000 tokens.

Released Components

ProtectDrive for Windows 2000/XP/Server 2003/Vista:

Supported Platforms for Client Management (on Server)

- Windows 2003 Server, Service Pack 2

Supported Platforms for Client

- Windows 2000 Professional, Service Pack 4
- Windows 2000 Advanced Server, Service Pack 4
- Windows Server 2003, Service Pack 2
- Windows Server 2003 R2, Service Pack 2
- Windows XP Home, Service Pack 3
- Windows XP Professional, Service Pack 3
- Windows Vista 32-bit editions, Service Pack 1

Advisory Notes

- Virus protection software may cause the ProtectDrive installation to fail. It has been observed that this is due to the quarantining of files in the *C:\SECURDSK* folder by the AVS. If this occurs, disable virus protection for the duration of the ProtectDrive installation.

- It is strongly recommended that all machines upgrading to the current version of ProtectDrive run "chkdsk /f" and "Windows Defrag" before upgrading from a previous version.

- It has been observed that BIOS legacy USB support for USB keyboards and mice on some computers interferes with the ProtectDrive USB stack, and can prevent two-factor authentication from completing successfully. If this occurs, disable the legacy port for USB keyboards and mice in the BIOS.

Smart Card / Token Support

ProtectDrive uses smart cards and tokens to provide two-factor authentication prior to operating system startup. Most CCID-compliant smart card readers should work with ProtectDrive. Some of these include (but are not limited to):

- SafeNet DKR 630 – GemPC430
- SafeNet DKR 631 – GemPC USB
- SafeNet DKR731 - OmniKey CardMan 3121 (max 1024 bits)
- SafeNet DKR830 – SCR 331
- Precise 200MC Bio Keyboard (no Biometric support at PBA, integrated smart card only)
- Precise 250MC Bio Keyboard (no Biometric support at PBA, integrated smart card only)

The table shown below provides an overview of tokens and smart cards supported by this ProtectDrive release.

Model	Information
SafeNet Borderless Security Smart Card 330 – FIPS, Non FIPS, and G3	**SafeNet CIP Utilities** G3 cards - BSEC 7.1.0_6 Else – BSEC 7.0.0_9 1024 and 2048 bit RSA keys supported
SafeNet Borderless Security iKey™ 2032	**SafeNet CIP Utilities** BSEC 7.0.0_9 1024 and 2048 bit RSA keys supported
SafeNet Borderless Security iKey™ 1000 and 1032	**N/A**
Aladdin eToken Pro 16k, 32k, 64k and NG-OTP	**Cryptographic Provider** RTE 3.65 (4.5 for Vista) 1024-bit RSA keys supported
Aladdin Smart card 4.2	**Cryptographic Provider** RTE 3.65 (4.5 for Vista) 2048-bit RSA keys support dependant on reader capabilities
Siemens CardOS v4.3b	**Siemens AG** HiPath SIcurity Card API V3.0 B
RSA SecurId 5100	**RSA Authenticator Utility**
Other supported smart cards include: Axalto Access Schlumberger Access Oberarthur Gemplus Gemalto Nexus	

Removable Device Support

Efforts have been made so that ProtectDrive is compatible with all removable media. However, some third-party removable media security software will interfere with ProtectDrive, and in most of these cases, is not recommended. Most version 1.0 and 2.0 USB removable devices and USB hard drives should be compatible with ProtectDrive.

