Dell Data Protection | Personal Edition

Technical Advisories v8.12

Legend

⚠ | CAUTION: **A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

⚠ | WARNING: **A WARNING icon indicates a potential for property damage, personal injury, or death.**

ⓘ | IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: **An information icon indicates supporting information.**

Personal Edition Technical Advisories

2017 - 02

Rev. A01

Contents

Technical Advisories

To ensure the security of your confidential data, Personal Edition encrypts the data on your Microsoft Windows computer. You (or authorized users) can always access the data when logged into the computer, but unauthorized users will not have access to this protected data. Data always remains encrypted on the drive, but because our encryption is designed to be transparent to you, there is no need to change the way you work with applications and data.

Contact Dell ProSupport

Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell Data Protection product.

Additionally, online support for Dell Data Protection products is available at dell.com/support. Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

Be sure to help us quickly connect you to the right technical expert by having your Service Code available when you call.

For phone numbers outside of the United States, check Dell ProSupport International Phone Numbers.

New Features and Functionality v8.12

- A standalone version of Encrypt for Sharing, Encrypt4Share.exe, is now added to the <installation folder>\Dell Data Protection \Encryption folder at installation and can be accessed from the Windows Start menu.

Resolved Technical Advisories v8.12

All Products

- Very long installation times no longer occur on Windows 7, due to removal of Windows KB2913763 from the installer. If KB2913763 is not yet installed on the computer, install it then reboot before installing Personal Edition. For more information, see https://support.microsoft.com/en-us/kb/2913763. [DDPC-4257, DDPC-1619, CSF-847]

Encryption

- On Windows 10, the Encryption icon now displays as expected on encrypted files in File Explorer. [DDPC-1186, DDPC-2817, DDPMTR-1864]
- Debug-level logging is improved. [DDPC-2307]
- Upgrade to Windows 10 now proceeds as expected when the installation media is stored in a folder that is encrypted with the User or Common key. [DDPC-4146]
- The Secure Windows Hibernation File and Prevent Unsecured Hibernation policies are now enforced after upgrade. [DDPC-4786]
- The WSScan **Unencrypted file in Violation** option now initiates a sweep of unencrypted files as expected, without the files having to be selected or accessed. [DDPC-4790]
- An issue is resolved that resulted in Windows Update failures with Office and Windows 10 feature updates. [DDPSUS-1323]

Resolved Customer Issues

- An issue is resolved that resulted in a long delay after pressing **Ctrl+Alt+Del** on a computer running Dell Desktop Authority. [DDPC-500]
- An issue is resolved that resulted in multiple restart prompts. [DDPC-4484, DDPC-4535]

Advanced Authentication

- The Enroll Credentials window no longer occasionally displays after a computer with fingerprint or smart card enrolled credentials resumes from sleep. [DDPC-4269]

Technical Advisories v8.12

Encryption

- To display advanced properties PDAID, Length, and Tag on the **Properties** > **Encryption tab** of an encrypted file, add the following registry setting:

  ```
  [HKEY_LOCAL_MACHINE\SYSTEMCurrentControlSet\ServicesCmgShieldFFE]

  "CredDBCEFAllowProcessList"=explorer.exe,explorer.ex,explorer.e,explorer.,explorer,explore,explor,dllhost.exe,dllhost.ex,dllhost.e,dllhost,dllhost
  ```

  [DDPC-4185]
- If Personal Edition is uninstalled before activation, an error message displays: "EmbeddedServer service is in a pending delete state. error 0z430." To work around this issue, before uninstalling, allow the client to activate and then restart the computer before beginning uninstallation. [DDPC-4886]
- When encryption or decryption is paused, the Compliance/Provisioning status may not be accurately indicated in the Local Management Console. [DDPC-5063]

Resolved Technical Advisories v8.11

Encryption

- An issue is resolved that resulted in the Local Management Console appearing unresponsive while the Encryption client performed tasks in the background. [DDPC-2769]
- The WSScan user interface now opens to the option of Unencrypted Files, as expected, when commands `-ua-`, `-ua`, and `-uav` are used to launch the user interface. [DDPC-3473]
- An issue is resolved that caused the Shield service to occasionally crash when the user logged out. [DDPC-3939]

Resolved Customer Issues

- An issue is resolved that resulted in the user's temporary inability to access User and Common encrypted files due to a timeout in communication with the Shield service. [DDPC-2230, DDPC-3486, DDPC-4134]
- Sparse files are no longer populated during encryption and decryption sweeps. [DDPC-3201]
- WSScan now functions as expected when processing file names longer than 260 characters. [DDPC-3928]

Technical Advisories v8.11

Encryption

- Cumulative encryption exclusions are now automatically applied when the Encryption client is upgraded. This will require an encryption sweep for each user upgraded to v8.11 or later. However, subsequent updates will require a sweep only if the update includes new exclusions. [DDPC-1334, DDPC-5138]
- Activation fails after attempting to roll back an External Media Edition upgrade. [DDPC-4449]
- In some cases, an encryption sweep pauses and the Local Management Console continues to display "Compliance in progress...." To restart encryption, copy WSProbe from the installation media, and run it: at the command line, enter `wsprobe`. [DDPC-4499]
- The user receives an access denied error when attempting to access removable media, although policy is set to allow full access to unShielded media. [DDPC-4523]
- After upgrade to Windows 10 Fall Update using WSProbe -E on a computer with Hardware Crypto Accelerator, during re-encryption with WSProbe -R, the Local Management Console freezes and a message displays regarding HCA key backup and provisioning. [DDPC-4645]
- The WSScan Unencrypted Files in Violation option to list Unencrypted Files option does not indicate that the files in violation should be encrypted. Using a previous version of WSScan will properly show these files. [DDPC-4790]
- Amended 2/2017 - Due to hibernation changes introduced in the Windows 10 Anniversary Update, computers will no longer be able to resume from hibernation when the Secure Windows Hibernation File policy is enforced. If you rely on secure hibernation, Dell recommends that you not upgrade to Anniversary Update at this time. This issue will be fixed in a future release. [DDPSUS-1346]

Advanced Authentication

- When dual authentication is configured for a user, but one of the authentication options is not yet enrolled, the icon for the unenrolled option does not display on the user's logon screen. [DDPC-4690]

New Features and Functionality v8.10.1

- The Encryption client now supports Microsoft Windows 10 Anniversary Update (Redstone release).
- Customers upgrading to Windows 10 from an earlier version of Windows OS are no longer required to decrypt and re-encrypt data at OS update.
- The Encryption client now supports Audit Mode. Audit Mode allows administrators to deploy the Encryption client as part of the corporate image, rather than using a third-party SCCM or similar solutions to deploy the Encryption client. To suppress activation until deployment is complete, install the Encryption client and perform the necessary restart when the configuration computer is in Audit Mode.
- The Encryption client is now supported with TPM 2.0.

Resolved Technical Advisories v8.10.1

Encryption

- On computers running Windows 10 Education Edition, log files are now stored in \ProgramData\Dell\Dell Data Protection\Encryption as expected, rather than in \ProgramData\Application Data\Dell\Dell\Data Protection\Encryption\. [DDPC-2651]
- An issue that caused the computer to very rarely become unresponsive when renaming a file has been resolved. [DDPC-3086]
- An issue that caused a prompt to reboot in some cases with SDE encryption enabled is resolved. [DDPC-3525]
- UEFI computers with Secure Boot enabled now boot as expected after Microsoft Security Bulletin MS16-100 is applied. [DDPC-4032]
- Added 12/2016 - Hardening against credential update failures within the Encryption client is now enabled by default. [DDPC-936]

Technical Advisories v8.10.1

Encryption

- After upgrade to Windows 10, a second restart may be required for encryption to resume. [DDPC-4080]
- When migrating from one edition of Windows to a different edition during a Windows 10 upgrade, the Encryption client is not migrated. The same issue occurs if either the option to keep only personal files or to keep nothing is selected during a Windows 10 upgrade. To resolve this issue, reinstall the Encryption client after upgrade. [DDPC-4191]
- When WSProbe -z is run to prepare for the Windows 10 Anniversary Update on a computer with Dell Data Protection-encrypted data, an error may display that says an encryption sweep could not be stopped. To work around this issue, restart the computer and then re-run WSProbe -z. [DDPC-4254]
- If an encryption sweep is in progress when upgrade is started, the progress bar does not advance in the installer dialog and the length of upgrade may be extended. [DDPC-4261]
- Direct upgrade from v8.5.1 and earlier on 32-bit operating systems is not supported. To work around this issue, uninstall the previous version then install the latest version. [DDPC-4268]
- Aventail Access Manager is not supported with the Encryption client on Windows 10 computers. [DDPC-4335]

New Features and Functionality v8.10

- The Windows USB selective suspend feature is now supported.
- Beginning with v8.9.3, Dell Data Protection | Hardware Crypto Accelerator is not supported. Installation and upgrade do not proceed if Hardware Crypto Accelerator is detected and the computer is disk encrypted with it. In cases where Hardware Crypto Accelerator is installed but the computer is not disk not encrypted with it, upgrade will proceed. However, Hardware Crypto Accelerator will be ignored. The last Personal Edition client version to support Hardware Crypto Accelerator functionality is v8.9.1. Support for v8.9.1 will continue through April 8, 2020.

