Dell Data Security

Encryption Enterprise Technical Advisories v8.17.1

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2018 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Registered trademarks and trademarks used in the Dell Encryption, Endpoint Security Suite Pro, Endpoint Security Suite Enterprise, and Data Guardian suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of Dell EMC. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. This product uses parts of the 7-Zip program. The source code can be found at 7-zip.org. Licensing is under the GNU LGPL license + unRAR restrictions (7-zip.org/license.txt).

Encryption Enterprise Technical Advisories

2018 - 01

Rev. A03

Contents

1

Technical Advisories

Encryption Enterprise enables an enterprise to support a mobile workforce with the peace of mind that sensitive information is secure.

Contact Dell ProSupport

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

Additionally, online support for Dell 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 Tag or Express Service Code available when you call.

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

New Features and Functionality v8.17.1

- FDE is now supported with smartcard preboot authentication on supported Dell computers running in UEFI boot mode
- FDE is now supported on non-English operating systems:
  - EN - English
  - JA - Japanese
  - ES - Spanish
  - KO - Korean
  - FR - French
  - PT-BR - Portuguese, Brazilian
  - IT - Italian
  - PT-PT - Portuguese, Portugal (Iberian)
  - DE - German
- FDE is available for beta testing in non-production environments on Dell computers running legacy boot mode.
- FDE encryption drivers are now compatible with HVCI .

Resolved Technical Advisories v8.17.1

Encryption Enterprise for Windows

- Italian translations have been corrected for the Home/Advanced tab names. [DDPC-5825, DDPC-5826]
- An issue that resulted in a the computer becoming unresponsive when Dell Encryption and Symantec Endpoint Protection were installed on the same device has been resolved. [DDPC-7808]
- An issue causing the smart card login to fail when the smart card certificate information in the registry missing has been resolved. [DDPC-7904]
- An issue resulting with an error message of "Unable to generate catalog" after an upgrade from Redstone 2 to Redstone 3 with encryption client installed has been resolved. [DDPC-7946]

Preboot Authentication

- An issue where a popup notification would warn the user to not to turn off the computer during PBA configuation has now been resolved. [DDPC-7019]
- PBA now shows the smart card certificates and smart card PIN labels. [DDPC-7066, DDPC-7976]
- An issue where PBA would crash when a smart card was plugged in after PBA loaded has been resolved. [DDPC-7676]

Full Disk Encryption

- An issue where the Windows logo screen was taking a few minutes to appear after FDE had been activated with the machine set to hibernate and then authenticated on PBA has now been resolved. [DDPC-7804]
- An issue where Full Disk Encryption authenticated back to PBA after a combination of multiple restarts and multiple hibernations during encryption has now been resolved. [DDPC-7850]

Technical Advisories v8.17.1

Encryption Enterprise for Windows

- The Dell Data Security Console no longer shows Protection or encryption status for Policy-Based encryption. [DDPC-7046]
- In some cases, a device may not show in compliance after sweep completes. The current workaround is to reboot the device. [DDPC-7977]
- The following folders are suggested to be added as exclusions to Policy Based Encryption to prevent conflicts with Windows Updates.
  - C:\ProgramData
  - C:\Program Files
  - C:\Program Files (x86)

  These will be enabled by default in a future release of Dell Encryption. For more information on modifying policy in your Dell Server, please visit:http://www.dell.com/support/article/us/en/19/sln302271/how-to-modify-policies-on-the-dell-data-protection-server?lang=en [DDPC-8037]

Preboot Authentication v8.17.1

- In some cases, the intensity of USB Type C mouse seems to strengthen while user is in PBA on a UEFI machine. [DDPC-7885]
- When PBA is active and a sleep cycle that forces the computer to sleep after 1 min is enabled, the user is unable to login after turning the computer back on. [DDPC-7919]
- When a network cable is unplugged after loading the PBA, there is no IP address captured which causes the server sync to fail. [DDPC-7936]
- The username text is not displayed in French on the PBA screen after FDE has been installed on a UEFI machine. [DDPC-8012]
- When the network cable is disconnected during PBA recovery and then connected after FDE has been activated, the PBA screen on a UEFI machine displays "Loading data please wait" and freezes. [DDPC-8014]
- When FDE has been activated and policy "check for PBA commands" has been applied, a lock command on the PBA screen appears after the machine has been restarted. [DDPC-8021]

SED Management v8.17.1

- Currently, an error message of "Unhandled exception has occurred in your application" appears during an upgrade of Digital Persona's Auth when the Dell Data Security Console is also open during the upgrade. [DDPC-7836]

- The Oberthur chip only smart card ID-One COSMO V7.0 is read by the PBA but fails to log in on a UEFI machine. [DDPC-7985]
- In some cases, Smart card readers are not detected on legacy machines. [DDPC-8030]

Full Disk Encryption v1.1

- Currently, an error message of "Unhandled exception has occurred in your application" appears during an upgrade of Digital Persona's Auth when the Dell Data Security Console is also open during the upgrade. [DDPC-7836]
- The username text is not displayed in French on the PBA screen after FDE has been installed on a UEFI machine. [DDPC-8012]
- When the network cable is disconnected during PBA recovery and then connected after FDE has been activated, the PBA screen on a UEFI machine displays "Loading data please wait" and freezes. [DDPC-8014]
- If the primary partition on the disk is over 1.5TB, FDE activation fails. [DDPC-8020]
- When FDE has been activated and policy "check for PBA commands" has been applied, a lock command on the PBA screen appears after the machine has been restarted. [DDPC-8021]

Legacy Boot Mode FDE

For beta testing in non-production environments

- The system fails to boot to Windows and results with a black screen after activating PBA and logging in after a reboot. [DDPC-6915]
- When booting to a Windows 7 machine after activating PBA, the machine becomes unresponsive. [DDPC-7496, DDPC-7796]
- Operating system Feature updates are not supported with Full Disk Encryption. [DDPC-7527]
- In some cases, there is a longer than usual delay when switching between PBA Authentication and Windows login screen on a Windows 7 machine. [DDPC-7677]
- Touchpad becomes unresponsive after a PBA activation. [DDPC-7758]
- Currently, a message of " Missing OS" appears after FDE has been activated and machine has been rebooted. [DDPC-7806]
- After authenticating PBA on a HP Elitebook machine, the PBA screen repeatedly asks for user credentials. [DDPC-7852, DDPC-8032]
- In some cases, SSO to Windows issues appear in Legacy FDE. [DDPC-7926, DDPC-7944]
- When Legacy full disk encryption is in preview, multiple disks in the system may cause partitioning failures. The workaround is to remove the secondary disk. Currently, multi-disk support is not available for Full Disk encryption. [DDPC-7986]
- After enabling FDE and activating PBA on a machine with a non-SED drive, the machine is unable to detect the hard drive. [DDPC-7999]

Bitlocker Manager v8.17.1

- Currently, an error message of "Unhandled exception has occurred in your application" appears during an upgrade of Digital Persona's Auth when the Dell Data Security Console is also open during the upgrade. [DDPC-7836]
- The policy line of: <PasswordUse MinimumPasswordLength="8" PasswordComplexity="Allow" Usage="Allow" />
  is forcing a secondary drive, which the D: drive is being seen at, to unlock with a password. Before the password unlock, this volume is not mount-able. It seems that once this is unlocked, the shield is not properly seeing this drive being mounted as a "Fixed disk", even though PCS is classifying it as:

  [01.15.18 15:03:37:219 PCSInfoLogger: 53 D] [PCSQuery] Retrieved drive information from PCS driver. DeviceType: 0, Device Class: 0, Device ID: SCSI\Disk&Ven_HFS512G3&Prod_9MND-3520A\4&9e95efc&0&000200

  The workaround is to change the BitLocker Policy under the Fixed Disks to: Configure Use of Passwords for Fixed Data Drives and setting this to "Disallow". The disk will use the TPM settings for the OS disk to provision a protector instead of the password that is user-defined. [DDPC-8002]

New Features and Functionality v8.17

- Added 01/2018- Dell's Preboot Authentication environment for Self-Encrypting Drive and Full Disk Encryption now has built-in resiliency. If the data-store for user credentials in the PBA becomes corrupted, it will revert to a known-good database. This can be manually initiated by holding the Control and Alt keys, and then pressing 'b' on the keyboard.
- The Encryption client is now supported with Windows 10 Fall Creators Update (Redstone 3 release). Upgrades to Fall Creators Update are now supported.
- The Preboot Authentication is now supported with Windows 10 Fall Creators Update (Redstone 3 release). Upgrades to Fall Creators Update are now supported.
- The Encryption client local console now shows status of "In Compliance" when there are no pending policies and an initial sweep is complete, regardless whether the Encryption policy is enabled on the Dell Server.
- System-created files in the \Windows folder are no longer encrypted, regardless of policy settings. This behavior can be changed by adding a Category 3 inclusion to SDE Encryption Rules.