Resolved Issues

Severity	Classification	Definition
C	Critical	No reasonable workaround exists
H	High	Reasonable workaround exists
M	Medium	Medium level priority problems
L	Low	Lowest level priority problems

Issues Resolved in this Release

Issue	Severity	Synopsis
37350	H	Upgrades of ProtectDrive from an encrypted Windows 2000 FAT32 partition will now work
39724 39821 39825	H	Various enhancements for the use of ProtectDrive via RDP – installation, RM settings, client licensing
39730	H	Improved implementation of installs with a valid authorization code
41489	H	Nonpaged pool empty Event 2019 errors (reported by NationWide).
38603 38926 39591	L H M	More efficient handling of ProtectDrive upgrades
31457	M	Improved support for msi install variables
36674	M	More consistent handling of shared key account removal
37013 40086	M	More accurate LMC reporting of drive status
37044	M	Removed a duplicate entry from the Application Event Log when a partially encrypted partition is modified to remove encryption
37719	M	Enhanced support for ‘msiexec’ installs with the ‘/a’ argument
39632	M	Better handling after an incorrect smart card login attempt
41626	M	ProtectDrive logon processing: Users which are neither found nor added are not provided with default device privileges.
38834	L	Improved messaging with the Certificate Wizard on Vista
39289	L	Enhanced usability with Certificate Wizard regarding default file location within a Cert Wizard session

Known Issues and Workarounds in this Release

Issue	Severity	Synopsis
40488	H	**Summary:** Incompatibility with Wave security software **Workaround:** Uninstall Wave software before installing ProtectDrive.
40979	H	**Summary:** Possible problem with updating groups to the client **Workaround**: Ensure there is at least one user included in PD Users.
41134	H	**Summary:** Updating a group to a client in an ADAM environment **Workaround:** Use AD environment or add users individually.
41823	H	**Summary:** Icons in Active Directory Users and Computers disappear **Workaround:** Load Service Pack 2 for Microsoft Windows 2003 Server.
40127	L	**Summary**: Some examples of the Ativa brand of removable media are not supported **Workaround:** Use another brand.
40280	L	**Summary**: Cannot install ProtectDrive after ProtectDrive Admin Tools have been installed on a server **Workaround:** Uninstall ProtectDrive Admin Tools and perform a custom reinstall incorporating Client and Admin Tools.

Known Issues and Workarounds from Previous Releases

Issue	Synopsis
9735	**Summary**: Use of the '/e' option with 'decdisk' when using a bootable USB thumb drive **Workaround:** Copy decdisk and recovery file/s to bootable floppy if the decdisk '/e' option is necessary.
39628	**Summary**: USB card readers do not respond to all ports in a Dell D820 **Workaround:** Use one of the other USB ports**.**
39577	**Summary**: Addition of local "Users" group to ProtectDrive **Workaround:** If the addition of a local users group is encountered then add the local users individually.
39576	**Summary**: Dell USB Smart Card Reader Keyboard issues on D620 and D820. **Workaround:** Use the internal reader or USB reader for ProtectDrive pre-boot authentication if needed.
39569	**Summary**: With some Vista hardware combinations Smart Card SSO may fail with "No valid certificates found" message **Workaround:** Re-insert the smart card. If that fails, then re-insert it again.
39379	**Summary**: ProtectDrive PCMCIA support may be lacking with machines with internal card readers **Workaround:** Use the internal reader or a USB reader.
39291	**Summary**: If problems are encountered removing ProtectDrive after a decdisk with recovery files **Workaround:** Decrypt all drives with decdisk. Boot to Safe Mode. Delete the *HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\GinaDLL* registry entry. Run 'services.msc' and disable Client Data Manager and Storage Encryption Service. Reboot normally. Uninstall ProtectDrive by running *'msiexec /x safenetprotectdrive.msi ERA_AUTO_UNINST=Y'*.
39241	**Summary**: Support for encrypted RM formatted with exFAT file system **Workaround:** Format the RM with another file system.
39086	**Summary**: PCMCIA readers may return error if smart card is queried after short interval of time **Workaround:** Pause before querying the card or remove, reinsert and pause.
38998	**Summary**: Recovering the ProtectDrive mbr with 'rmbr' from a USB thumb drive after running 'fdisk /mbr' **Workaround:** Run 'rmbr' from a boot floppy or CD.
38968	**Summary**: Windows format prompt with Vista for encrypted RM **Workaround:** On some systems, inserting encrypted removable media may result in a prompt to format the device. This prompt can be safely ignored and the device unlocked as usual.
38912	**Summary**: Systems with C: on Disk1 **Workaround:** Ensure the C: drive is on Disk0.