Resolved Technical Advisories v8.10

Encryption

- Installer logging of launch conditions is improved. [DDPC-918]
- An issue that resulted in a computer occasionally becoming unresponsive after reboot is now resolved. [DDPC-1255]
- The Encryption Removal Agent no longer crashes during decryption of HCA- or SDE-encrypted files if the key bundle is missing or inaccessible to the Agent. Instead, a message displays that files could not be decrypted. [DDPC-1359]
- An issue that caused the Shield Service to crash is now resolved. [DDPC-2189]
- An issue that led to unresponsiveness after restarting a Windows 10 computer running Advanced Threat Protection is now resolved. [DDPC-2336]
- An issue that caused a restart and lock at the Windows startup screen on Windows 7 computers running Bitdefender Antivirus is resolved. [DDPC-2561, DDPSUS-842]
- Default SDE Encryption Rules have been refreshed. [DDPC-2689]
- SDE encryption now proceeds on computers with HCA or a SED, and a log entry stating SDE policies are blocked due to FVE or a SED disk no longer displays. SDE Encryption is now enabled by default in new installations and upgrades, based on the registry entry HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMgShield\AlwaysApplySDE set to "1." [DDPC-3273]
- Encryption handling of files that are always in use is improved. [DDPC-3331, DDPC-3333, DDPC-3334]
- Additional data is now provided to Dell Data Protection Server for endpoint status reporting. [DDPC-3332, DDPC-3335]
- Users with common access card authentication can now successfully activate Personal Edition. [DDPSUS-807]
- Windows logon with a smart card now proceeds as expected. [DDPSUS-855]
- Encryption sweep performance is improved on Windows 10 computers running Sophos. [DDPSUS-866]
- An issue that led to an error when EnCase attempted to access encrypted files is resolved. [DDPSUS-923]
- An issue that resulted in occasional computer unresponsiveness after installation but before activation is resolved. [DDPSUS-1037]

- An issue that led to multiple restarts is now resolved. [DDPSUS-1087]

Advanced Authentication

- On Dell Latitude 3450 and 3550 computers running Windows 10, fingerprint authentication now proceeds as expected. [DDPC-1598/ CSF-772]
- After restoring credentials in Password Manager, a second authentication prompt no longer displays. [DDPC-1617]
- Password Manager logon now functions as expected with Dell Remote Management Console logon. [DDPC-2356]
- Occasionally after the computer hibernates or restarts, enrolled fingerprints must be re-enrolled. [DDPC-2812]

Technical Advisories v8.10

Encryption

- Standard practice is that the master installer version is the same version number as the Encryption client installer. However, in this release, the master installer is v8.10 and the Encryption installer is v8.9.3. Versions will be aligned in the future, to avoid confusion. In the event that you need support, ProSupport will need your **Encryption client** version number.
- Setup and activation are not completed for a roaming profile user. [DDPC-2604]
- To upgrade with HCA-encrypted data, issue a policy of Hardware Crypto Accelerator (HCA) = Off. After data is unencrypted, issue a policy of Policy-Based Encryption = On. Then run the v8.10/v8.9.3 installation. [DDPC-2608]
- Added 09/2016 - In the rare case that a user with smart card authentication becomes deactivated, smart card authentication succeeds for the first logon after restart for each user but fails on subsequent smart card logon attempts until at least one user restarts the computer. [DDPC-2721]
- After a computer crash or forced shutdown, encrypted files occasionally become unavailable. To work around this issue, run WSDeactivate then reactivate the Encryption client. [DDPC-3228]
- With Kaspersky Small Office Security installed, the Encryption client fails to activate. To work around this issue uninstall Kaspersky Small Office Security. [DDPC-3388]

Preboot Authentication

- Added 09/2016 - When PBA is activated on a Windows 7 computer without Microsoft Security Advisory 3033929 installed, the computer becomes unstable when resuming from sleep (S3). To work around this issue, install Microsoft Security Advisory 3033929 before installing Personal Edition. If Personal Edition is already installed, deactivate PBA and uninstall. After installing the Microsoft Security Advisory, reinstall Personal Edition. For more information, see https://technet.microsoft.com/en-us/library/security/3033929. [DDPC-4237]

Resolved Technical Advisories v8.9.1

Encryption

- A Dell Data Protection-encrypted Windows 10 computer can now be upgraded to the Windows 10 Fall Update, after a few prerequisites are met. The prerequisites must be met, due to a change Microsoft has made to the Windows update process beginning with Windows 10. For more information, see Upgrade to the Windows 10 Anniversary Update. [DDPC-928, DDPC-1146, DDPC-1443]
- Corrected a misspelling of szRegValueLoginTimeout in the registry override variable and log message. [DDPC-966]
- The computer now boots as expected after Intel Rapid Storage Technology drivers are installed. [DDPC-1246]
- The HideOverlayIcons registry setting that is used to hide the encryption icons for all managed users on a computer after the original installation now works as expected. The HideOverlayIconsOverlay registry setting now effectively hides Dell Data Protection Encryption overlay icons when File Explorer is refreshed or reopened. [DDPC-1267, DDPC-1327]
- External Media Shield Explorer now launches properly after more than one incorrect password entry when accessing media that has been provisioned on a Mac. [DDPC-1273]

- A few WSProbe options have been deprecated to improve security. The WSProbe utility no longer supports the following options: -u (enable or disable Application Data Encryption), -x (exclude application from Application Data Encryption), and -i (revert an excluded application back to included in Application Data Encryption). [DDPC-1279]
- All characters of the 32-character Endpoint Code now fully display in the External Media Shield manual authentication dialog. [DDPC-1295]
- Excess logging of file-create operations no longer occurs. [DDPC-1339]
- An issue that caused excessive memory consumption has been resolved.[DDPC-1468]
- On a Windows computer, External Media Shield now successfully opens files and folders named with accented characters that are stored on external media and provisioned using a Mac computer. [DDPC-1517]
- When encryption models are changed (SDE to HCA) after an encryption sweep has completed, the computer no longer experiences a temporary blue screen. Previously, this occurred while key types were swapped, and allowing the computer to reboot typically restored functionality. [DDPC-1536]
- External Media Shield no longer displays Access Denied errors when the Windows Media Encryption and Windows Port Control policies are set to Off and Disabled. [DDPC-1572]
- After upgrade from Security Tools v1.3.1, the computer shuts down normally. [DDPC-1606]
- Processes related with pop-up notifications during the encryption sweep have been streamlined, reducing CPU usage. [DDPC-2115]
- Decryption with the Encryption Removal Agent at uninstallation now succeeds. Previously, in a few cases, decryption began but did not finish sweeping the entire volume. [DDPSUS-751]
- An issue that caused multiple reboots during installation or upgrade on some computers is resolved. [DDPSUS-766]

Advanced Authentication

- A non-administrator user can now run an application through User Account Control on a Windows 8, 8.1, or 10 computer with Security Tools installed. [CSF-1313, DDPC-1578]
- Windows password entry now succeeds when entered first in dual-factor authentication on Windows 10, after upgrade to the Windows 10 Fall Update. [DDPC-1675]

Preboot Authentication

- A non-administrator user can now run an application through User Account Control on a Windows 8, 8.1, or 10 computer with Security Tools installed. [CSF-1313, DDPC-1578]
- The issue that led to shutdown at PBA login on a computer running ActivClient v7.0.2 is resolved. [DDPC-1898]

Resolved Technical Advisories v8.9

Encryption

- The Encryption client uninstaller now defaults to the uninstall/decrypt option instead of uninstalling but leaving files encrypted. When the option to uninstall without decrypting is selected, the Encryption Removal Agent is no longer installed. [DDPC-857, DDPC-1455]
- Silent uninstallation now supports decryption with pre-download key material on locally and remotely managed clients. [DDPC-930]
- The Shield Service no longer crashes during an HCA encryption sweep when the Volumes Targeted for Encryption policy is set to All Fixed Volumes. [DDPC-955]
- Files larger than 64Kb that are encrypted with the User or Common key on computers with HCA cards are no longer corrupted after decryption during uninstallation. [DDPC-1000]
- Upgrades now succeed, and an error no longer occurs with the message, "Error 1303: The installer has insufficient privileges to access this directory." [DDPC-1178]
- An issue that resulted in rare crashes of the local console when the console was open during an encryption sweep is resolved. [DDPC-1199]
- A default SDE Encryption Rules policy which caused problems with Windows updates has been resolved. The issue resulted from encryption of \System32 executable files. [DDPC-1207]
- Restarting or shutting down a computer during an encryption sweep no longer causes a Shield Service crash. [DDPC-1233]

- External Media Shield is now updated on a non-Shielded computer when that computer is used to access an encrypted removable media that has been updated. [DDPC-1259]
- The issue that prevented the Managed Migration Utility from converting Personal Edition to Enterprise Edition when attempting to obtain the User Principal Name (UPN) from the operating system is resolved. [DDPC-1260]
- An issue that allowed re-encryption of encrypted files when an encryption sweep started and ended during a single user login session is resolved. [DDPC-1262]
- An issue that occasionally caused a computer to become unresponsive during an encryption sweep is resolved. [DDPC-1275]
- Files stored in redirected folders on computers running HCA encryption are no longer corrupted. Previously, the last 4Kb of such files could be corrupted. [DDPC-1282]
- The Encrypt for Sharing context menu option is now present when the user right clicks a file or folder in Windows Explorer. [DDPC-1291]
- An issue that led to the computer becoming unresponsive during the reboot following installation is resolved. [DDPS-1328]
- The issue that flagged services as suspicious or offline injection attacks and blocked them from starting is resolved. Previously, this issue led to restart failures. [DDPC-1346, DDPC-1463]

Preboot Authentication

- Upgrade from v8.1 and later with PBA activated succeeds. [DDPLP-397]

Technical Advisories v8.9

All Products

- On computers running both the Windows 10 Fall Update and Kaspersky Anti-Virus, installation is blocked. [CSF-1223]

Encryption

- The Setup Wizard does not automatically launch on computers running Kaspersky Antivirus. [DDPC-1001]
- Added 04/2016 - A computer running Windows 7 hibernates although the client is unable to encrypt the hibernation data and the Prevent Unsecured Hibernation policy is enabled. [DDPC-1220]
- A fully-qualified network path must be used instead of browsing to select a mapped network drive to back up encryption keys with the Setup Wizard. [DDPC-1247]
- On HCA-encrypted computers running the Windows 10 Fall Update, HCA decryption does not start after the HCA encryption policy is changed to Off. [DDPC-1452]
- If the backup key location has changed or is no longer available, the backup fails with no obvious user notification other than a red exclamation point (!) that displays above the key backup button in the local console. To work around this issue, click the key backup button and enter a new backup location. [DDPC-1472]
- On some USB drives, External Media Shield leaves some files unencrypted and renamed with "CEF????<original filename>ERR." This occurs only occasionally, with USB drives or drivers that repeatedly disconnect and reconnect the drives. To work around this issue, rename the files with their original filenames, then remove and reconnect the drive. If the EMS Scan External Media policy is On, the resulting encryption sweep will process the files. [DDPC-1532]
- If the HCA algorithm is changed after encryption, HCA encryption does not start. [DDPC-1533]

Advanced Authentication

- The fingerprint reader on the Latitude 7510 running Windows 10 loses functionality after upgrade to Windows 10 Fall Update. To work around this issue, perform two restarts and the fingerprint reader will function again. [CSF-1210]
- Occasionally on computers running the Windows 10 Fall Update, fingerprints may need to be re-enrolled. [CSF-1225]
- The Crypto Erase Password policy does not erase the SED but, instead, deletes the authentication tokens for all users and locks the SED. Afterward, only an administrator can forcibly unlock the device. [DDPLP-370, 26862]

Preboot Authentication

- After recovering PBA access through recovery questions, the password change page displays a message that, if no action is taken, the user will be automatically logged in to the Windows session, although no automatic login occurs. [CSF-1083]

Resolved Technical Advisories v8.7.1

Encryption

- With both VMware Mirage and Webroot running on Windows 7, the computer now starts normally. [DDPC-958]
- Access is now available to non-encrypted files that became inaccessible when encryption policy was changed or the file's directory was moved. [DDPC-977]
- An issue that led to occasional computer unresponsiveness when running Trend Micro and Office 365 is now resolved. [DDPC-1125]
- Performance is improved on computers running Trend Micro Behavior Monitoring and FireAMP. [DDPC-1216, DDPSUS-391]
- Upgrade to Windows 10 now proceeds as expected, after decrypting and uninstalling Enterprise Edition. If previous upgrade attempts have failed on a computer, delete the hidden temporary folder, %systemdrive%\$Windows.~BT, before attempting upgrade. [DDPC-1237]
- On Dell Latitude E7450 and Venue Pro 11 (7130), the issue of Access Denied errors preventing encryption of some Windows folders is now resolved. [DDPSUS-521]

Advanced Authentication

- Single sign-on now succeeds on computers running Windows 7, with installation of the Microsoft KB, https://support.microsoft.com/en-us/kb/2533623. [CSF-788]
- Installation now proceeds normally on computers running Windows 10 (64-bit). [CSF-968]

Preboot Authentication

- With PBA activated on the Dell Latitude E5250, E5450, and E5550, hibernation now proceeds normally. [CSF-5]
- Preboot Authentication now accepts the apostrophe character (') in the username field. [DDPLP-376]

New Features and Functionality v8.7

- The Windows USB selective suspend feature is now supported.