Resolved Technical Advisories v8.17

Encryption Enterprise for Windows

- An issue that resulted in Windows Explorer crashing when logged into a domain user account has been resolved. [DDPC-4620]
- An issue that resulted in the Port Control Policy for USB ports to not work properly when connected to a TB-16 dock has been resolved. [DDPC-7446]
- Encryption External Media can now be uninstalled through the Apps list in Windows 10. [DDPC-7465]
- SDE contents are now decrypted after SDE has been turned off on an encrypted machine. [DDPC-7574]
- An issue resulting in an error message "Invalid Value for 100" on the local client when character limit had been exceeded for EMS whitelisting policies has been resolved. [DDPC-7602]
- An issue that resulted in a hibernation when the Secure Hibernation Policy was turned on has been resolved. [DDPC-7906]

Preboot Authentication

- An issue that resulted in Preboot Authentication login failure when the Dell Security Management Server is unavailable has been resolved. [DDPC-4503, DDPC-4505, DDPC-7181]
- An issue that resulted in Encryption Enterprise users to lock their screen at PBA activation for the Sync Users at PBA Activation policy has been resolved. [DDPC-6924]
- An issue that resulted in a popup notification that warned the user to not turn off the computer during PBA configuration has been resolved. [DDPC-7019]
- An issue that resulted in an inability to log in at Preboot Authentication after shutting down the computer during PBA synchronization. [DDPC-7336, DDPC-7584]
- An issue that resulted in an error message in PBA after replacing motherboard hardware or resetting the TPM has been resolved. [DDPC-7337]

Technical Advisories v8.17

All Clients

- No Technical Advisory exists for all clients

Dell Encryption v8.17

- During recovery, volumes may not display. If this occurs with the recovery tool option "My system fails to boot and displays a message asking me to perform SDE Recovery," follow these steps:
  a Run the following command, from the location of the LSARecovery key: ...\'LSARecovery.exe' -x 1 -p password1 -d C:\users
  b Copy CMGKRcvr.txt from C:\users\ to C:\
  c Restart the computer.

If volumes do not display with the recovery tool option "My system does not allow me to access encrypted data, edit policies, or is being reinstalled," follow instructions in Encryption Enterprise Advanced Installation Guide, Uninstall Encryption, and select Encryption Removal Agent installation to decrypt files. After decryption is complete, reinstall the Encryption client. If files must be temporarily accessed but remain encrypted, follow instructions in Dell Data Security Recovery Guide, Encrypted Drive Data Recovery, to run the Administrative Unlock (CMGAu) utility.

[DDPC-7794]

Preboot Authentication v8.16.1

- Upgrade from Windows 7 to Windows 10 Fall Creators Update (Redstone 3 release) is supported according to Microsoft's supported upgrade paths. For more information, seehttps://docs.microsoft.com/en-us/windows/deployment/upgrade/windows-10-upgrade-paths

SED Management v8.16.1

- Upgrade from Windows 7 to Windows 10 Fall Creators Update (Redstone 3 release) is supported according to Microsoft's supported upgrade paths. For more information, seehttps://docs.microsoft.com/en-us/windows/deployment/upgrade/windows-10-upgrade-paths

Full Disk Encryption v1.1

- FDE is not supported on the Dell Optiplex 5055, XPS 13 9365, or Latitude 5495. [DDPC-7970]
- When Legacy full disk encryption is in preview, multiple disks in the system may cause partitioning failures. The workaround is to remove the secondary disk . Currently, multi-disk support is not available for Full Disk encryption. [DDPC-7986]

BitLocker Manager v8.16.1

- When upgrading the Dell Bitlocker Manager and using a PIN for authentication, the user may be re-prompted to re-set the PIN on the endpoint. [DDPC-7649]
- Upgrade from Windows 7 to Windows 10 Fall Creators Update (Redstone 3 release) is supported according to Microsoft's supported upgrade paths. For more information, seehttps://docs.microsoft.com/en-us/windows/deployment/upgrade/windows-10-upgrade-paths

New Features and Functionality v8.16

- Encryption Enterprise now supports TLS 1.2 when used with a Dell Server v9.9 or newer.
- Encryption Enterprise now supports IPv6.
- Full Disk Encryption is now optionally available with Encryption Enterprise for Dell computers running in UEFI boot mode with non-SED drives. Full Disk Encryption provides administrators central management of Preboot Authentication in addition to disk encryption, with the capability to remotely disable endpoint login and lock the device. Keys are protected with the Trusted Platform Module (TPM), preventing access to encrypted data in the event that the hard drive is removed from the computer.

- The Data Security Uninstaller is now included in all installation bundles. This utility gathers the currently installed products and removes them in the appropriate order. For more information, see http://www.dell.com/support/article/us/en/19/sln307791.
- Password Manager has reached End of Life. For more information, see http://www.dell.com/support/article/us/en/19/sln305349.

Resolved Technical Advisories v8.16

All Clients

- The following issues are now resolved after an encryption sweep with the Secure Post-Encryption Cleanup policy set to an Overwrite value: The Local Management Console becomes unresponsive; File Explorer filename sorting is not functioning; or Skype displays unrecognized characters. [DDPC-5764]

Encryption Enterprise for Windows

- An issue that resulted in Encryption External Media leaving some files unencrypted and renamed is resolved. [DDPC-1532]
- The Windows 10 Feature Update preparation phase will no longer fail to stop the sweep state and will not fail on updating the registry on a computer running Encryption External Media. [DDPC-4254]
- Encryption sweeps no longer pause or require manual intervention to complete. [DDPC-4499]
- Pausing encryption from the system tray icon now properly pauses the encryption sweep. [DDPC-5372]

Resolved Customer Issues

- Windows now properly resumes from hibernation when the Secure Windows Hibernation File policy is enforced. [DDPSUS-1346]
- An issue that resulted in failed activation when a user's domain did not match the managed domain is resolved. [DDPC-5378]
- Registry keys are now properly removed at uninstall. [DDPC-5410]
- Server Configuration Tool logs are now included in DiagnosticInfo. [DDPC-6114]
- An issue that resulted in failed activation of endpoints is resolved. [DDPC-6119]
- An issue that resulted in the Port Control System causing intermittent BSOD during upgrades is resolved. [DDPC-6357]
- An issue resulting in BSOD when resuming from hibernation using an NVMe drive in AHCI is resolved. [DDPC-6456]
- An issue is resolved that resulted in customized Encryption External Media dialogue boxes to display incorrectly. For more information, see http://www.dell.com/support/article/us/en/19/sln302925. [DDPC-6537]
- Applications using Microsoft's Encrypted File System no longer conflict with Policy Based Encryption. [DDPC-6846]
- A USB 3.0 driver causing BSODs when interacting with Dell Encryption is resolved. [DDPC-6893]
- Encrypt for Sharing files created on a 64-bit computer now open on a 32-bit computer. [DDPC-6998]
- An issue that resulted in BSOD after enabling HyperVisor is resolved. [DDPC-7028]

SED and FDE Preboot Authentication

- Inserting a smart card for PBA login on the OptiPlex 3240 All-In-One now functions as expected. [DDPC-5907]
- Keys on Canadian French and British/English keyboards now function as expected on computers running in UEFI mode. [DDPC-5969, DDPC-5369]

Resolved Customer Issues

- An issue that resulted in an incorrect error message displaying after smart card authentication failure is resolved. [DDPC-6578]

SED Management v8.16

Resolved Customer Issues

- An issue that caused the Local Management Console to become unresponsive following successful Policy-Based Encryption is resolved. [DDPC-5176]

BitLocker Manager

No Resolved Technical Advisories exist.

Technical Advisories

Dell Encryption v8.16

- During installation, when entering the address as part of the SERVERHOSTNAME, it must be surrounded by brackets when using IPv6. In this scenario, a port number cannot be included as it cannot be resolved as part of the address. [DDPC-7036]
- In some cases, the Port Control Policy for USB ports may not work properly with USB ports on a connected TB-16 dock. To work around this issue, set policy for the USB devices instead of the USB ports. For example, set the Windows Port Control Storage policy to Disabled on the Dell Server. [DDPC-7446]
- Encryption External Media cannot be uninstalled through the Apps list in Windows 10. To remove the application, uninstall through Programs and Features. [DDPC-7465]

PBA Advanced Authentication v8.16

- The popup notification that warns the user not to turn off the computer during PBA configuration may persist. If this occurs, to suppress all popup notifications, set the PbaToastersAllowClose registry value to 1 in the following location:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" = DWORD:1

  0=Enabled (default)

  1=Disabled

  [DDPC-7019]
- Advanced Authentication options display only under the following conditions:
  - When upgrading to v8.16 with the PBA inactive, Advanced Authentication options display at the Windows login screen upon the first reboot after installation of v8.16. After the next reboot, Advanced Authentication options display only if PBA is activated.
  - When upgrading to v8.16 with the PBA active, Advanced Authentication options display at the Windows login screen upon the first reboot after installation of 8.16.
  - After a clean install of v8.16, Advanced Authentication login options will not display until the PBA is activated. [DDPC-7087]
- When installing Advanced Authentication to a non-default directory, files will still be written to the default location of **C:\Program Files (x86)\Dell\Dell Data Protection\Authentication\bin**. These files must remain at this location. Files being written to multiple locations will not affect functionality. [DDPC-7128]
- With Preboot Authentication enabled for Full Disk Encryption or Self Encrypting Drive technologies, booting into the preboot environment or manually syncing server communication may fail if the Dell Security Management Server is unavailable but listening on the remote port. [DDPC-7181]

Preboot Authentication v8.16

- Encryption Enterprise users who have the Sync Users at PBA Activation policy will have to lock their screen at PBA activation. To do this, select the **Lock Now** option on the notification. If locking via some other method (Ctrl+Alt+Delete), users will still need to lock their screen via the **Lock Now** option. If you use the **Lock Now** option, only a single lock/unlock cycle is required. [DDPC-6924]

SED Management v8.16

- The Latitude 5289 does not support SED Management. [DDPC-7144]

Full Disk Encryption v1.0

- The Latitude 5289 does not support Full Disk Encryption. [DDPC-7144]
- Full Disk Encryption is supported in managed configuration only. [DDPC-7208]
- Full Disk Encryption is not supported with BitLocker or BitLocker Manager. Do not install Full Disk Encryption on a computer on which BitLocker or BitLocker Manager is installed. [DDPC-7311]
- After replacing motherboard hardware or resetting the TPM, the PBA delays several minutes then displays the error: "Device is locked, please contact your administrator". To work around this issue, decrypt the endpoint encrypted with Full Disk Encryption. [DDPC-7337]
- Full Disk Encryption requires a 180 Mb partition at the end of the drive to write the Preboot Authentication environment to the local disk. The sectors used for this partition are stored within the registry for tracking within the host operating system and the Preboot Authentication environment. If the 180 Mb partition is removed, the registry key location is: HKLM\software\Dell\Dell Data Protection \PBA.