Issue	Synopsis
38906	**Summary**: decdisk with recovery files for non-system partition **Workaround:** Remove the *HKLM\SYSTEM\CurrentControlSet\Servers\e_dasdf$\parameters\SBlkRba* registry entry, then reboot, or uninstall immediately by running the ProtectDrive msi with the parameter ERA_AUTO_UNINST=Y.
38764	**Summary**: Vista system restore points created during encryption process **Workaround:** Do not create Vista restore points during encryption.
37433	**Summary**: A newly created Configuration Object in the ProtectDrive Management Console may not show in the Config Management tab (within PD Settings tab) of an ADUC computer object **Workaround:** Close and reopen PD Management Console to force a refresh.
37363	**Summary**: ProtectDrive pre-boot authentication with a DKR 731 and 2048 bit certificates on DK 330 smart card **Workaround:** ProtectDrive does not support 2048 bit certs with the DKR 731 - use another reader or smaller cert size.
37217	**Summary**: Vista - Storage Encryption Service error may be in the event log after PD is installed **Workaround:** This error message can be ignored.
37054	**Summary**: Vista - Switching RM after encryption and decryption to another Vista machine may prompt for hardware scan **Workaround:** It is safe to ignore the prompt.
36838	**Summary**: Removal of the last user from ProtectDrive Users' list even if pre-boot authentication is deactivated **Workaround:** Leave at least one user in the PD database.
36829	**Summary**: Release of a USB session at pre-boot to use another token **Workaround:** Reboot with another token inserted if problems are encountered.
36790	**Summary**: Hardware installation wizard may show an error when installing USB RM storage drivers **Workaround:** Device still works as expected.
36715	**Summary**: Windows may not recognize RM's Volume label if the ProtectDrive 'Lock media' process is applied **Workaround:** RM will still work as expected.
36666	**Summary**: Central Config Management: Dynamic updates on Management Console **Workaround:** Close and reopen the server Management Console to ensure latest updates.
36627	**Summary**: An event log entry relating to “Storage Encryption Service” may show when encryption/decryption of hard drive finishes with the user logged off’ **Workaround:** It is safe to ignore this entry but it will be avoided by not logging off during encryption/decryption.
36618	**Summary**: Remote logon may have problems with LMC while RM is inserted **Workaround:** Safely remove RM and reboot the system.

Issue	Synopsis
36525	**Summary**: Running "rmbr.exe" in Windows Vista **Workaround:** 'rmbr' is a 16-bit utility which can display an error if run in a 32 bit Vista environment. This has no impact on the 32 bit environment.
36498	**Summary**: Vista - ProtectDrive system tray icon does not have a right click 'Lock computer' menu item **Workaround:** Press Ctrl+Alt+Del and lock the machine.
36497	**Summary**: After login, pressing Ctrl+Alt+Del to access task manager while the Protect Drive Info Dialog Box is open may cause user to log off **Workaround:** Close ProtectDrive Info Dialog Box before pressing Ctrl+Alt+Del.
36468	**Summary:** Manage a parent domain from a child domain in Management Console **Workaround:** None. ProtectDrive does not support management across domain boundaries.
36405	**Summary:** Management Console and special characters (e.g. ",") **Workaround:** Avoid special characters in Configuration Object names.
35887	**Summary:** Changing ProtectDrive "Device Control" permissions **Workaround:** A reboot may be required for changes to "Device Control" to take affect.
35885	**Summary:** Enabling (disabling) ProtectDrive system tray icon **Workaround:** Logoff and re-login.
35693	**Summary:** Single SignOn functionality after resuming from hibernation **Workaround:** Go to **Control Panel > Power Options Properties > Advanced**. De-select the **Prompt for password when computer resumes from standby** check box.
35603	**Summary:** RM encryption continuance after resumption from sleep or hibernation **Workaround:** Do not allow machine to sleep or hibernate until RM encrypt/decrypt is complete OR reboot machine.
34446	**Summary:** PD may not appear in the 'Add Remove programs' on Vista systems **Workaround:** This is a Microsoft issue and occurs with many programs on Vista. To remove PD, the MSI installer can be rerun and then navigate to 'Remove'.
35320	**Summary:** Pre-boot Authentication (PBA) process may hang with certain USB devices plugged in directly to some laptops (non-docked). The problem does not exist if the USB devices are plugged in directly to the Docking Station. Most common failures: iPods, BlackBerrys, Removable Media, other power drawing/rechargeable USB devices, and some USB keyboard and USB mouse combinations. Below is a list of several individual workarounds that may remedy the issue. **Workarounds:** * Disconnect common problematic USB device(s). * Plug the USB device(s) into a docking station only. * Insert the USB device(s) into a different USB port. * Adjust the USB emulation on/off setting in the computer BIOS.
32768	**Summary:** Local Management Console (LMC) does not reflect removable media correctly with dynamic updates. **Workaround:** Close LMC and the reopen it to get the updated status.