Resolved Technical Advisories v8.7

Encryption

- Installation of the Encryption Removal Agent no longer results in an error following uninstallation when the option to install Encryption Removal Agent is not selected. [DDPMTR-1179]
- When SDE Encryption is enabled and SDE Encryption Rules is set to F#:\, the computer restarts as expected after system volume encryption. [DDPMTR-1360]

Advanced Authentication

- With Windows 10 on Dell Latitude E7250 or E7450, after the computer resumes from sleep, hibernation, warm boot, or cold boot, the user can now authenticate with an enrolled contactless smart card without having to occasionally re-enroll the card. [CSF-362]
- Added 11/2015 - The following drives are now supported:

  Drives with "X" are supported but are not qualified for or shipped in Dell systems.

Drive	Availability	Standard
Seagate ST320LT014 (Julius 320GB)	✓	Opal 1
Seagate ST500LM001 (Kahuna 500GB)	✓	Opal 2/eDrive
Seagate ST1000LM015 (Kahuna 1000GB)	✓	Opal 2/eDrive
Seagate ST500LM023 (Yarra X)	✓	Opal 2/eDrive
Seagate ST500LT025 (Yarra R)	✓	Opal 2/eDrive
Seagate ST500LT033 (Asagana)	✓	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3.5-inch 1000GB)	X	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3.5-inch 2000GB)	X	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3.5-inch 3000GB)	X	Opal 2/eDrive
Samsung SM850 PRO 2.5-inch MZ-7KE128 - MZ-7KE2T0 (2.5-inch SED SSD 128GB to 2000GB)	X	Opal 2/eDrive
Samsung SM850 EVO 2.5-inch MZ-75E120-MZ-75E2T0 (2.5-inch SED SSD 120GB to 2000GB)	X	Opal 2/eDrive
Samsung SM850 EVO mSATA MZ-M5E120 - MZ-M5E1T0(mSATA SED SSD 120GB to 1000GB)	X	Opal 2/eDrive
Samsung SM850 EVO M.2. MZ-N5E120- MZ-N5E500(M.2. SED SSD 120GB to 500GB)	X	Opal 2/eDrive
Samsung PM851 OPAL SSD - mSATA (mSATA 128GB - 512GB)	✓	Opal 2/eDrive
Samsung PM851 OPAL SSD - M.2. (M.2. 128GB - 512GB)	✓	Opal 2/eDrive
Micron M500 SSD 2.5-inch (120GB - 960GB)	X	Opal 2/eDrive
Micron M500 SSD mSATA (120GB - 480GB)	X	Opal 2/eDrive

Technical Advisories v8.7

Encryption

- If the HCA algorithm is changed during encryption, SDE encryption rather than HCA re-encryption begins. To work around this issue, restart the computer. After log in, HCA encryption begins normally. [DDPMTR-406]

- Reinstallation may fail with an error such as a file or folder access error or an EMSService crash, if the \temp folder was previously encrypted with the Common Encryption Key and files were not fully decrypted before uninstallation. To work around this issue, before reinstalling, remove files from the \temp folder. [DDPMTR-1647, DDPMTR-1782]
- When the Encryption Removal Agent is used to decrypt and uninstall, if an invalid Encryption Administrator Password is entered, an incorrect error message displays: "Failed to deserialize the specific file" [DDPMTR-1649]
- Running Diagnostic Info results in a file archiving error if run when files that must be accessed are locked or in use. [DDPMTR-1830]
- When running the Setup Wizard after WSDeactivate, access to Common and User encrypted data is lost. To work around this issue, after running WSDeactivate, do not run the Setup Wizard. Instead, perform File/Folder Encryption recovery as explained in the *Recovery Guide*. Select the option, My system does not allow me to access encrypted data.... Reboot the computer then run the Setup Wizard to re-activate the user. [DDPMTR-1831]
- When the EMS Access Code Failure Action policy is set to Apply Cooldown, the cooldown is not applied. To work around this issue, after the allowed number of password attempts, the user must manually authenticate to the device. For more information, see "EMS Authentication Failure" in *AdminHelp*, accessible from the Remote Management Console. [DDPMTR-1859]

Advanced Authentication

- A warning is truncated on the Encryption screen in the Setup Wizard. The warning advises the user not to unplug or shut down the computer during SED activation. [CSF-579]
- After upgrade from v8.2 or later, authentication with fingerprints fails. To work around this issue, re-enroll fingerprints after upgrade. [CSF-746]
- After uninstallation, the DDP Console icon remains on the desktop. To work around this issue, delete the icon after uninstallation. [DDPMTR-1815]

Preboot Authentication

- If activation fails with an error message that the SED must be recovered, perform a recovery using the instructions in the *Recovery Guide*, then reinstall Advanced Authentication and re-activate. [DDPLP-305]

Windows 10 In-Place Upgrade Not Supported

- Windows 10 in-place upgrade is not supported on computers with Dell Data Protection-encrypted data. BEFORE upgrading to Windows 10, uninstall and decrypt Dell Data Protection | Encryption for Windows, then upgrade to Windows 10, then re-install Dell Data Protection | Encryption for Windows. Failure to follow these steps will result in loss of data.

New Features and Functionality v8.6.1

- Dell Data Protection | Encryption Personal Edition, External Media Edition, Advanced Authentication clients now support Windows 10.

Resolved Technical Advisories v8.6.1

Encryption

- During an upgrade, the following error no longer displays: "error Opendatabase,Databasepath,Openmode/error 80004005, (MSI API error)." This error occurred intermittently and the upgrade successfully completed after the user acknowledged the error. [DDPC-882]
- An issue that previously occurred on some Dell Latitude E5540 computers with USB external drives connected that resulted in a blue screen has been resolved. [DDPMTR-955, DDPSUS-259]
- An issue that resulted in occasional SDE key load and unlock failures is now resolved. [DDPMTR-1278]
- During upgrade, when Encryption Removal Agent is installed in order to proceed with uninstall, after the user selects the backup key location and enters the password, the following error no longer displays: "Error trying to verify the key bundle is for this machine. Continue without verifying the key bundle?" The installation now proceeds as expected. [DDPMTR-1366]
- Upgrades from pre-v8.5 no longer fail due to encryption notifications being sent during the upgrade. [DDPMTR-1404]
- On computers with more than one version of Apache log4net installed and registered with the Global Assembly Cache, uninstallation now proceeds as expected. [DDPMTR-1519, DDPMTR-1536]

- The issue with continued rebooting on a computer with the number of users nearing 300 has been resolved. [DDPSUS-37]
- The issue that caused upgrade to fail with the logged error, "CInstallInf::ProcessInf - Error calling SetupInstallServicesFromInfSection," is now resolved. [DDPSUS-283]
- Encryption of the \Regback folder after a scheduled backup no longer requires a reboot for encryption to begin. [DDPSUS-302, DDPSUS-342]

Advanced Authentication

- The user can now use the external keyboard, in addition to the virtual keyboard, to submit answers to Recovery Questions. [CSF-332]
- When using HCA, an issue with single sign-on with domain smart cards is now resolved. [CSF-94]

Preboot Authentication

- On Windows 10, the issue that occasionally resulted in a blue screen when resuming from sleep on a computer with a SED installed and PBA activated has been resolved. [CSF-363]
- The issue that resulted in unnecessary reboots after the "DellMgmtAgent" service starts is resolved. [CSF-523, CSF-541]

New Features and Functionality v8.6

- Personal Edition now provides beta support of Windows 10 Technical Preview.
- The virtual keyboard is now available with Preboot Authentication on the Dell Venue Pro 11 (Model 7139).
- A customer feedback form is now available within the DDP Console. Feedback is delivered to Dell along with the Dell Data Protection product name and version number.

Resolved Technical Advisories v8.6

Encryption

- At uninstallation, decrypting a registry hive that exceeds 52 MB now succeeds and the computer no longer experiences a blue screen when uninstallation is complete. [DDPC-867]
- Encryption Removal Agent failure due to file sharing violations is now resolved. [DDPMTR-883]
- Issues that resulted in rollback of upgrades when installation was attempted more than once are now resolved. [DDPMTR-1029]
- Upgrade from v8.x no longer fails due to encryption processing during installation. [DDPMTR-1114]

Advanced Authentication

- In Security Tools - Setup, clicking the **Defaults** button on the Recovery Questions page no longer returns the prompt to confirm deletion of recovery questions but now more accurately prompts the user to confirm a reset of Recovery Questions settings. [CSF-91]
- Password Manager now functions properly with Mozilla Firefox v36.0.1 and later. [CSF-199]
- When One-time Password is used to recover access to a computer, if the user enters a blank value for the password, error messages now display "Unknown user name or incorrect password/One or more arguments are not correct." After the user acknowledges the messages, the OTP screen displays. [CSF-233]

Preboot Authentication

- The System Shutdown Required message that displays before PBA activation begins can now be properly minimized and maximized by clicking the system tray icon. [CSF-195]
- On a German operating system, the PBA logon button text is now sized correctly and fully visible. [DDPLP-276]

- On a UEFI computer with PBA activated and with default Title, Legal Notice, and Support Information for the PBA logon screen, selecting **Options > System Information** no longer returns the message “Support Information is not enabled.” [DDPUP-510]
- On a UEFI computer running a Japanese or Korean operating system with PBA activated, the PBA logon screen now loads and functions as expected. [DDPUP-547]
- On the Dell Precision T1700 and OptiPlex XE2, enabling Secure Boot and activating the PBA no longer results in the error, "No bootable devices found." [DDPUP-614, DDPUP-615]