  This key and it's sub-key can be safely deleted if the Preboot Authentication environment is not in place. [DDPC-7453]
- Operating system Feature updates are not supported with Full Disk Encryption. [DDPC-7527]
- Full Disk Encryption is not supported with the Encryption client in this release. Do not install Full Disk Encryption on a computer on which the Encryption client is installed.
- Full Disk Encryption is only supported with English operating systems.

BitLocker Manager v8.16

- No Technical Advisories exist.

New Features and Functionality v8.15

- A new policy in Security Management Server/Security Management Server Virtual v9.8 allows the administrator to enable or disable users' ability to select **Remember Me** on the PBA login screen and customize Support dialog text.
- The Encryption client drivers pass the Hypervisor Code Integrity (HVCI) checks.
- Operating system downgrade is now supported with the Encryption client.
- SSL is no longer supported with Advanced Authentication, SED Management, or BitLocker Manager. TLS 1.0, 1.1, or 1.2 should be used rather than SSL.
- Enterprise Edition is rebranded to Encryption Enterprise.
- The Security Tools Mobile application has reached End of Life. For more information, see www.dell.com/support/article/us/en/19/sln305349.

Resolved Technical Advisories v8.15

All Clients

- The user name now displays in the Authentication Required dialog during credential enrollment in the Dell Data Security Console. [DDPC-6013]

Encryption Enterprise for Windows

- Performance of Encryption client upgrade that begins during an encryption sweep is improved. [DDPC-4261]
- The Encryption client now displays the EMS Device Whitelist policy rather than an error when the policy setting exceeds 2048 characters. [DDPC-4382]
- The Local Management Console Preferences setting, **Indicate encryption status using Windows Shell Extension icon overlays**, is removed. Previously, the setting was present, but icon overlay behavior is controlled by Dell Server policy rather than the local setting. [DDPC-5227]
- An issue is resolved that caused the Encryption Removal Agent to occasionally become unresponsive during decryption. [DDPC-5583]
- Encrypted files can now be accessed after operating system downgrade. [DDPC-5676]
- The Encrypt for Sharing dialog no longer continues to display after the user locks the Dell Latitude 5289. [DDPC-5719]
- Communication between a client server running Encryption and the Dell Server is hardened.

Resolved Customer Issues

- An issue is resolved that resulted in unresponsiveness of the computer following hibernation. [DDPC-1475]
- An issue is resolved that caused the computer to become unresponsive, followed by a Windows bugcheck. [DDPC-2349, DDPC-3284]
- Two issues are resolved that led to errors in applications that were running during an encryption sweep. [DDPC-2751, DDPC-4444]
- After upgrade to Windows 10, a second restart is no longer required in certain cases for encryption to resume. [DDPC-4080]
- The computer now restarts after Port Control policies are enabled or updated. [DDPC-5255]
- Diagnostic Info performance and error messaging are improved. [DDPC-5559]
- File names on the Start menu are now correctly translated into French. [DDPC-5895]

Preboot Authentication

Resolved Customer Issues

- An issue is resolved that resulted in pop-up messages persisting rather than closing. [DDPC-3604]

Enterprise Edition for SED

- The Crypto Erase Password policy now cryptographically erases the SED, deletes the authentication tokens for all users, and locks the SED. Afterward, only an administrator can forcibly unlock the device. [DDPLP-370, DDPC-5472, 26862]

BitLocker Manager

- An issue is resolved that caused a BitLocker encryption delay, with the log message "volume C: waiting on SED status to be reported," on a computer running Dell Encryption. [DDPC-4840]

Resolved Customer Issues

- An issue is resolved that related with Microsoft platform validation profile changes that prevented BitLocker encryption from beginning on Windows 10. [DDPC-5790]

Technical Advisories v8.15

Encryption Enterprise for Windows

- The Secure Hibernation policy is not supported with Legacy BIOS on Windows 7. [DDPC-2279]
- Encryption status displayed in the Dell Data Security application for a fixed or removable drive may differ from the actual status of the drive, which is correctly displayed in the Local Management Console.

[DDPC-5521, DDPC-5670]

- Encryption is not supported on servers that are part of distributed file systems (DFS). [DDPC-6130]
- If the CmgHiber.sys or CmgHiber.dat file is missing from C:\windows\system32\drivers on a computer that hibernates, the computer will not resume. Ensure that disk cleaner and optimization tools do not delete these files. [DDPC-6211]
- When removable media is connected to a computer running Windows 7, 8, or 8.1 with the Subclass Storage: External Drive Control policy set to Blocked, the device name is not included in the access-blocked message or in the Local Management Console. [DDPC-6503]
- Encrypted user and common data on a computer with an HCA card is unrecoverable if the user clears HCA ownership, even though the computer is not HCA-encrypted, because the user and common keys are wrapped in the GPE (HCA) key. [DDPC-6505, DDPC-6535]
- A file may become corrupted on USB external media provisioned with Encryption External Media when the file is created, edited, and reopened on both Windows and Mac computers. [DDPC-6592]

Advanced Authentication

- SSL is no longer supported. TLS 1.0, 1.1, or 1.2 should be used rather than SSL.

Preboot Authentication

- A few keys on Canadian French and British/English keyboards behave differently than expected on computers running in UEFI mode. [DDPC-5369, DDPC-5969]

- An intermittent "System Failed" error may display after inserting a smart card for PBA login on the OptiPlex 3240 All-In-One. [DDPC-5907]
- A few keys on a Brazilian Portuguese keyboard behave differently than expected on the Dell Precision M4800 running in UEFI mode. [DDPC-5975]
- A delay in display of the PBA login screen has been observed on the following Dell computers: Optiplex 5055, Precision 5820T, Precision 7820T, and Precision 7920T. [DDPC-6375]
- Recovery of a SanDisk X300 drive with the Recovery All bundle succeeds but may require up to two minutes to complete. [DDPC-6389]
- The backslash/pipe (\ |) key on an Arabic behaves differently than expected. [DDPC-6529]
- SSL is no longer supported. TLS 1.0, 1.1, or 1.2 should be used rather than SSL.

Enterprise Edition for SED

- SSL is no longer supported. TLS 1.0, 1.1, or 1.2 should be used rather than SSL.

BitLocker Manager

- The Local Management Console does not report status of a drive that is both Dell-encrypted and BitLocker-encrypted when the drive is locked. [DDPC-6329]
- SSL is no longer supported. TLS 1.0, 1.1, or 1.2 should be used rather than SSL.

New Features and Functionality v8.13

- The Encryption client is now supported with the Windows 10 Creators Update (Redstone 2 release).
- BitLocker Manager is now supported with Server 2016.
- Added 5/2017 - Remote PBA management of local user accounts is now available.
- Enterprise Edition is **not** supported with Windows Server 2008 (non-R2 version).
- Secure Lifecycle is rebranded to Dell Data Guardian and is no longer included in Enterprise Edition. For more information about Data Guardian, see http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/research.

Resolved Technical Advisories v8.13

Enterprise Edition for Windows

- An issue is resolved that occasionally resulted in access denial errors for SDE-encrypted files stored in the \users folder. [DDPC-3170]
- An activation issue with Kaspersky Small Office Security installed is resolved after upgrade to the latest version of Kaspersky. [DDPC-3388]
- The Encryption Removal Agent Installation dialog now displays when uninstalling a Deferred Activation Encryption client. [DDPC-3867, DDPC-4004]
- All text now displays as expected in Japanese Encryption Removal Agent dialogs. Previously, some text did not display in one dialog. [DDPC-4159]
- VDI client activation error handling is improved. [DDPC-4474]
- Log files are now collected when Diagnostic Info is run on a server OS. [DDPC-5206]
- Changes to Common Encryption exclusions are now enforced while the user is logged in. [DDPC-5213]

Resolved Customer Issues

- Setting the registry entry, EnableNGMetadata, resolves an issue that resulted in Microsoft update failure on computers with Common key-encrypted data and performance issues related to encrypting, decrypting, or unzipping large numbers of files within a folder.