Issue	Synopsis
32720	**Summary:** The default password can be entered with more than the Pre-boot Authentication maximum password length (20 characters). **Workaround:** Use passwords less than or equal 20 characters.
33487	**Summary:** CAC not working with the Dell D620 internal reader if USB 2.0 enabled in BIOS.
32585	**Summary:** No support for CD and DVD as Removable Media (RM).
32353	**Summary:** German: Pre-boot unable to enter the (Alt-GR +3) at pre-boot.
32176	**Summary:** Japanese: Shared Key registration attempt errors have invalid characters.
35029	**Summary:** Dell USB Smart card Reader Keyboard works for smart card logon, but it fails to work as keyboard right after PBA (with USB mouse present).
29660	**Summary:** Windows 2000: Smart card/eToken removal doesn't lock the workstation after token SSO. **Workaround:** The user can manually lock the computer via **Ctrl-Alt-Del**.
29340	**Summary:** DKR731 reader fails on PBA decryption for Siemens cards with 2048-bit certificates. **Workaround:** Use another reader, card, or a smaller certificate size.
29089	**Summary:** Pressing **Ctrl-Alt-Dell** when the PD Logon Information Window appears on the screen logs off the user. **Workaround**: Press **OK** after the PD Info window appears before pressing **Ctrl-Alt-Del**
--	**Summary**: Single Sign-On in conjunction with Novell GINA logon is not supported.
21095	**Summary**: XP Pro 64-bit installations fail: "Unsupported OS version." **Workaround:** None. 64-bit installations are NOT supported at this time.
25402	**Summary**: Single Sign-On does not work on a Windows Server 2003 system when a smart card or token has been used for PBA.
25654	**Summary:** ProtectDrive removable media issues on systems running Norton Ghost version 10.0—No ProtectDrive prompt to encrypt or unlock removable devices.
25657	**Summary:** The number of users and certificates are not updated on-the-fly in the **PD Users** tab when users are removed. **Workaround:** Close and reopen the Local Management Console to fix the issue.
25297	**Summary:** While the “prompt to encrypt” message is shown, if the user attempts to access their removable media as they would without ProtectDrive, an "Access is denied" message displays. The setting for **Deny access to non-encrypted media** was not selected, so the removable media should have been accessible. **Workaround:** On the “prompt to encrypt” screen, choose the **Do Not Encrypt** option before attempting to access the removable media.

Publications

The publications associated with this release are:

- *ProtectDrive Administration Guide*, 007054-001 (Rev D, May 2008)
- *ProtectDrive User Manual*, 007053-001 (Rev D, May 2008)