Technical Advisories v8.6

Encryption

- Added 09/2015 - In order to add new features, functionality, and the newest operating systems, Personal Edition will support Windows XP through Shield version 8.5.
- Added 08/2015 - If Microsoft TPM Base Services is improperly installed, the following functionality is affected: HCA provisioning, fingerprint enrollment in the DDP Console/Security Console, and BitLocker Manager operation. For more information and to work around this issue, refer to this KB article: http://www.dell.com/support/article/us/en/19/SLN296706. [CSF-454]
- During Configuring for Encryption, if the user selects a backup location that becomes unavailable or to which the user loses write permissions before setup is complete, the Setup Wizard continues to prompt for a valid location even after such a location is entered. To work around this issue, close the Setup Wizard and launch the system tray application again. When prompted, enter a valid backup location. [DDPC-764]
- If HCA policy is disabled or the HCA encryption algorithm is changed during encryption, the computer may experience a blue screen after reboot or at PBA logon. [DDPMTR-282]
- During SDE encryption, a popup notification displays to prompt the user to cancel encryption when an application is waiting for encryption of a file to complete. If this occurs rapidly during a short length of time, multiple notifications may simultaneously display. [DDPMTR-943]
- When Encryption with Deferred Activation is installed but not activated, the user cannot uninstall and reinstall a different DDP edition. Because activation did not occur, retrieval of encryption keys and decryption are not possible. A different DDP edition cannot overwrite the deferred activation Encryption client. [DDPMTR-944]
- Due to Microsoft's change in the way Windows handles stopping a critical service, stopping a DDP service such as CMGShield service, EMS service, or the Dell Data Protection | Encryption process in Task Manager will result in the computer experiencing a blue screen. [DDPMTR-945]
- In Windows 10, when using EMS Explorer to open a 5GB file on encrypted removable media an error displays, "The... file is too large for notepad," and the file does not open. [DDPMTR-990]
- When opening a file on encrypted removable media through EMS Explorer on a non-Shielded computer, if the removable media is removed without being ejected, the file remains in the computer's Ems Explorer Temporary Files folder in clear text after the file is closed. Properly ejecting the removable media properly removes these clear-text files. [DDPMTR-1157]
- After recovery of a computer running Windows 10 with HCA policy enabled, if HCA policy is then disabled the computer experiences a blue screen rather than decrypting as expected. [DDPMTR-1303]

Advanced Authentication

- When a user begins credential enrollment but quits without saving before enrollment is complete, the credentials are enrolled rather than discarded. To work around this issue, if policy allows the user to modify their own credentials, the user can open the DDP Console, select the **Enrollments** tile, select and delete the credentials. Otherwise, an administrator must remove them. [CSF-146]
- During activation, if the selected backup location is not available, the user cannot set a new backup location in the activation dialog but must instead set the new location through **Administrator Settings > Backup Location** before activation can proceed. [CSF-238]
- Password Manager does not support the Windows 10 web browser, Microsoft Edge. [CSF-281]
- When running on Windows 10, the DDP Console About window displays incorrect BIOS information and an incorrect serial number for the computer's motherboard. [CSF-291, CSF-301]
- When a contactless smart card is moved across the card reader, a popup notification prompts the user to enroll the smart card. If the card is moved multiple times in a short length of time, multiple popup notifications may simultaneously display. [CSF-293]
- On Windows 10, if the Validity Fingerprint Sensor driver is out-of-date, when PBA is activated, the computer experiences a blue screen. To work around this issue, ensure that PBA is not enabled by policy, then follow these steps:

1 Install Dell Data Protection then reboot.

2. In Windows Control Panel, navigate to Device Manager.
3. Under Biometric Devices, disable the Validity Fingerprint Sensor.
4. Activate the PBA.
5. After reboot, the Validity Fingerprint Sensor can be re-enabled, and the fingerprint reader functions as expected.

   To download the latest Validity Fingerprint Sensor driver, go to http://www.dell.com/support/home/us/en/19/Products/?app=drivers and select your computer model to check and download the latest driver.

   [CSF-349]

- When running Windows 10 on Dell Latitude E7250 or E7450, when the computer resumes from sleep, hibernation, warm boot, or cold boot, the user may be unable to authenticate with an enrolled contactless smart card. To work around this issue, change the policy to require only password authentication. The user should log on and re-enroll the contactless smart card. After re-enrollment, the user will be able to log on with the contactless smart card. [CSF-362]
- Added 08/2015 - If Microsoft TPM Base Services is improperly installed, the following functionality is affected: HCA provisioning, fingerprint enrollment in the DDP Console/Security Console, and BitLocker Manager operation. For more information and to work around this issue, refer to this KB article: http://www.dell.com/support/article/us/en/19/SLN296706. [CSF-454]

Preboot Authentication

- Upgrade from v8.1 or v8.2 to v8.6 on a computer with a SED installed and PBA activated fails. [CSF-449, CSF-461]
- Upgrade on a computer with a LiteOn M3 series SSD installed and PBA activated fails due to the small disk size. To work around this issue, before upgrading, deprovision the PBA. After upgrade, the PBA can be reactivated. [CSF-528]
- With PBA activated on Dell Latitude E7450, navigation of the Advanced Boot Options menu is not possible because the native keyboard is not available. To work around this issue, deactivate the PBA, access the Advanced Boot Options menu, and keyboard navigation is available. [DDPLP-286]
- On Dell Latitude E7250, E7350, E7450, and Venue Pro 11 (Model 7139), recovery fails with Dell Opal SED Recovery Utility one-time unlock of the drive. To work around this issue, use the recovery key to unlock a drive on one of these models. [DDPUP-763]

Resolved Technical Advisories v8.5.1

All Products

- Enhancements have been made to the installer to ensure that the correct PBAAuthURI is maintained, even if the installation reboot occurs before the authentication agent is upgraded. [CSF-123, CSF-125]
- The issue of failing attempts to open a Microsoft Excel workbook, with either a message that a problem occurred sending the command to the program or a message that the file path or file name could not be found, is now resolved. [CSF-157]
- The issue of upgrading or uninstalling Dell Data Protection | Encryption with the tray application or console application running causing upgrade and uninstallation failures has been resolved. The tray application and console now close gracefully so that the upgrade or uninstallation can complete as specified. [DDPC-449]
- The issue of some special unicode characters, particularly German language umlaut characters, failing to be recognized during entry of password recovery questions, is resolved. [DDPLP-202]

Encryption

- HCA activation time-outs when using Security Tools' One-time Password have been resolved. [CSF-12]
- When reactivating the PBA, a message to shut down the computer now properly displays. [CSF-20]
- TPM ownership is now properly taken after being cleared in BIOS when using DDP. [CSF-21]

Advanced Authentication

- When using Security Tools, the enrollment credentials wizard summary page now shows the chosen login option in the summary. [CSF-93]

- When using Security Tools' One-time Password feature, for devices that are already enrolled, enrollments are now properly deleted when the policy "Mobile Device Require Password" is changed from Off to On. [CSF-94]
- When using Security Tools' One-time Password feature, null reference pointers have been resolved. [CSF-98]
- The issue of using Security Tools, Windows 8.1, and the GPO "Do Not Display Last Username", causing single sign-on to fail has been resolved. [CSF-100]
- Improvements have been made to make user login and start-up more reliable. [CSF-114, CSF-116]
- Issues related to the "DellMgmtAgent" service failing to start or starting slowly have been resolved. These issues presented in the Windows System Event Viewer under the Service Control Manager with a message similar to the following: "The DellMgmtAgent service failed to start due to the following error: The service did not respond to the start or control request in a timely fashion." [CSF-116]
- Encryption statistics now properly display in the Security Tools Console. [CSF-121]
- The issue of "Security Tools - Setup" being incorrectly translated in Chinese to "Security Tools - Installation" has been resolved. [CSF-128]
- When running Security Tools, "DDP Console – Admin Settings" is now properly displayed in the All Programs menu instead of NewShortCut3. [CSF-129]
- The size of the Security Tools Console now stays constant, unless it is manually enlarged or reduced. [DCF-2]
- The issue of some special unicode characters, particularly German language umlaut characters, failing to be recognized during entry of password recovery questions, is resolved. [DDPLP-202]

Resolved Technical Advisories v8.5

Encryption

- Previously, FFE was used for Common and User encrypted files, even though HCA encryption was specified. This issue is resolved. [28029, DDPC-58]
- The user now has proper access to User and Common encrypted files after HCA decryption. [28810/DDPC-98]
- Previously, in some scenarios, a delay occurred when moving files between folders during Microsoft Word autosaves when using Trend Micro AV and when DDP encryption was installed. This issue is resolved. [DDPC-127]
- Windows Explorer now updates its icon cache after a successful decrypt/uninstall when running Windows 8.1. The Windows Explorer folders no longer display the DDP Encryption icon after successful decrypt/uninstall. [28332/DDPC-253]
- Legacy FVE can now optionally be used with an updated BIOS (without requiring an Enterprise HCA installation) on Dell Latitude E5430, E5530, E6230, E6430, and E6530 computers. [DDPC-304]
- When using Dropbox, if a user is accessing files from a *new* computer or if a user account name changes, files synchronized with Dropbox no longer appear corrupt and the user no longer receives Access Denied messages when attempting to access the files. [DDPC-391]

Advanced Authentication

- On Dell Venue tablets, after the Enrollment Wizard is launched, the on-screen keyboard can now be opened by tapping the keyboard icon in the Wizard or the keyboard system tray icon. [MMW-524]
- When using HCA, single sign-on is now available when using multi-certificate Common Access Cards (CACs). [MMW-559]

Technical Advisories v8.5

Encryption

- Amended 06/2015 - If the computer restarts during encryption with legacy HCA on Dell Latitude E5420 or E6420 or Precision M4600 or M6600, the computer becomes unresponsive. [DDPMTR-341]
- Amended 06/2015 - On Dell Latitude E7250 and E7450, SDE rather than HCA encryption is provisioned. [DDPMTR-822]
- Amended 06/2015 - When running WSDeactivate, following the prompted reboot, the user is prompted to finish setup rather than to enter the recovery key for activation as expected. [DDPMTR-1213]

New Features and Functionality v8.4.1

- Multi-certificate Common Access Cards are now supported.