  Set the EnableNGMetadata registry entry in the following location:

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CmgShieldFFE]

"EnableNGMetadata" = dword:1

0=Disabled (default)

1=Enabled

[DDPC-694, DDPC-794, DDPSUS-863]

- An issue is resolved that resulted in access denial errors for non-domain users. [DDPC-854]
- Decryption performance is improved when SDE Encryption is enabled. [DDPC-3577, DDPSUS-975]
- The Local Management Console now indicates that an SD card is present in the Ports view as well as in the Device view with External Media Edition and the Port Control policy, Port:SD, set to Bypassed. [DDPC-5037]
- An issue is resolved that occasionally caused the Encryption client to become unresponsive with warnings in the log files. [DDPC-5311]

Advanced Authentication

- When a user is removed from a computer just before the computer is shut down, the removal process is now completed as expected. [DDPC-4260]

Resolved Customer Issues

- An issue is resolved that resulted in a delay in displaying the User Account Control prompt. [DDPC-5017]

Preboot Authentication

- Preboot Authentication is supported on the following computers:
  - Latitude 5280
  - Latitude 5480
  - Latitude 5580
  - Latitude E7280
  - Latitude E7480
  - Precision M5520
- The smartcard reader now functions as expected for PBA login on Dell Optiplex All-in-One computers. [DDPC-3465, DDPC-5014]
- With smart card authentication, the **Sign In** button is now enabled after the user enters the smart card PIN. [DDPC-5125]
- The updated domain now displays in the Challenge/Response dialog after the domain is changed on a computer with PBA activated. [DDPC-5132]
- The correct information is now included in the "About" information accessed from the PBA login screen. [DDPC-5178]

Enterprise Edition for SED

- When a user is removed from a computer just before the computer is shut down, the removal process is now completed as expected. [DDPC-4260]

BitLocker Manager

- When a user is removed from a computer just before the computer is shut down, the removal process is now completed as expected. [DDPC-4260]
- Logging is improved. [DDPC-4305]

Technical Advisories v8.13

Enterprise Edition for Windows

- Pausing encryption from the system tray icon does not pause the encryption sweep. [DDPC-5372]
- After policy update that requires reboot, the reboot prompt occasionally displays off-screen on the Dell Latitude 7280. [DDPC-5376]
- Encryption overlay icons display on unmanaged users' files when overlay icons are enabled for managed users on the same computer. [DDPC-5415]
- High resolution prevents use of the recovery option on the Precision Mobile Workstation 7520 and 7720, due to the sizing of the recovery user interface. [DDPC-5421]
- The Local Management Console temporarily displays the messages "No fixed storage is found" and "Not connected to the encryption system" when running the Encryption client on a virtual machine that is paused after an Encryption sweep with the registry entry, EnableNGMetadata, enabled. To immediately work around this issue, close then reopen the Local Management Console. [DDPC-5567]
- On some computers, a file extraction error displays during prerequisite installation. To work around this issue if it occurs, delete files in the \temp folder and resume installation. [DDPC-5582]
- After an encryption sweep with the Secure Post-Encryption Cleanup policy set to an Overwrite value, the following issues may occur: The Local Management Console becomes unresponsive; File Explorer filename sorting is not functioning; or Skype displays unrecognized characters. To work around this issue, add the following exclusion to the SDE Encryption Rules policy: "-^3C:\Windows \Globalization". For information about setting policies, refer to *AdminHelp*, available from the Dell Server Remote Management Console. [DDPC-5764]
- An executable file cannot be run a second time from EMS Explorer if the user runs the file but then cancels the operation at the prompt after entering the EMS password. To work around this issue, close then reopen EMS Explorer and run the file. [DDPC-5781]
- On some computers, Microsoft KB4015219 may fail to install. [DDPC-5789]

Preboot Authentication

- Amended 8/2017 - Preboot Authentication fails with some docking stations and adapters. For a list of docking stations and adapters that are supported with PBA, see www.dell.com/support/article/us/en/19/sln296720/. [DDPC-2693, DDPC-6228]
- On some non-UEFI computers, the touchpad is not functional at the PBA login screen. Functionality resumes when Windows opens. [DDPC-5362]
- On some non-UEFI Dell Latitude computers, the touchpad is not functional after the computer resumes from sleep (S4). [DDPC-5363]
- The error, "No boot device found," may display after PBA activation on some 2017 Dell Latitude and Optiplex computers. For instructions to work around this issue if it occurs, refer to http://www.dell.com/support/article/us/en/19/SLN305978. [DDPC-5705]
- A SED SATA drive may not boot after Legacy PBA login on some 2017 Dell Latitude and Optiplex computers. For instructions to work around this issue if it occurs, refer to http://www.dell.com/support/article/us/en/19/SLN306020/sata-sed-drives-fails-to-boot-the-os-after-pba-authentication?lang=EN. [DDPC-5957]

Enterprise Edition for SED

- Amended 7/2017 - Configuration of self-encrypting drives for Dell's SED management differ between NVMe and non-NVMe (SATA) drives, as follows.
  - Any NVMe drive that is being leveraged as an SED – The BIOS' SATA operation must be set to RAID ON, as Dell's SED management does not support AHCI on NVMe drives.
  - Any NVMe drive that is being leveraged as an SED – The BIOS's boot mode must be UEFI and Legacy option ROMs must be disabled.
  - Any non-NVMe drive that is being leveraged as an SED – The BIOS' SATA operation must be set to AHCI, as Dell's SED management does not support RAID with non-NVMe drives.
    - RAID ON is not supported because access to read and write RAID-related data (at a sector that is not available on a locked non-NVMe drive) is not accessible at start-up, and cannot wait to read this data until after the user is logged on.

- The operating system will crash when switched from RAID ON > AHCI if the AHCI controller drivers are not pre-installed. For instructions on how to switch from RAID > AHCI (or vice versa), see http://www.dell.com/support/article/us/en/19/SLN306460.

Supported OPAL compliant SEDs require updated Intel Rapid Storage Technology Drivers, located at http://www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/drivers.

Dell recommends Intel Rapid Storage Technology Driver version 15.2.0.0 or later, with NVMe drives.

[DDPC-5941, DDPC-6219]

BitLocker Manager

- The top part of the option "Use a password to unlock the drive" is cut off in the BitLocker Drive Encryption dialog. [DDPC-5728]
- Added 8/2017 - Due to changes to Microsoft validation profiles level (PCRs), BitLocker Manager might not begin encrypting on Windows 10. To correct this issue, obtain and apply the Enterprise Server v9.7 update that corrects this issue or upgrade to Security Management Server v9.8. For more information about the v9.7 update, see http://www.dell.com/support/article/us/en/19/sln305948/. [DDPC-5790]

New Features and Functionality v8.12

- Secure Lifecycle now offers the following:
  - Audit events logs can now be exported from the Dell Server to SIEM.
  - Protected Office Mode now protects macro-enabled Office documents (.docm, .pptm, .xlsm).
  - File sharing is improved with introduction of the Full Access List, which replaces the Whitelist and Graylist, in the Dell Server Remote Management Console.
  - Internal users now auto-activate after installation.
  - When Office documents or macro-enabled documents are created on an Android or iOS client that is not connected to the Dell Server, keys are generated offline and then uploaded to the Dell Server the next time the device is online.
  - New geofencing policies for Android and iOS clients allow administrators to restrict protected Office document and .xen file access to a specified region. Regions currently include the United States and Canada.
- Added 4/2017 - The Encryption client is now supported with Windows Server 2016 - Standard Edition, Essentials Edition, and Datacenter Edition.
- Added 4/2017 - BitLocker Manager is now supported with Server 2012 and Server 2012 R2 - Standard Edition and Enterprise Edition (64-bit).
- The PBA user interface has a new look and feel.
- New policies allow the administrator to configure the maximum number of Dell Server connection attempts and the retry interval for the Encryption client running on a server OS.
- 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 Clients

- 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 Enterprise Edition. For more information, see https://support.microsoft.com/en-us/kb/2913763. [DDPC-4257, DDPC-1619, CSF-847]

Enterprise Edition for Windows

- 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]
- Administrative Download Utility (CMGAd) and Administrative Unlock Utility (CMGAu) are now functioning as expected with non-domain users. [DDPC-4109]
- 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]
- Performance is improved on computers running Secure Lifecycle. [DDPC-5113]
- 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]
- Effective policies from the Dell Server are now automatically exported and stored in C:\ProgramData\Dell\Dell Data Protection\Policy \Policy-xxxxxxxx.xml, where "xxxxxxxx" is the sequence number of the policy. By default, the last 10 policies received from the Server are stored. To change the default number of policies stored, change the value of the following registry key. The valid range is 0 - 100.