Resolved Technical Advisories v8.4.1

Encryption

- The DDP installation process now proceeds normally on laptops connected to a power source, even if the battery charge falls below 10 percent. [27974/DDPC-56]
- Previously, when using Dell Digital Delivery, installation could fail based on the order of installation of Security Tools or the DDP master installer. Logic has been added to correct this issue. [28070, MMW-293]
- A few previously unlocalized master installer screens are now localized. [28619, 28620, DDPC-73, DDPC-262]
- Previously, when upgrading, an error message displayed indicating that *ushradiomode64.exe* was not able to start correctly. The issue of a third-party installer incorrectly attempting to install Microsoft .Net Framework 3.5 on the computer is resolved. [29049, DDPC-182, MMW-357]
- Installation/upgrade failures related to SQL Compact have been resolved. [DDPC-43, DDPC-384]
- Multiple performance improvements have been made to file/folder and HCA encryption. [DDPC-171, DDPC-279]
- In Windows 8.1, the Metro HelpAndTips app now opens and functions normally. [DDPC-264]

Advanced Authentication

- Previously, when using a non-USH external fingerprint reader, after the computer went to sleep or was rebooted, logon using fingerprint failed. The issue with the credential provider timing out when attempting to confirm the fingerprint reader is connected to the computer is resolved. [28605, MMW-360]

Preboot Authentication

- Previously, on some computers with Security Tools and Preboot Authentication enabled, the computer would not boot after entering credentials into the PBA logon screen, and the computer would halt at a black screen with the words "Parity Error". [DDPLP-137]

Technical Advisories v8.4.1

Encryption

- After installation, HCA encryption and the Preboot Authentication environment are not provisioned until after the computer reboots a second time and the user provides the Encryption Administrator Password. [DDPC-448]
- The Shield does not detect password changes for non-domain accounts when the password is reset from another account. As a result, when the non-domain user attempts to logon again, the logon fails because the Shield did not synchronize the password change. [DDPC-490]

Advanced Authentication

- Amended 12/2014 - Fingerprint enrollment does not prevent the user from using fingerprints from different fingers when enrolling a single finger. [MMW-212]

Preboot Authentication

- Single Sign-on intermittently fails on computers with self-encrypting drives on which Preboot Authentication is activated. [DDPLP-144]
- When replacing a provisioned self-encrypting drive (with the Preboot Authentication environment active) with a *new* self-encrypting drive and provisioning the Preboot Authentication environment, after the new SED is provisioned, the old SED can no longer be recovered. [DDPLP-150, MMW-581]
- On the Dell Latitude Rugged Extreme, the user is able to detach the tablet from the dock. However, the dock is needed to log in through the PBA. Detach the tablet only after the PBA authentication step is complete. [DDPLP-162, DDPLP-163]
- After successfully authenticating to the Preboot Authentication environment, the computer will not complete Single Sign-on. Instead, the computer halts at the Windows Logon screen for another user. Microsoft Windows 8.1 defaults to the Logon screen for the previously authenticated user. To complete logon, return to the User Tiles screen by selecting the back arrow in the top right of the screen and then selecting the correct user tile for the user authenticated in the PBA. SSO data captured by the PBA may still be present and once the user tile is selected, Windows authentication may be completed automatically. [MMW-564]

Resolved Technical Advisories v8.4

Advanced Authentication

- Pre-enrolled Contactless Smart Card users are no longer lost after joining the computer to the domain. [28386/DDPC-61, MMW-347]

Technical Advisories v8.4

Encryption

- When USB external media with little or no space available are inserted into Shielded computers to be encrypted, users receive no indication that the media are full and will not be encrypted. [DDPC-243]

New Features and Functionality v8.3.2

- Dell Data Protection | Encryption Personal Edition, External Media Edition, and Advanced Authentication clients now support Windows 8.1 Update 1.
- This release of adds support for the following platforms when using the DDP | Hardware Crypto Accelerator:
    - Dell Precision M4800
    - Dell Precision M6800
    - Dell Precision T1700
    - Dell OptiPlex 7010
    - Dell OptiPlex XE2
    - Dell OptiPlex 9020 AIO
    - Dell OptiPlex 9020

Resolved Technical Advisories v8.3.2

All Products

- Occasional failures when running the master installer have been resolved. The *Wizard was interrupted* message no longer displays. [28491]

Encryption

- A new user is no longer presented a logon screen for a different user when logging on to the PBA for the first time with dual-factor authentication configured for Password + Fingerprints. [28886]

Advanced Authentication

- Fingerprint credentials are now retained when upgrading from v8.2.1 or earlier. [28457, 28766]
- Upgrade failures related to a USH fingerprint sensor configuration file error have been resolved. [28845]
- Attended enrollment is no longer needed when the Authentication Policy is set to Fingerprints + Contactless Smart Cards. [28873]

Technical Advisories v8.3.2

Encryption

- Local options to manage the secondary drive are unavailable in the Dell Data Protection | Encryption console until after a policy change on that drive is applied and the computer is re-booted. [29046]
- USB external media provisioned with Dell Data Protection | External Media Edition cannot be accessed and the message *All encryption key material has been deleted* is displayed to the user.

  This condition occurs when external media provisioned by Dell Data Protection | Encryption for Mac is accessed on Windows computers running Dell Data Protection | Encryption for Windows. To recover from this condition, follow the instructions below. [29055]

  Instructions

  a Insert the external media into a computer without Dell Data Protection | Encryption installed (a clean computer, WinPE image, Windows boot disc, etc.).

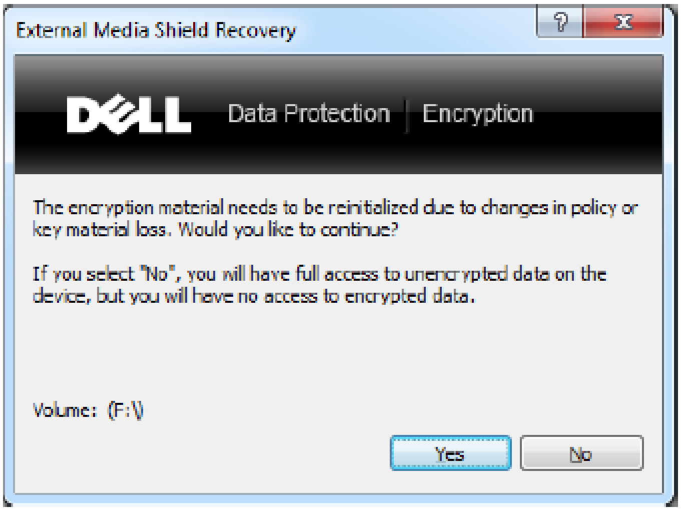
  b Manually delete the hidden *_Encryption_Data_Do_Not_Delete_* folder. If running this from a command prompt you may need to remove the hidden attributes first (i.e. attrib -r -h -s _Encryption_Data_Do_Not_Delete_).

  c Manually delete the *Access Encrypted Files (Mac).dmg, AccessEncrytpedFiles.exe*, and *autorun.inf* files from the root of the device.

  d Login to a computer running Dell Data Protection | Encryption with the same user account that originally encrypted the external media. Older versions of Dell Data Protection | Encryption will also require both the same user **and** same computer that originally encrypted the external media.

  e Insert the EMS-encrypted external media.

  f You are prompted to perform a recovery. Click **Yes**.


External Media Shield Recovery
DELL Data Protection | Encryption

The encryption material needs to be reinitialized due to changes in policy or key material loss. Would you like to continue?

If you select "No", you will have full access to unencrypted data on the device, but you will have no access to encrypted data.

Volume: (F:\)

g Enter a new password to restore access to encrypted files.

- PCIe SSDs are not supported on Precision T-series computers.

New Features and Functionality v8.3.1

- Dell Data Protection | Encryption Personal Edition now supports Offline Files and Folders. For an overview of Offline Files and Folders, see http://windows.microsoft.com/en-us/windows/understanding-offline-files#1TC=windows-7.
- Dell Data Protection | Encryption Personal Edition now supports OneDrive on Windows 8.1. [28300, 28303, 28304]

Resolved Technical Advisories v8.3.1

Encryption

- Enhancements have been made to improve Shield stability and performance. Additionally, improvements have been made around memory allocation and CPU usage during file encrypt and decrypt operations. [28376, 28377, 28547, 28672, 28721, 28733, 28737, 28815, 28836, 28849, 28943]
- SDE key load and unlock failures after installing Microsoft Windows Management Framework 3.0 (KB2506143) have been resolved. [28654, DDPC-325]
- Uninstallation of the Security Tools Authentication component no longer fails when uninstalled with the master installer. [28807]
- Occasional instability issues with WSScan have been resolved. [28869]

New Features and Functionality v8.3

- DDP | Hardware Crypto Accelerator - updated software to provide full Enterprise manageability, including:
  - Network logon to domain
  - Single Sign-on
  - Single PC - Multi-user support
- This release of the new DDP | Hardware Crypto Accelerator software runs on the following platforms:
  - Dell Latitude Model E6440
  - Dell Latitude Model E6540
  - Dell Latitude Model E7240
  - Dell Latitude Model E7440

Resolved Technical Advisories v8.3

Encryption

Revised 04-2014

- The Shield now properly processes category 3 policies to override ADE-encrypted (category 2) files. [25211]
- Previously, a message stating "Invalid Value for 103" was displayed in the local console and current settings were not viewable. This issue has been resolved. [27005]
- Sweep status update failures are reduced due to improved processing around renaming of internal lists to ensure that the rename does not fail if the file already exists. Additionally, logging of errors around list file deletion is improved. [27853]
- Improved processing of exception handling has been implemented. [28431]
- Previously, if EMS encrypted a device on a Dell Data Protection | Encryption 8.x computer, used the device on a Dell Data Protection | Encryption 7.2.x computer, then returned to use the device again on the original 8.x computer, a failure occurred. Better handling of mixed environments has been added to EMS. [28453]
- Several enhancements have been made to improve stability and performance. [25816, 27497, 28508, 28538, 28543, 28643]
- The upgrade process has been improved to reduce errors and failures. [28403, 28720]
- A system deadlock during the boot cycle when Dell Data Protection | Encryption 8.x is installed alongside Kaspersky Endpoint Security has been resolved. [28425]
- Errors related to upgrading CMG v6.8/7.3 to Dell Data Protection | Encryption v8.x have been resolved. [28466]
- When running the Shield on a VMWare image with SCSI hard drives, the Shield will now properly identify the drive as Internal, rather than Removable. [28540]
- Previously, after upgrading to v8.x and then uninstalling from the user interface, errors related to the Decryption Agent would display. This issue has been resolved. [28552]
- An upgrade of Symantec Endpoint Protection from 11.x to 12.x now works as expected. The Shield no longer blocks access to the SEP services. [28622]
- Errors related to SQL Compact 3.5 SP2 have been resolved. [28726]
- Previously, after full HCA encryption and then hibernating, the computer would fail to retain the system state after returning from hibernation. This issue has been resolved. [28738]

-----------**End of Revision**

- During an encryption sweep, the user can now pause encryption from the tray icon rather than having to launch the local console. [26785]
- An encryption sweep triggered by a policy update or encryption sweep request no longer times out when encrypting files larger than 4 GB. [27705]
- Previously, after decryption following an HCA algorithm change, SDE encryption began rather than HCA re-encryption. Now, after decryption following a change to the encryption algorithm, and after a reboot, HCA is provisioned and encryption begins normally. If the computer is not equipped with an HCA card, SDE encryption begins as expected. [27986]
- After upgrade from a v7.x Shield for Windows, log files no longer include the entry, "Credential Sweep - Failed to process all entries." [28550]
- Performance is improved when using Windows Explorer to navigate large directories in network shared folders. [28640]

Advanced Authentication

- During password recovery, when answers to Recovery Questions are entered, the answers now display as obfuscated characters rather than in clear text. [27977]
- The fingerprint reader no longer fails at sign on due to Microsoft Windows fingerprint reader private sensor pool issues. [28085]
- In landscape view on Dell Venue tablets, buttons and the side scroll bar now display correctly on all screens. [28346, 28347]
- On French operating systems, version information that is displayed in the Security Console > Settings > About page is now correct. [28385]

Cloud Edition

- Users can no longer access protected sites when the policy is set to block those sites. [DDPCE-24]
- When using OneDrive and an iOS app, files uploaded to the cloud are no longer deleted by the sync client running on a Windows computer. [DDPCE-97]
- While IPv6 is not supported, the web browser no longer intermittently toggles between protected and unprotected states when IPv6 is enabled on the network adapter. IPv4 should be used, for Cloud Edition for Windows to function properly. [DDPCE-98, DDPCE-107]
- Compatibility issues with 64-bit computers are now resolved. [DDPCE-108, DDPCE-138]
- Encrypted files are no longer re-encrypted when downloaded with the browser and saved into protected sync folders. [DDPCE-109]
- Protection status no longer intermittently toggles between protected and unprotected. [DDPCE-113]
- Encryption client behavior during device suspension is improved. [DDPCE-118]
- Auditing functionality is improved. Event IDs now map directly to Event Types. Audit volume is reduced, up to 98 percent. Uploads and downloads are now logged as Events.
- Compatibility with Windows Sync Client is improved.

Technical Advisories v8.3

Encryption

- If Windows updates are not installed before the master installer runs, installation may fail. [28835]
- The computer does not Single Sign-on (SSO) after waking up from Hybrid Sleep. After the user enters their credentials at the Preboot Authentication (PBA) screen, the computer stops at the Windows logon screen and the user must manually log on to the computer.

  Dell Data Protection | Security Tools and Dell Data Protection | Encryption do not support Hybrid Sleep states and SSO when Preboot Authentication (PBA) is Active. Disable Hybrid Sleep when using Preboot Authentication if your organization intends to use SSO. [25785]
- During a command line uninstall, the installer will not download the encryption keys for the computer unless Silent mode is specified using the parameter CMGSILENTMODE=1. To work around this issue, specify CMGSILENTMODE=1 in the command. [27979]
- All registry keys and installation files are not removed after uninstallation. [28219]
- After uninstallation, logon with cached credentials occasionally fails when the computer is not connected to the network. During uninstallation, the cached credentials are decrypted. If this decryption fails for any reason, the user will not be able to login while disconnected from the network. To work around this issue, reconnect to the network and log on to cache the credentials. [28277]
- The encryption icon that indicates that a drive is encrypted does not display when a drive has been encrypted using HCA. [28400]
- During an attended (non-silent) upgrade from v8.1, the installer does not prompt the user to confirm that the upgrade is desired before continuing the installation. [28574]
- Preboot Authentication uses a "Basic" disk partition and cannot be converted to "Dynamic" partition (for RAID arrays). Attempts to convert the partition will result in the PBA not being created or the PBA not starting. [28587]
- After partial decryption recovery on a computer with an HCA card, the local Dell Data Protection | Encryption console may display duplicate information about local disks. To work around this issue, reboot the computer. After the restart, disk information displays properly. [28656]
- After installation of Enterprise Edition, the Microsoft Usbccid Smartcard Reader is intermittently reported as being in a problem state in Device Manager. However, smart cards and fingerprints seem to function normally. Dell ControlVault relies on the Microsoft Usbccid drivers. A premier case has been opened with Microsoft regarding this issue. [28697]
- Decryption on computers with HCA cards removes Preboot Authentication, which must be reinstalled. At the next logon, both an Encryption Administrator Password prompt and a Security Tools shutdown message display. When the computer is shut down, PBA activation begins. However, provisioning will be completed only after a subsequent reboot and entry of the Encryption Administrator Password. [28722]
- Infrequently, after HCA policy is set, the Preboot Authentication screen does not display until the computer is restarted a second time. [28762]
- Support for migrating the Personal Edition HCA preboot environment into Enterprise Edition is not available in v8.3. [28794]
- After encryption is enabled, the computer intermittently logs a Critical System Event 41 in the System Event Logs with this description: "The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or

lost power unexpectedly." The issue occurs only during a reboot and does not impact the security of the data or the performance of the computer. [28795]

- Amended 12/2014 - Secure Boot is a Unified Extensible Firmware Interface (UEFI) protocol that Windows 8 and 8.1 users can enable in the computer's BIOS to ensure that the computer boots using trusted firmware signed by the computer manufacturer. The feature is not supported when the following conditions are met:

  - HCA with Dell Data Protection | Security Tools installed
  - HCA with Dell Data Protection | Encryption installed
  - HCA with Dell Data Protection | Security Tools and Dell Data Protection | Encryption installed

    To upgrade to Windows 8 or 8.1 on a Dell computer with SED or HCA, Secure Boot cannot be enabled in BIOS. The Secure Boot setting is disabled by default for computers shipping with Windows 7 or Windows 8/8.1 Downgrade Rights. This setting should not be changed.

    Instructions:

1. Turn on the power to your Dell computer. If the computer is already powered on, reboot it.
2. Press **F2** or **F12** continuously during boot until a message displays at the upper right of the screen that is similar to "preparing to enter setup" (F2) or "preparing one-time boot menu" (F12). This launches the system BIOS.
3. In Setting > General > Boot Sequence, ensure that the Legacy Boot List Option is selected.
4. In Settings > General > Advanced Boot Options, ensure that the Enable Legacy Options ROMs check box is selected.
5. In Settings > Secure Boot > Secure Boot Enable, ensure that the Secure Boot Enable selection is Disabled.
6. Apply the changes.
7. Now that the computer BIOS has been changed to a legacy boot mode, the computer must be re-imaged.

   [28790]

- When running Windows 7, a computer that is HCA encrypted may not boot in Windows Safe Mode. [28819]
- When using EMS Explorer, cutting and pasting a file does not remove the file from its original location. [28848]
- After an upgrade from v8.2 to v8.3, the v8.2 Dell Data Protection | Encryption installer remains on the computer. [28885]
- During an SDE encryption sweep, although the disk is only partially encrypted based on the progress of the sweep, the Security Console Encryption screen shows the disk as Protected. [28888]
- Fingerprints and smart cards stop working after the Port Control System policy to disable USB ports is applied. Broadcom USH hardware is a USB-attached device. When the policy to disable USB ports is applied, it prevents data transmission to and from the Broadcom USH hardware, which prevents users from logging on with fingerprints or smart cards. The problem can be resolved by applying a combination of policies that restrict access to USB external media by setting Windows Portable Device and External Storage Device class policy to Read Only. This policy combination allows the Broadcom USH hardware to function properly but prevents data from being transferred from the computer to external media such as USB flash drives and smart phones. [28895]

Advanced Authentication

- Removing the USB Fingerprint reader without ejecting the device causes Dell ControlVault to fail. The issue occurs because Windows handles the removal action of biometric devices incorrectly. To correct this issue, download and install the Hotfix available at http://support.microsoft.com/kb/2913763. [27696]
- A contactless card may not be immediately recognized, because Windows does not load its driver. To work around this issue, in Windows Device Manager, disable the smart card device. For more information, see http://support.microsoft.com/kb/976832. [27981]
- On Dell Venue tablets, the touch keyboard is not automatically available at the Windows logon screen. To work around this issue, touch the keyboard icon to display the touch keyboard. [28257]
- When the Password Manager option, Fill in logon data, is selected and credentials are enrolled with Password Manager, data is populated into a logon screen but log on does not occur. [28502]
- With Windows 8.1, after a Password Manager logon is deleted in the Security Console, the link to the logon page remains in the list of Password Manager logons. [28515]
- Password Manager is not available in Google Chrome until it is activated. To activate Password Manager in Google Chrome, follow these steps:

1. In the Google Chrome Settings page, select **Make Google Chrome my default browser**.

2. Select **Show advanced settings** > **Content settings** > **Disable individual plug-ins** and then select **Always allowed** for the Dell Data Protection | Security Tools Plug-in. Close the Plug-ins page.
3. In the Google Chrome Settings page, select **Extensions** and check the Enable box next to the Dell Data Protection | Security Tools Extension.
4. Exit Google Chrome and re-launch.

   When you access a site that contains a logon form you will be prompted with the pre-train icon to capture the logon credentials for the site.