  ["HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "MaxPoliciesStored" =dword:00000010

  Valid range = 0 - 100

  [DDPC-4583]

Preboot Authentication

- Amended 4/2017 - Preboot Authentication is supported ***only*** with UEFI mode (with and without SecureBoot) on the following computers:
  - OptiPlex 3050 All-In-One
  - OptiPlex 5250 All-In-One
  - OptiPlex 7450 All-In-One
  - OptiPlex 3050 Tower, Small Form Factor, Micro
  - OptiPlex 5050 Tower, Small Form Factor, Micro
  - OptiPlex 7050 Tower, Small Form Factor, Micro
  - Latitude 3180
  - Latitude 3189
  - Latitude 3380
  - Latitude 3480
  - Latitude 3580
  - Latitude 5285
  - Latitude 5289
  - Precision 7520
  - Precision 7720

  - Precision 5720 All-in-One
- When the Dell Latitude 7370 with PBA activated is docked, the user is now prompted at the PBA login screen for the authentication method set by policy rather than the access code. [DDPC-2693]
- An issue with smart card single sign-on that resulted in an error, "User did not sync with PBA," is now resolved. [DDPC-3539]
- An issue is resolved that resulted in brief and intermittent PBA login screen unresponsiveness on a UEFI computer. [DDPC-3753]
- The Options menu now remains anchored to the Options button in the PBA login screen when accessed using **Tab+Enter**. [DDPC-4104]
- After upgrade to the Windows 10 Anniversary Update on non-UEFI computers with PBA activated, the Challenge/Response popup now displays as expected after the user exceeds the maximum allowed attempts to correctly enter the password and answer Recovery Questions. [DDPC-4126]
- An issue is resolved that resulted in a computer with PBA activated reporting No OPAL Drive after resuming from hibernation. [DDPC-4476]
- Keyboard layout changes are now retained on computers with PBA activated. [DDPC-4684]

Enterprise Edition for SED

- When installing SED Management using the child installers, the installation no longer fails if the **Validate URL** button is pressed. [DDPC-4271]
- Effective policies from the Dell Server are now automatically exported and stored in C:\ProgramData\Dell\Dell Data Protection\Policy \Policy-xxxxxxxx.xml, where "xxxxxxxx" is the sequence number of the policy. By default, the last 10 policies received from the Server are stored. To change the default number of policies stored, change the value of the following registry key. The valid range is 0 - 100.

  ["HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "MaxPoliciesStored" =dword:00000010

  Valid range = 0 - 100

  [DDPC-4583]

BitLocker Manager

- Effective policies from the Dell Server are now automatically exported and stored in C:\ProgramData\Dell\Dell Data Protection\Policy \Policy-xxxxxxxx.xml, where "xxxxxxxx" is the sequence number of the policy. By default, the last 10 policies received from the Server are stored. To change the default number of policies stored, change the value of the following registry key. The valid range is 0 - 100.

  ["HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "MaxPoliciesStored" =dword:00000010

  Valid range = 0 - 100

  [DDPC-4583]

Secure Lifecycle

- Encryption sweep performance is improved. [DDPCE-4183]
- An issue is resolved that previously prevented the Save As function in Google Drive to overwrite a protected file with an unprotected update to the file. [DDPCE-4275]

Secure Lifecycle Mobile Application

- The bookmark feature now functions as expected on iOS and Android operating systems. [DDPCE-4124, DDPCE-4160]

Technical Advisories v8.12

All Clients

- BitLocker Manager is selected by default in the Select Features dialog of the installer. To avoid installing BitLocker Manager, clear its check box in the features list. [DDPC-5016]

Enterprise Edition for Windows

- 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]
- The computer becomes unresponsive when Encryption with Deferred Activation is uninstalled using the option to create an Encryption Removal Agent log file. [DDPC-4829]
- When the Encryption client is installed on Windows Server 2016 Standard Edition, the OS/Version field for the Endpoint reads "Unknown/null" in the Dell Server. [DDPC-4836]
- When encryption or decryption is paused, the Compliance/Provisioning status may not be accurately indicated in the Local Management Console. [DDPC-5063]

Preboot Authentication

- Added 4/2017 - Changes to the Self-Encrypting Drive policy, Self Help Question/Answer Attempts Allowed, take effect only for users activating PBA after the policy change and for existing PBA users when the updated policy value is lower than the previous value. [DDPC-4998]
- Smart cards can be provisioned for PBA authentication on UEFI computers but cannot be used for login. This will be corrected in a later release. [DDPC-5062]

Secure Lifecycle

- When a protected macro-enabled document is opened in Excel, the macro cannot be edited from the **Macros** menu. To work around this issue, use **Alt+F11** to open the macro editor. [DDPCE-4418]
- On rare occasion, Secure Lifecycle may display an error when opening or saving protected files. To work around this issue if it occurs, follow these steps:

  a From the Windows Start menu, select **Run**, then enter `services.msc`.

  b Delete the following files from the **C:\Program Files\Dell\Dell Data Protection\Secure Lifecycle** folder:

  XendowData.xdb

  XendowSys.xdb

  xendow.xtc

  c Restart the computer.

  [DDPCE-4420]

- Added 4/2017 - If an external user is blacklisted and later re-activated, to regain access to keys, the user may be required to uninstall then reinstall Data Guardian. [DDPCE-4458]
- When an internal user attempts to grant protected file access to an unprotected file, an error displays rather than a message that the file is unprotected and, therefore, does not need to be shared. [DDPCE-4461]
- After upgrade from Cloud Edition v2.0, issues may occur with certificates and systray application functionality. To work around these issues, follow instructions in *Cloud Edition User Guide* to uninstall Cloud Edition, and then install Secure Lifecycle. [DDPCE-4474]
- A date-protected Word file stored in a mapped drive does not show the date-protection period in **File** > **Info** when the file is opened from the mapped drive. [DDPCE-4566]
- If auto-activation fails, disable auto-activation on the client computer. To disable auto-activation, create the following registry key:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection\Secure Lifecycle]

  "DisableAutomaticActivation" =dword:00000001

  To re-enable auto-activation, delete the registry key.

  [DDPCE-4573]
- Added 4/2017 - A protected Office document cannot be opened from a File Explorer Search result when running Office 2016 on Windows 7. [DDPCE-4577]
- On a computer running Windows 10 and Office 2016, the **Protected Save As** menu item is disabled after setting a date restriction and saving an Excel file. [DDPCE-4587]

New Features and Functionality v8.11

- Enterprise Edition now supports Secure Lifecycle. Secure Lifecycle provides data security, wherever it goes - data at rest, data in motion and data in use - through encryption. Data Loss Prevention (DLP) ensures no data is lost in motion or in flight, while Digital Rights Management (DRM) defines access and usage control. Additionally, file monitoring provides detailed data usage visibility to support forensics needs. Secure Lifecycle provides security, authority, visibility, and cross-platform compatibility - all through a single solution - with the following features:

  - Auditing and reporting on file activity, files synced, files accessed by whom, where and when, and compliance reporting.
  - Geolocation with map visualization as well as multiple filtering options for audit events.
  - Enforcement of whitelists/graylists/blacklists of email domains and addresses for control over file sharing.
  - Enforcement of policies for access to cloud services, folders, and applications.
  - Management of key expirations and polling periods.
  - Ability of administrators to monitor all known IP addresses for cloud service providers and match them with the application process to centrally manage encryption, encryption keys, data recovery, policies and forensics.

  Secure Lifecycle Protected Office mode offers enhanced security on Office documents (Word, PowerPoint, and Excel) for internal users.

  - Files remain encrypted for unauthorized users, for example, when files are attached in email, moved in a web browser or File Explorer, or stored on removable media.
  - A callback beacon can be inserted into every protected Office file, when the beacon server is installed as part of the Dell Server Front End/Proxy Mode installation.
  - Protected Office documents are supported with Mozy, our companion solution, as well as other cloud, email, and nfs storage products.

Resolved Technical Advisories v8.11

Enterprise Edition for Windows

- An issue is resolved that resulted in the Local Management Console appearing unresponsive while the Encryption client performed tasks in the background. [DDPC-2769]
- Slotted activation now proceeds as expected for users who change their passwords before activation. [DDPC-3279]

- 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]

Preboot Authentication

- An issue is resolved that resulted in the computer becoming unresponsive when a smart card was inserted during startup on the Dell Latitude E5270, E5470, E5570, E7270, E7470, or Precision M3510. [DDPC-4547]
- Preboot Authentication is supported with UEFI mode ***only*** on the following computers:
  - Latitude 5280
  - Latitude 5480
  - Latitude 5580
  - Latitude E7280
  - Latitude E7480
  - Precision 3520

Technical Advisories v8.11

Enterprise Edition for Windows

- 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]
- On a computer with no files on the desktop, Windows Explorer occasionally becomes momentarily unresponsive or crashes. If it is necessary to reopen File Explorer, select **Start Menu > Run >** type **explorer.exe**. [DDPC-4620]
- 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]

Secure Lifecycle

- When Folder Management is enabled, the Dropbox option remains in Folder Management after Dropbox is uninstalled. [DDPCE-417]
- Files cannot be downloaded directly from a cloud storage provider's website. To work around this issue, open files in the Secure Lifecycle virtual drive on the client computer. [DDPCE-1511]
- When a new folder is created in the Secure Lifecycle virtual drive and a new file is added to it, the help file specified in the Help File Name and Help File Contents policies is not added to the folder. [DDPCE-1824]
- When a user with a personal Dropbox account joins a Dropbox for Business team, the user must restart the computer in order for Secure Lifecycle to protect all Dropbox files. [DDPCE-1854]
- If a cloud profile is removed from the Cloud Storage Protection Providers policy, files can be uploaded in cleartext. Cloud profiles are included in the policy value by default and must remain there. [DDPCE-1888]
- If Google Drive is installed before Secure Lifecycle activation, files can be uploaded in cleartext until activation. Dell recommends that sync clients are not installed prior to Secure Lifecycle activation. [DDPCE-1951]
- If the Obfuscate Filenames policy is changed, only new folders and their contents are named based on the policy change. Existing folders and their contents are named based on the Obfuscate Filenames policy value at the time the folder is created. [DDPCE-1956]
- When the Dropbox Encrypt Personal Folders policy is Not Selected, a folder that is cut and pasted from a personal Dropbox folder to a Dropbox for Business folder is not encrypted. [DDPCE-1957]
- When a file is downloaded to a computer and decrypted, a copy of the file with a .xen extension remains. The copy of the .xen file can be deleted. [DDPCE-2297]
- Added 4/2017 - The user receives no error message when attempting to copy data from a protected Office document to a new unprotected document, with Office 2013. [DDPCE-2618]
- A protected Word or Excel file can be inserted into an unprotected non-Office file (.txt or .csv) if the non-Office file is opened with Word or Excel and the user inserts it as an object. Embedded Office files are not supported with protected Office mode. [DDPCE-2591, DDPCE-2647]
- Added 4/2017 - Occasionally, due to Office Clipboard cache, protected content remains in the cache and can be copied to new unprotected Office documents although Force-Protected mode is enabled. [DDPCE-2646]