   [28528, 28678, 28719]

- In Password Manager, the Select Logon Data window does not show the user name of the first enrolled user. [28531]
- When using Password Manager with Firefox, double-clicking the pre-train icon does not open the Add Logon dialog. [28693]
- The Password Manager shortcut (CTRL+WIN+H) cannot be used on tablets, because the WIN button is not present. [28706]
- Password Manager prompts for credentials only when accessed for the first time after the user logs on and not again until the next log on or computer restart. This is working as designed. [28714]
- The Password Manager version number may differ across web browsers. [28808]
- In the Security Console, the Backup and Restore feature is described as providing data backup and restore functions but is specifically related to backup and restore of Password Manager data. [28856]
- When dual-factor authentication is enabled and the computer resumes from sleep, the computer intermittently stops responding and the screen is black. To recover from this situation press and hold the power button until the computer shuts down, then reboot the computer. [28900]
- The computer does not Single Sign-on (SSO) after waking up from Hybrid Sleep. After the user enters their credentials at the Preboot Authentication (PBA) screen, the computer stops at the Windows logon screen and the user must manually log on to the computer.
- Windows logon fails with some new CAC smart cards, which use multiple certificates with the same name. One certificate is the authentication certificate and the other is a signing certificate. The algorithm used to select the certificate uses the newest certificate. If the newest certificate is the signing certificate, Windows logon will fail. To work around this issue, create an Active Directory entry for the principle name for the signing certificate. [27857]
- Preboot Authentication fails if a self-encrypting drive is configured as drive 1. To work around this issue, configure a self-encrypting drive as the boot drive (drive 0) for Preboot Authentication to function properly. [28266]
- Single Sign On does not function properly when cached credentials in UPN format are used. [28660]
- When Security Tools Authentication components are uninstalled, the user is not warned that Preboot Authentication is provisioned. Uninstalling Security Tools Authentication will impact only the user's ability to update credentials in the PBA but will not prevent the user from authenticating with existing user accounts. The proper uninstallation sequence is as follows:

  Deactivate the PBA

  Uninstall Security Framework

  Uninstall Security Tools Authentication

  [28791]

Cloud Edition

- Pop-up windows that alert the user to reboot or to run an update should persist but do not. [DDPCE-39, DDPCE-40]
- When creating a folder in the Dropbox client, the user is unable to assign a name to the new folder. [DDPCE-74]
- Occasionally, slow performance is observed when listing files through a managed browser section. [DDPCE-93]
- When using Box, new local folders are not synchronized in the cloud if a folder named "New..." exists in cloud storage. To work around this issue, delete the folder with the name "New...." [DDPCE-96]
- Occasionally, if Cloud Edition is left running and idle, an error occurs and the system tray icon cannot reconnect to the service. To work around this issue, restart the computer and log on to Cloud Edition. [DDPCE-157]
- When using Box and Dropbox, some files that are deleted locally are not removed from cloud storage. [DDPCE-168]

New Features and Functionality v8.2.1

- Personal Edition now supports Microsoft Windows 8.1.

Resolved Technical Advisories v8.2.1

Encryption

- Personal Edition provides improved support for the touch keyboard on the Microsoft Windows 8.1 Sign On Screen.
- Log files are now placed in the proper directory on localized operating systems. [25463]
- An unrecoverable error no longer occurs upon encryption completion when the Local Management Console is left open and the computer is locked for an extended period of time. [27545]
- Interoperability issues when using VMware image files have been resolved. [28355]
- Previously, when uninstalling the Encryption client, if the uninstaller failed, the Decryption Agent would be installed before the uninstaller failed. This caused issues because the uninstaller would not re-run if the Decryption Agent was already installed. This issue is resolved. [28364]

Technical Advisories v8.2.1

Advanced Authentication

- Pre-enrolled Contactless Smart Card users are lost after joining the computer to the domain. Therefore, the indicator on enrollment status shows that no users have been enrolled using Contactless Smart Cards. To work around the issue, log on to the computer with a user ID and password, then re-enroll Contactless Smart Cards for local and domain users. [28386]
- Amended 03/2014 - When using Microsoft Windows 7 on the All-in-One computer without an external keyboard, the On-Screen Keyboard does not automatically display after the computer resumes from the sleep or hibernate state. To display the On-Screen Keyboard, select the On-Screen Keyboard button at the lower left of the Windows Login Screen. [28606]
- Amended 04/2014 - Integrated fingerprint readers on Latitude E6430u and Latitude E5430 do not work after installing Dell Data Protection | Security Tools 1.2.1 or later on Windows 7 (64-bit). To use the integrated fingerprint reader on these computer models, use Dell Data Protection | Security Tools 1.2 (or Dell Data Protection | Encryption 8.2). [28979/DDPC-157, MMW-393]

New Features and Functionality v8.2

- Personal Edition now supports Microsoft Windows 8.1 on Dell Venue Pro 11, Dell Venue Pro 8, and Dell OptiPlex 3020.

Technical Advisories v8.2

Advanced Authentication

- If the "Interactive logon: Smart card removal behavior" Group Policy Object is configured to lock or force log off when a smart card is removed, the computer will be locked or the user will be logged off during Dell Data Protection | Encryption installation, because smart card reader drivers are updated during Dell Data Protection | Encryption installation. To work around the issue, unmount the smart card from the reader prior to installing Dell Data Protection | Encryption. [27856]
- Amended 01/2014 - When using Microsoft Windows 8.1, Single Sign-On with Password Manager does not work with some email providers. [28259]
- Amended 01/2014 - The Password Manager prompt to add a login screen displays after de-selecting "Prompt to add logons for logon screens" in the Security Console Settings or when selecting "Exclude this screen" in Internet Explorer Icon Settings. To correct the issue, download and install Microsoft KB2888505 https://support.microsoft.com/kb/2888505. [28334, 28445, 28536]
- Touch capability is not available for Password Manager icons on Dell Venue Pro 11 and Dell Venue Pro 8 tablets.
- Updated drivers for the Eikon to Go external fingerprint reader for Windows 8.1 can be found on support.dell.com.

Resolved Technical Advisories v8.1.1

Encryption

- Upon upgrade to 8.1, EMS was failing to prompt CD/DVD media to encrypt due to the controller driver failing to provide the correct device type to EMS. This release resolves the issue and CD/DVD media is now properly prompted to encrypt. [28150]
- Additional hardening and stability fixes have been added to this release.
- This release resolves the issue of encrypting/decrypting files larger than 4GBs.

New Features and Functionality v8.1

- Personal Edition adds class level port controls to block data leakage to smartphones
- Personal Edition adds Windows XP support for software encryption

Resolved Technical Advisories v8.1

All Products

- Windows Vista is no longer a supported operating system.

Encryption

- The Dell Data Protection | Encryption v8.x conflict with Symantec Endpoint Protection v12.x. has been resolved. The SEP v12.x product uses 2 separate filter drivers which led to a dead-lock with the re-architected Dell Data Protection | Encryption v8.x file encryption driver. [27660]
- A registry override has been created to allow SDE encryption on a self-encrypting drive. By default, the 8.x client disables SDE encryption if a self-encrypting drive is detected on the computer. It does not matter if the drive is the primary disk or not. This can be a problem if the customer only wishes to use SDE encryption and has a self-encrypting drive that is not configured. Use this registry setting to always enable SDE on a self-encrypting drive that is not configured. A reboot is required for this setting to take effect. [27565]

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]
  AlwaysApplySDE=REG_DWORD:1
  ```
- If an SDE encrypted file is moved (not copied) to a Common or User encrypted folder, the Shield now properly applies the Common or User encryption policy, rather than remaining SDE encrypted. [27752]

Advanced Authentication

- The Tab key can now be used to navigate through the recovery questions in the Security Console. [26974]
- When using Password Manager, the default values in the Live.com/Hotmail.com credential fields are now correct. [27033]
- The Authentication tab in the Security Console no longer displays a blank page after switching tabs. [27112]

Technical Advisories v8.1

Encryption

- When running Windows 8, the Shield's Fast User Switching message is hidden behind the Windows 8 log off screen. [26272]
- DVDs become corrupt after a PCS policy change to Read Only in the following scenario: When PCS is enabled for Optical Drives with 'UDF-Only' policy and the user copies files over (opens a session), before the session is closed (usually by ejecting the media) a new PCS policy comes down that sets the optical drive to 'Read-Only'. The Shield starts a reboot-snooze cycle when changing from 'UDF-Only' to another policy. If the user accepts the reboot request, Windows reboots without closing the session, because it assumes it can close after the reboot. However, after the reboot, the device is in 'Read-Only' mode and Windows cannot close the session, so whatever filesystem changes had been made in that session are now unrecoverable. [26966]

Cloud Edition

- Deselecting a folder from "Selective Sync" does not remove the folder. The folder can be manually removed. [25349]
- The Cloud Edition tray icon may disconnect during high processing scenarios. [26115]
- An error may be received while moving a Dropbox folder to another location. Simply dismiss the dialog to continue. [26396]
- If sharing the same Box account, but have two different computer (both with Cloud Edition and different activated users) and you move the My Box Files folder on one of them, then when you create a new folder on the other computer, it will create "New Folder" and sync that folder along with the newly created folder. [27081]

Resolved Technical Advisories v8.0.1

Encryption

- The issue of some computers experiencing a blue screen under extremely heavy load is resolved. [27366]

Resolved Technical Advisories v8.0

Encryption

- To reduce the chances of DPAPI authentication failure, the registry is now notified of cached credential changes.
- Deleting a file to the recycle bin during an encryption sweep no longer causes the wait notification pop-up to sit on-screen the duration of the sweep. [25987]
- To avoid Windows update failures, %SYSTEMROOT%\SysWOW64 was added to the hard-coded SDE exclusion list. [26475]
- The runtime error in EmsServiceHelper.exe has been resolved. [26545]
- EMS no longer blocks access to slaved Shield-encrypted drives. [26671]
- The Port Control feature for "PCIe" has been renamed to "Express Card Slot". [23446]

Cloud Edition

- The issue of Cloud Edition creating extra folders in the cloud when a folder is created locally is resolved. [26048]
- When using Box, the issue of Cloud Edition adding multiple help files up to the cloud is resolved. [26048]
- The issue of several commas being added to the *networkprovider* registry key upon uninstallation and reinstallation of Cloud Edition is resolved. [26053]
- When uploading or downloading a file through the browser, the "1. How to Access Secure Files..." help file now properly displays only one time. [26076]

Technical Advisories v8.0

Encryption

- EMS cannot be used side-by-side with most third-party USB device encryption solutions, whether hardware or software. To use EMS, either add your third-party USB device to your whitelist, or remove the third-party encryption software.
- When the local console is left open and the computer sleeps, a message displays that "no fixed storage is found." Closing and re-opening the local console corrects the issue. If the local console cannot contact its internal server because the computer is sleeping, it correctly displays this message.
- When uninstalling Personal Edition, an error may display stating, "An error occurred while trying to uninstall DDP|CSF." You may safely dismiss this error. The application will refresh, and Client Security Framework (CSF) will be properly uninstalled. [26866]

Cloud Edition

- If multiple users activate Cloud Edition and then access a folder at the same time that has already been shared between them all, they will all try to encrypt those files independently, creating multiple conflicting files.

Technical Advisories v7.7

Encryption

- Due to a Windows operating system update that interacts with the Dell Data Protection PCS driver, DVD media fails to be formatted/burned when PCS is set to UDF only. *CD and USB media are not affected*. [24833]

Resolved Technical Advisories v7.2.3

Encryption

- SDE recovery triggered by changes to the registry no longer occur.
- Performance tuning enhancements were made in this release to improve hibernation file decryption performance.
- Improvements have been made to External Media Edition to improve handling of inaccessible system files, such as locked or read-only autorun.ini file. [22100]
- When a computer is equipped with a Hardware Crypto Accelerator that is operational and owned, it is not required to use HCA policies, although it is a best practice. File/folder encryption policies optionally can be used in addition to HCA policies. [23541]
- When using DropBox, syncing of the CredDB.cef file now works as expected. [23667]
- When using External Media Edition and there is not enough space on the media to complete an encryption sweep, a dialog now displays that alerts the user that one or more files were not able to be encrypted. [23675]
- When uninstalling External Media Edition, all External Media Edition system files are properly removed. [23768]
- When cutting/pasting a file from Windows Explorer to EMS Explorer, the file is now properly "cut" from Windows Explorer as expected. [24040]
- The "Open" command from the EMS Explorer right-click menu has been removed. [24040]
- File corruption issues related to an Intel update to the CPU IPP libraries no longer occur. [24086]
- Changes were made to the SDE key unlock mechanism to accommodate processors that reflect battery life in CPU ID. [24195]
- Improvements have been made to timing issues related to start up that resulted in blue screens. These issues occurred rarely, but were serious in nature. [24212]
- When using HP Trim (which is an internal cloud sharing/collaborative file repository) file corruption issues no longer occur. [24250]
- The issue of "Double Fault (NO_MORE_IRP_STACK_LOCATIONS BSOD)" have been resolved. This problem occurred because a Microsoft driver assumed that no more than three file-system drives are in use at the same time. New logic has been implemented to correct the issue. [24477]

- Rare instances of computers failing to resume after hibernation have been addressed. [24571]
- When running the Shield on a computer that has recently updated to the latest version of McAfee Virus Scan 8.7 Patch 5, McAfee Virus Scan 8.8 Patch 1, or McAfee HIPS 8.0 Patch 1, files can become corrupted.

  The issue is that the McAfee driver is being injected below Dell Data Protection | Encryption in the filter stack. Microsoft has confirmed that there is an problem in the automatic ordering of the drivers when mini-filters and legacy file system filter drivers are present. Microsoft has also approved our approach of introducing a pass-through mini-filter driver at higher altitude/class to resolve the issue. This issue is not specific to Dell and was reproduced at Microsoft using only the samples from the Driver Development Kit. Other backup and encryption vendors affected by McAfee's patches are also using the same approach to resolve the issue.

  To resolve this issue, remove the McAfee software patches listed above, restart the computer, and install Dell Data Protection | Encryption v7.2.3. [24085]
- Previously, when waking from a sleep state, a "No fixed storage is found" message was displayed in the local console under the System Storage tab on some X4 and ACER platforms. This issue has been resolved. [24581]

Technical Advisories v7.2.3

Encryption

- Under some circumstances, the local console "compliance status" displayed for the eSATA port may be different than the actual status. To resolve the issue, reboot the computer.
- On some Dell platforms, the desktop background turns black after the computer wakes from a sleep state. To work around this issue, go to display settings and reset the desktop background. [24574]

Technical Advisories v7.2.1

Encryption

- When using a *desktop computer* and attempting to block SD card ports by using the "Port: SD" policy, blocking SD ports will not be successful. For *desktop computers*, the "Storage Class: External Drive Control" policy must be used to effectively block SD ports. The use of the "Storage Class: External Drive Control" policy blocks access to all external storage devices irrespective of what bus they are on. When using a *laptop computer*, SD ports can be blocked using the "Port: SD" policy. [23530]
- The F8 "discard the hibernation data" option *MUST* be used on the first system restart after software HCA decryption (using the recovery tool/bundle) is performed on a system drive that contains a valid hibernation file. HCA maintains a drive state value that identifies what drives are encrypted. Because of this, during hibernation resume, HCA attempts to decrypt data that is read from the disk and encrypt data that is written to the disk (this transition in the hibernation file causes disk corruption). Instructions: 1. Allow HCA decryption to complete. 2. During the first reboot after HCA decryption, before the operating system loads, press F8 and select "discard the hibernation data". The user can now resume normal operation of the computer.
- When using a computer equipped with a Hardware Crypto Accelerator, the Preboot Password Requirement dialog that is displayed is misleading regarding Hardware Crypto Accelerator usage. The message will be changed in the next major release to display: "A recent policy update requires the initial setup of the preboot authentication system. To enter the BIOS setup, reboot and click F2 during the Dell splash screen. Go to the "Security" option and select Preboot Authentication > Set System Password. Enter a password and exit the BIOS setup." [23205]
- When the Hardware Crypto Accelerator has used all of its lifecycles, the Shield erroneously asks the user for their Hardware Crypto Accelerator Password and Preboot Password. The message should notify the user that the computer does not have any remaining lifecycles and to contact their Administrator to get a replacement Hardware Crypto Accelerator. We expect this scenario to rarely occur. [22492]
- Amended 01/2014 - When using VMware, if the host computer is Shielded (essentially meaning that the port control drivers are installed on the host), when a user connects a USB device to their computer, and forces it to connect to the OS running on the VMware computer instead of the host OS, the VMware OS will not be able to access the files on the USB. The Dell port control driver is a filter driver running on USB stack. VMware is not compatible with USB filter drivers. For more information, see VMware KB article: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1016809. [20280, 22820, 28522]
- When using Windows Vista (x86 or x64), the Shield failed to load the user's profile. To workaround this issue, reboot the computer. [23496]

- The Encryption Removal Agent can decrypt files with path lengths up to 256 characters. Files paths longer than 256 characters result in a decryption failure. To work around this issue, shorten the path length to less than 256 characters and re-initiate the Encryption Removal Agent. [23474, 23510]

Technical Advisories v7.2

Encryption

- When scanning very large files on removable media, there is a slight screen refresh delay between the local console and the External Media Edition dialog that displays the files name that are being processed. No loss of functionality is experienced. [23453]
- When ejecting removable storage without clicking the "safely removing devices" option in the system tray, the local console status line briefly flashes the "Not Attached to the Encryption System" message. The status resolves to the correct status within a second or two. This is slight screen refresh delay between the local console and External Media Edition. No loss of functionality is experienced. [23454]
- Repeatedly switching between multiple users and using fast user switching will eventually result in Dell Data Protection | Encryption becoming unmanaged. To identify if you are experiencing this issue, you will get a message from the local console stating the "Connecting to Dell Data Protection | Encryption..." message, however, the connection will never be made. A computer restart corrects the issue. [23448]
- System Restore is not a full backup/restore utility. Only the following are restored when using System Restore:

  Registry

  Profiles

  COM+ DB

  WFP.dll cache

  WMI DB

  IIS Metabase

  File types which are monitored by System Restore are as specified in http://msdn.microsoft.com/library/en-us/sr/sr/monitored_file_extensions.asp. Using System Restore on any of these files which are encrypted by Dell Data Protection | Encryption can potentially cause corruption. Backup and restoration of Shield-encrypted files should be done at the folder level and not on an individual file basis. [23437]

Workarounds

Before you begin, be aware of the following workarounds that have been identified during testing.

- Performing an upgrade during an encryption sweep may prevent the Shield Service from restarting normally after the installation finishes. A system restart corrects this issue. To work around the issue, we recommend upgrading when no encryption sweep is running. [14344]
- Encrypted data must be backed up while its owner is logged in. If encrypted files are backed up to an unencrypted location, the result is an unencrypted backup. To work around this issue, back up encrypted data while its owner is logged in. [3139, 11389, 12479]
- When Dell Data Protection | Encryption is installed, Guest accounts work properly, and Guest user account data is deleted at logoff, but Guest user account folder structures (located in the Windows user hives, normally Documents and Settings) may not be deleted at logoff. Because the data is deleted, the folder structures take up very little disk space. If this happens, you can work around the issue by having an administrator delete the excess folders periodically. [8900]
- If a user adds or removes smart card reader hardware without rebooting the Windows smart card, Dell Data Protection | Encryption may not properly recognize authentication. If this happens, the Dell Data Protection | Encryption prompts for alternate authentication. To work around this issue, reboot the Windows device. [9135]

Software and Hardware Compatibility

Personal Edition is tested with third-party software and hardware as needed. Dell reports problems found during testing to other vendors, where appropriate.

Upgrade to the Windows 10 Anniversary Update

- To upgrade a computer running the Encryption client to the Windows 10 Anniversary Update version, follow the instructions in the following article: http://www.dell.com/support/article/us/en/19/SLN298382.

Aventail Access Manager

- Aventail Access Manager is not supported with the Encryption client on Windows 10 computers. [DDPC-4335]

Norton 360

- On computers running Norton 360, the PC Tuneup option to remove Windows Temporary Files must be disabled during Dell Data Protection installation. Installation fails if Windows Temporary Files that are used by the installer are removed. After installation is completed, the PC Tuneup option can be re-enabled. [28732]

Norton Ghost

- The Encryption client is compatible with Norton Ghost 10.0. However, Ghost implements several file restore workflows, and not all of them are recommended with the Encryption client.

  The preferred method to recover files from a Ghost image is the Advanced Explore Recovery Points. Consult the Ghost documentation for instructions. [10574]

AVG Antivirus Protection

- On UEFI computers running the Windows 10 Fall Update and AVG Antivirus, Advanced Authentication installation is interrupted and never completes. [CSF-1192]

Kaspersky Anti-Virus Protection

- On computers running both the Windows 10 Fall Update and Kaspersky Anti-Virus, installation is blocked and never completes. [CSF-1223]

Windows Devices

- Whole-disk compression is not supported with the Encryption client.
- The Volume Shadow Copy Service provides the backup infrastructure for Microsoft Windows XP, Microsoft Windows Server 2003, and Vista operating systems, as well as a mechanism for creating point-in-time copies of data known as shadow copies. Although the Encryption client is compatible with other file backup mechanisms, it is not fully compatible with the Volume Shadow Copy Service, and may cause log files to fill quickly and use more than normal CPU resources. [11744]

Synaptics TouchPad

- Random system errors may be caused by not having an updated Synaptics TouchPad driver when the Encryption client is installed. To correct this issue, download a driver update from http://www.synaptics.com. [10228]

McAfee Host Intrusion Detection

- When using the Shield and McAfee HID, McAfee HID may prevent the Encryption client from changing the registries and Services. To work around this issue, add the Encryption client to the McAfee HID trusted applications list.

Webroot

- Webroot is not compatible with the Encryption client, with Webroot in its default installation. Webroot places several Encryption client files in quarantine, resulting in the client being unable to access the files for encryption/decryption. However, Webroot users can add the Encryption client to the Webroot whitelist to prevent quarantine problems. See Webroot support for instructions.

Hacks and Utilities

- Hacks or utilities that alter device manufacturer performance specifications are not supported. For example, the AfterBurner hack adjusts the clock speed of a device processor, affecting the results of certain math operations. Because some of these math operations are required for encryption and decryption, using this hack could lead to data corruption.