  When a OneDrive file is uploaded from a computer without Secure Lifecycle installed, a placeholder file (.plh) is created in the Secure Lifecycle virtual drive. Attempting to open the file results in a File Access Denied error. To work around this issue, simply delete the .plh file. [DDPCE-2702]
- Syncing a file that is copied and modified outside the sync folder then pasted back into the sync folder occasionally requires more time than syncing other files. [DDPCE-2717]
- If the sync client is not installed on the computer, protected Office documents cannot be opened in the Office application by selecting the Open in Protected View option and entering the file name. [DDPCE-2818]
- If the administrator installs Secure Lifecycle, the user must be logged in when the administrator enters the administrative user name and password. If the user is not logged in, the Secure Lifecycle directories are placed in the administrator's User folder. The user gets an unknown error and cannot open protected Office files. [DDPCE-2992]
- Added 2/2017 - After two or more Excel copy/cut and paste operations in rapid succession on a computer running either Windows 7 or Office 2010, Secure Lifecycle becomes unresponsive. With other OSs and Office versions, Excel occasionally returns an error, but Secure Lifecycle continues to function as expected. [DDPCE-3246]
- With Secure Lifecycle and protected Office documents, users can have multiple PowerPoint or Word documents open. However, if a user selects multiple protected PowerPoint or Word documents in Windows Explorer, right-clicks, and selects **Open** from the menu, an error message may display or some files may fail to open. If this occurs, open the documents one at a time or, for multiple documents, select **File > Open**. [DDPCE-3287]
- Some files may remain after deleting multiple Google Drive files from the Secure Lifecycle virtual drive. To work around this issue, delete the files in the browser or from the command line. [DDPCE-3366]
- When running protected Office mode, saving an existing Word file does not convert it to a protected Office file. To work around this issue, select **File > Save As** and rename the file. [DDPCE-3448]
- New files in pre-existing sync client folders are encrypted rather than remaining unencrypted as expected when Secure Lifecycle is installed and the Force Protected File Only policy is Selected. [DDPCE-3594]
- Added 4/2017 - The watermark may not display in a protected Word document when the user selects **File > Print > Settings > Print Selection** although the Print Control policy is set to Watermark. [DDPCE-3617]
- When the Enable Time to Live and Embargo Control policy is Selected, a previously unprotected file is protected even if the user cancels after selecting to Date Restrict/embargo the file and does not save edits. [DDPCE-3692]

- Audit events are not uploaded to the Dell Server if the user removes the audit certificate from the Windows store. To work around this issue, restart the computer to regenerate the audit certificate. This is possible since the certificate remains in memory although it has been removed. Ensure that certificates are not purged through Group Policy. [DDPCE-3820]
- Added 2/2017 - After canceling an operation to add a date restriction to a file, the Secure Lifecycle window is unresponsive for a short time. [DDPCE-3845]
- Added 4/2017 - Embargo dates occasionally do not display when an embargoed Office document is saved directly to a network drive. To work around this issue, save the file on a local drive and then copy it to the network drive. [DDPCE-4058]
- Secure Lifecycle protects the Clipboard when a user copies from a protected Office document and pastes to an unprotected location. This impacts **Open > Recent** if a user selects a recent Office file and right clicks to select **Copy path to clipboard**. Currently, for Office 2013 and 2016, if a user has a protected Office document open or if the enterprise has policies set for Force-Protected mode, the user cannot paste any path in the list to an unprotected location. The user must manually type the path or paste it into a protected Office document. [DDPCE-4130]
- Added 4/2017 - When a Dropbox and OneDrive user attempts to delete all folders from the virtual drive, files are deleted but the folders remain. To work around this issue, delete the folders in the cloud storage provider's website. [DDPCE-4224]
- Added 4/2017 - Encrypted (.xen) files cannot be opened directly from a cloud storage provider folder in File Explorer. To work around this issue, open files in the Data Guardian virtual drive. Protected Office documents are not affected by this issue. [DDPCE-4260]
- Added 4/2017 - A protected Word document may print without a watermark or Word may become unresponsive when the user right-clicks and selects **Print**, although the Print Control policy is set to Watermark. To work around this issue, use another print option, such as **File > Print**. [DDPCE-4261]

Secure Lifecycle Mobile Application

- When a large number of PowerPoint (.pptx) files with images and videos are added to the sync client folder after the application has been continuously open and in the foreground, a timeout may occur and the application becomes unresponsive. [DDPCE-3632]
- A few Dropbox items are not translated in the Android application. [DDPCE-3643]
- Files can still be made available offline although an Android device is suspended. [DDPCE-3652]
- Shared folders are not visible in the iOS application for Google Drive or OneDrive or in the Android application for OneDrive. [DDPCE-3755, DDPCE-3756, DDPCE-3757]
- In the iOS application, more than one file instance (offline and online) is created if a protected Office document is edited and saved multiple times while the network connection is intermittently interrupted. [DDPCE-3937]
- An incorrect file path displays in Audit Logs for a document created with the Android application on Google Drive or OneDrive for Business. To work around this issue, use the file name rather than the path for audit data. [DDPCE-4022]
- On rare occasion, the Android application is unable to provision a sync client in **Settings**. To work around this issue, retry provisioning. [DDPCE-4045]
- Occasionally, the iOS application may become unresponsive when a file is synced over a slow network connection. [DDPCE-4163]
- The file path in Audit Logs is an empty value for a document created with the iOS application. To work around this issue, use the file name rather than the path for audit data. [DDPCE-4239]
- In the iOS application, out-of-range Date Restricted/embargoed files can be copied from one sync folder to another. [DDPCE-4303]

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.
- A new policy allows the administrator to hide Encryption overlay icons in File Explorer for managed users.
- The Encryption client and BitLocker Manager are now supported with TPM 2.0.

Resolved Technical Advisories v8.10.1

Enterprise Edition for Windows

- A timeout message logged during a failed activation has been modified to clarify the timeout period in milliseconds. [DDPC-2625]
- 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]
- If the activation prompt times out for a second or subsequent user on a computer with an activated user, the prompt now displays again. [DDPC-3705]
- 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]

Preboot Authentication

- An issue is resolved that previously prevented users from authenticating on some non-UEFI computers when PBA was configured for smart card only. [DDPC-2578]

Technical Advisories v8.10.1

Enterprise Edition for Windows

- The recovery file that is downloaded from the Dell Data Protection Server does not execute with the provided recovery image, and the following message displays: "The subsystem needed to support the image type is not present." [DDPC-2409]
- 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]
- 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

- Dell Data Protection | Server Encryption is now supported. Server Encryption provides remote management of servers, including the following:
  - Software encryption
  - Port control
  - Removable storage encryption
  - Support for maintenance scheduling, which allows control over enforcement of policies that require reboot
- Dell Data Protection | Cloud Edition now supports Microsoft Windows 10, as well as Google Drive and OneDrive for Business. OneDrive is now supported with Microsoft Windows 8.1.
- Cloud Edition now supports the Unified OneDrive Desktop Sync Client. Support is limited in this release to a maximum of two linked business accounts per domain.
- 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 Enterprise 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

Enterprise Edition for Windows

- 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]
- 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]
- 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 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]

Preboot Authentication

- When the drive letter of a NTFS self-encrypting drive is changed on a computer with Preboot Authentication activated, the computer no longer becomes unresponsive. [DDPC-2973]

Technical Advisories v8.10

Enterprise Edition for Windows

- 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.
- 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]

Enterprise Edition for SED

- 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 the SED Client. If the SED Client is already installed, deactivate PBA and uninstall. After installing the Microsoft Security Advisory, reinstall the SED Client. For more information, see https://technet.microsoft.com/en-us/library/security/3033929. [DDPC-4237]

Preboot Authentication

- Occasionally, the access code prompt displays rather than the Preboot Authentication login screen on computers with a wired network connection. [DDPC-3188]
- 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 the SED Client. If the SED Client is already installed, deactivate PBA and uninstall. After installing the Microsoft Security Advisory, reinstall the SED Client. For more information, see https://technet.microsoft.com/en-us/library/security/3033929. [DDPC-4237]

Resolved Technical Advisories v8.9.1

All Clients

- Inaccurate "Failed to open service" error messages no longer display in the output of the FindMyProblem utility. [DDPC-1188]

Enterprise Edition for Windows

- 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]
- SDE key material download failures now result in a meaningful log entry, "Failed to validate key material bundle against the device." Erroneous validation failure warnings no longer display. [DDPC-960, DDPC-961]
- 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]
- 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]

Enterprise Edition for SED

- 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]
- Volumes with Unicode strings in their serial numbers are now correctly reported in inventory. [DDPC-1899]
- Added 07/2016 - The following Dell computer models are supported with UEFI:

Dell Computer Models - UEFI Support

- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7240
- Latitude E7250
- Latitude E7270
- Latitude E7275
- Latitude E7350
- Latitude E7440
- Latitude E7450
- Latitude E7470
- Latitude 12 Rugged Extreme
- Latitude 12 Rugged Tablet (Model 7202)
- Latitude 14 Rugged Extreme
- Latitude 14 Rugged
- Precision M3510
- Precision M4800
- Precision M5510
- Precision M6800
- Precision M7510
- Precision M7710
- Precision T3420
- Precision T3620
- Precision T7810
- Optiplex 3040 Micro, Mini Tower, Small Form Factor
- Optiplex 3046
- Optiplex 5040 Mini Tower, Small Form Factor
- OptiPlex 7020
- Optiplex 7040 Micro, Mini Tower, Small Form Factor
- Optiplex 3240 All-In-One
- Optiplex 7440 All-In-One
- OptiPlex 9020 Micro
- Venue Pro 11 (Models 5175/5179)
- Venue Pro 11 (Model 7139)

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]
- Volumes with Unicode strings in their serial numbers are now correctly reported in inventory. [DDPC-1899]

BitLocker Manager

- Volumes with Unicode strings in their serial numbers are now correctly reported in inventory. [DDPC-1899]

Resolved Technical Advisories v8.9

Enterprise Edition for Windows

- 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. The default policy has been changed for EE and VE Servers v9.2 and later. [DDPC-1207, DDPS-2952]
- 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]
- Slotted activation is now functioning as expected. Previously, in v8.5.1 and later versions, the Shield Service crashed without indication to the user and the activation request never occurred. [DDPC-1462]

Preboot Authentication

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

Server Encryption

- The Server Encryption client uninstaller now defaults to the uninstall/decrypt option instead of uninstalling but leaving files encrypted. [DDPC-857]

Technical Advisories v8.9

All Clients

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

Enterprise Edition for Windows

- 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]
- The organization and naming of some policies differ in the local console and EE or VE Server Remote Management Console. [DDPC-1253]
- Added 8/2017 - When the user inserts EMS-encrypted media and clicks **Access Encrypted Files** on a Windows 10 computer without the Encryption client installed, the options **Install EMS Service** and **Run EMS Explorer** are not available. [DDPC-1449]
- 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]
- 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

- On UEFI computers running the Windows 10 Fall Update and AVG Antivirus, Advanced Authentication installation with the child installer is interrupted and never completes. [CSF-1192]
- 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]
- Changes to the Logon Authentication Policy on EE or VE Server take effect on the endpoint only after a restart. [CSF-1216]
- Occasionally on computers running the Windows 10 Fall Update, fingerprints may need to be re-enrolled. [CSF-1225]

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]
- Added 4/2017 - Login or recovery fails when a German keyboard is used to enter special characters into the password or recovery answer fields. [DDPC-5531]

Resolved Technical Advisories v8.7.1

Enterprise Edition for Windows

- Client computers running Windows 10 are now correctly represented in DDP Server inventory as running Windows 10, rather than Windows 8.1. [DDPC-908]
- Silent uninstall now succeeds with decryption using a previously downloaded recovery key. [DDPC-941]
- 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]
- When PBA is disabled by policy, the client DDP Console now indicates that PBA is deactivated. [CSF-1015]
- Preboot Authentication now accepts the apostrophe character (') in the username field. [DDPLP-376]

Cloud Edition

- When an internal (domain) user renames a shared folder in the local synced folder, the existing folder name is now updated in external (non-domain) users' local synced folders and the renamed folder is no longer stored as a new folder. [DDPCE-841]
- When policy is changed to disable Cloud Protection, an error message that the virtual drive is unavailable no longer displays. [DDPCE-1789]
- On computers with the Encryption client installed, clicking the sync client shortcut now opens the DDP|CE virtual drive when an encryption sweep is in progress. [DDPCE-1921]
- After uninstallation, the cloud storage provider shortcut no longer attempts to open the DDP|CE virtual drive. [DDPCE-1925]
- Performance is improved on computers running the Encryption client. [DDPCE-1932]
- With Dropbox on computers running Windows 10, the Manage Folders menu item is now enabled. [DDPCE-1936, DDPCE-1955]
- With Dropbox, temporary files are no longer synced to the cloud. [DDPCE-1942]
- With OneDrive for Business, a file moved from one folder to another in the DDP|CE virtual drive now displays in the new folder. [DDPCE-1945]
- Cloud Edition is now supported with the GPO "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing." This GPO no longer must be set to Disabled or Not Defined. [DDPCE-1947]

New Features and Functionality v8.7

- Dell Data Protection | Server Encryption - provides remote management of servers, including:
  - Software encryption
  - Port control
  - Removable storage encryption
  - Support for maintenance scheduling, which allows control over enforcement of policies that require reboot
- Dell Data Protection | Cloud Edition now supports Microsoft Windows 10, as well as Google Drive and OneDrive for Business. OneDrive is now supported with Microsoft Windows 8.1.
- The Windows USB selective suspend feature is now supported.

Resolved Technical Advisories v8.7

Enterprise Edition for Windows

- 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]

Enterprise Edition for SED

- Added 11/2015 - The following drives are now supported for SED management:

  Drives with "X" are supported for SED management 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

Drive	Availability	Standard
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 v8.7.1

Preboot Authentication

- Added 8/2017 - The Dell Optiplex 7040 keyboard becomes unresponsive when the Advanced Boot Options menu is accessed with the PBA active. [DDPC-2684]

Technical Advisories v8.7

Enterprise Edition for Windows

- 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]
- If EMS Service (without the full version of the Shield) is installed, uninstall it prior to installing Enterprise Edition. Otherwise, installation will fail. [DDPMTR-1871]
- Cloud Edition is not supported with the GPO "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing." Set this GPO to Disabled or Not Defined. [DDPCE-1947]

Advanced Authentication

- 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]

Cloud Edition

- With Google Drive, copying files to the DDP|CE virtual drive results in a warning that properties will be stripped from the file. Security attributes are removed from the file. No data is lost. [DDPCE-1406]
- Files cannot be downloaded directly from a cloud storage provider's website. To work around this issue, open files in the DDP|CE virtual drive on the client computer. [DDPCE-1511]
- When an external (non-domain) user creates a text document in the DDP|CE virtual drive, an extra file named "New Text Document.txt" is created and encrypted along with the user-created file. The extra file can be deleted. [DDPCE-1608]
- When DDP|CE is installed but the Dropbox sync client is not, files and folders downloaded from the Dropbox website cannot be decrypted. To work around this issue, install the Dropbox sync client and open Dropbox files in the DDP|CE virtual drive on the client computer. [DDPCE-1810]
- On 64-bit browsers, the notification that the user has navigated away from a protected website does not display. Although the notification does not display, file encryption in the cloud proceeds as expected. [DDPCE-1823]
- When a new folder is created in the DDP|CE virtual drive and a new file is added to it, the help file specified in Cloud Storage policies Help File Name and Help File Contents is not added to the folder. [DDPCE-1824]
- If a web browser is removed from the providers list or assigned any protection level other than Protect in the Cloud Storage Protection Providers policy, files are not encrypted when that browser is used to upload files or folders to cloud storage provider websites. [DDPCE-1888]
- When an external user uses the cloud storage provider's website to create or upload an edited file into an internal user's folder with a filename that matches that of another file in the folder, the file will not sync to the DDP|CE virtual drive on either user's computer. [DDPCE-1897]
- After upgrade from v1.3 or earlier, an external Dropbox user's local files do not display in the DDP|CE virtual drive, although the files remain encrypted in the cloud. To work around this issue, after installation, click Relink in the Dropbox Folder Missing dialog. The files will be synced to the DDP|CE virtual drive. [DDPCE-1899]

Server Encryption

- If the user opens the local console before activation, a message displays that Administrator rights are required, without regard to the access rights of the logged on user. [DDPMTR-1402]
- The Cancel button on the Activation dialog is unresponsive. [DDPMTR-1430]
- The Activate option displays in the system tray icon menu for a few minutes after activation is completed. However, an attempt at a second activation will not succeed. [DDPMTR-1522]
- Clicking the system tray icon immediately after installation and restart may result in a message that access is denied. To work around this problem, wait a few minutes then click the system tray icon again. [DDPMTR-1559]
- In the local console, the Applies to: field on the Current Settings screen may be blank. To work around this issue, to view policies for the server's virtual user, click the pull-down arrow in the Applies to: field and select **SERVER_OS**. [DDPMTR-1696]
- After SDE recovery and a restart on Windows 10, the server does not boot directly into Windows but instead displays the Windows Automatic Repair screen. To work around this issue, restart the server until it boots directly into Windows. [DDPMTR-1751]
- With Hyper-V enabled, restart fails after an encryption sweep. To work around this issue, ensure that the SDE Encryption Rules policy excludes the following files from encryption:

  %systemroot%\system32\hvix64.exe

  %systemroot%\system32\hvax64.exe

  %systemroot%\system32\hvloader.exe

  [DDPMTR-1862]
- Enabling or disabling Hyper-V when SDE encryption is enabled causes a failure that requires SDE recovery. To work around this issue, before installation, enable or disable Hyper-V as needed. If DDP|SE is already installed, decrypt and uninstall,
- enable or disable Hyper-V, then reinstall and activate. [DDPMTR-1863]

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

- Enterprise Edition, External Media Edition, and Advanced Authentication clients now support Windows 10. Cloud Edition will support Windows 10 in a future release.
- BitLocker Manager is now included with every DDP | EE purchase. This requires the DDP | EE Server or DDP | VE 9.1 Server (DDP | VE 9.1 Server not yet released). The Server will first decrement BitLocker licenses from previous purchases and once those are depleted, additional BitLocker clients will decrement a DDP | EE client license. This applies to both new and existing customers.

Resolved Technical Advisories v8.6.1

Enterprise Edition for Windows

- 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]

Enterprise Edition for SED

- The issue that resulted in unnecessary reboots after the "DellMgmtAgent" service starts is now resolved. [CSF-523, CSF-541]

BitLocker Manager

- The issue that resulted in unnecessary reboots after the "DellMgmtAgent" service starts is now resolved. [CSF-523, CSF-541]

New Features and Functionality v8.6

- Encryption client, External Media Edition, Advanced Authentication, Enterprise Edition for SED, and BitLocker Manager now provide 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

Enterprise Edition for Windows

- 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]
- The issue that resulted in a computer experiencing a blue screen after External Media Edition is uninstalled from a computer with PBA activated is resolved. [DDPMTR-1020]
- 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]

BitLocker Manager

- Activation issues that previously occurred with the error message, "unable to create TPM only protector," and unexpected reboots are now resolved. [CSF-426]

Technical Advisories v8.6

Enterprise Edition for Windows

- Added 09/2015 - In order to add new features, functionality, and the newest operating systems, Enterprise Edition for Windows 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]
- 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]
- With Encryption with Deferred Activation, data is encrypted using the Common Encryption Key. However, the local console reports the values of the following policies not as Common Key but as they are set on the DDP Server: Application Data Encryption Key, User Data Encryption Key, and EMS Data Encryption Key. [DDPMTR-657]
- Attempting to upgrade Enterprise Edition to Encryption with Deferred Activation results in disabling of deferred activation after reboot and display of the Encryption client entry in Control Panel Programs and Features. [DDPMTR-808]
- With Encryption with Deferred Activation, to use Kerberos to silently decrypt and uninstall, the computer must be connected to the domain, and the user must have the following administrator privileges: domain administrator, local administrator, DDP Forensic Administrator, and administrator on the DDP Key Server. Furthermore, a local administrator who is logged on to the computer must decrypt all encrypted files on the computer before uninstallation, rather than having the option to uninstall without first decrypting files. [DDPMTR-868]
- 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]
- 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]
- Amended 08/2015 - When using the child installer, no reboot automatically occurs, but a restart is necessary. The user must manually restart the computer or, to force a restart after installation, add /forcerestart to the installation command. [CSF-336]
- 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]

- 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]
- When running Windows 10 on a computer with smart card authentication through PBA activated, after resuming from hybrid sleep, single sign-on fails. [DDPLP-308]
- To protect communications against the OpenSSL CVE-2014-3566 vulnerability, Dell Enterprise Server v8.5.1 and DDP Enterprise Server - Virtual Edition v9.0 and later are set to communicate using TLS, by default. However, SED and HCA v8.6 clients communicate with Enterprise Server using SSL. This means that when running Enterprise Server v8.5.1 and later, SED or HCA v8.6 clients with Preboot Authentication activated will fail to communicate with Enterprise Server. To work around this issue, refer to knowledge base article SLN296006 at http://www.dell.com/support/article/us/en/19/SLN296006. This workaround must be implemented as soon as possible, in order to prevent PBA client communication issues with Enterprise Server v8.5.1 or Virtual Edition v9.0 and later. [DDPUP-733, DDPMTR-1331]
- 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]

Enterprise Edition for SED

- Amended 08/2015 - When using the child installer, the installer will effect a reboot only if necessary. To force a restart after installation, add /forcerestart to the installation command. [CSF-246]

Cloud Edition

- When running Encryption with Deferred Activation, Cloud Edition policies may not flow from the DDP Server. If this occurs, in DDP Remote Management Console, check the list of endpoints. The list includes an endpoint for both the host name and the Machine ID for the computer. To work around this issue, ensure that Cloud Edition policies are set for the endpoint represented by the computer host name. Encryption policies must continue to be set on the endpoint represented by the computer Machine ID. [DDPMTR-825]

BitLocker Manager

- Amended 08/2015 - When using the child installer, the installer will effect a reboot only if necessary. To force a restart after installation, add /forcerestart to the installation command. [CSF-246]
- 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/SLN296006. [CSF-454]

Resolved Technical Advisories v8.5.1

Enterprise Edition for Windows

- 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]
- 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 BitLocker Manager or computers running DDP|HCA contacting the Server too frequently during encryption and decryption has been resolved. The Server is contacted only at encryption/decryption completion (or other regularly scheduled polling intervals). [CSF-243]
- The issue of upgrading or uninstalling 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 rare occurrence of NTFS corruption leading to truncated .pst files is resolved. [DDPC-625]
- Interoperability issues with Symantec Endpoint Protection v12.1.5 have been resolved. Upgrades from SEP v12.1.4 to v12.1.5 should not cause issues with Dell Data Protection | Encryption. [DDPC-759, DDPC-797]
- The issue of Windows reporting "Windows Not Genuine" when running a Microsoft KMS and Dell Data Protection | Encryption have been resolved. This issue occurred infrequently and only when a certain set of Encryption policies were applied, specific AV software was running, and a KMS server was being utilized. [DDPC-804]
- Roaming profiles are now properly deleted after log off. [DDPC-807]
- The issue of installation failures due to SQL Compact errors when upgrading from v8.3.2 to 8.5.x is resolved. [DDPC-810]
- 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]

Enterprise Edition for SED

- Occasional upgrade failures from Security Tools to Enterprise Edition have been resolved. If the initial upgrade fails due to the Server being unavailable, the client will continue to be locally managed until the Server can be contacted and a new policy set is received at the client. [CSF-1]
- 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]
- An SED client-side registry setting is now available to configure the retry interval when the Server is unavailable to communicate with the SED client. This registry setting can be used to prevent large numbers of clients from trying to contact the Server at once, thereby compounding the problem. [CSF-24]
- 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]
- 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 installer now properly installs UEFI PBA upon detection of a UEFI BIOS. Legacy PBA is installed if a UEFI BIOS is not detected. [CSF-148]
- 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]

- Previously, when installing the SED client or BitLocker Manager, if an external drive (or USB media) was connected during installation, but disconnected prior to the post-installation restart, the computer would fail to reboot until the external drive was reconnected. This issue is resolved. [MMW-693/CSF-15, CSF-14]

Cloud Edition

- Amended 10/2015 - With Dropbox v2.10.30 and later, a permission denied error no longer occasionally occurs when syncing files created by internal users within folders that have been created by external users. [DDPCE-834]

BitLocker Manager

- 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]
- Excessive network traffic caused by BitLocker Manager checking network and USB drive status has been resolved. [CSF-120]
- When installing BitLocker Manager through the UI, all options to select the startup policy are now displayed properly. [CSF-204]
- The issue of BitLocker Manager or computers running DDP|HCA contacting the Server too frequently during encryption and decryption has been resolved. The Server is contacted only at encryption/decryption completion (or other regularly scheduled polling intervals). [CSF-243]
- Previously, when installing the SED client or BitLocker Manager, if an external drive (or USB media) was connected during installation, but disconnected prior to the post-installation restart, the computer would fail to reboot until the external drive was reconnected. This issue is resolved. [MMW-693/CSF-15, CSF-14]

New Features and Functionality v8.5

- Preboot Authentication (PBA) with password is now supported on Windows 8 and Windows 8.1 on select Dell UEFI computers with qualified Opal Compliant SEDs.
- Secure Boot is now supported with the Encryption client and Security Tools on select Dell UEFI computers running Windows 8 and Windows 8.1 with qualified Opal Compliant SEDs.
- Intel RAID is now supported with legacy PBA on computers with Hardware Crypto Accelerators (HCAs).
- Manual entry One-time Password (OTP) is now supported for Windows logon and recovery of access to computers running Security Tools.

Resolved Technical Advisories v8.5

Enterprise Edition for Windows

- 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

- Computers now lock upon removal of a smart card from the smart card reader, based on Virtual Edition or Enterprise Server policy setting. [28561/DDPC-33, MMW-337]
- 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]

Enterprise Edition for SED

- On computers with Intel Rapid Start, the hibernation partition no longer has to be removed in order for the SED management client/ Security Tools to function properly. [28562/MMW-701]

Technical Advisories v8.5

Enterprise Edition for Windows

- After using the Managed Migration Utility, files that were encrypted with Personal Edition using the User Roaming key are not accessible. To work around this issue, before migrating, ensure that the User Roaming key is not set for either the *Application Data Encryption Key* or *User Data Encryption Key* policy. If the User Roaming key is used, change the key to either Common or User, and save the policy change. Each user on the computer must log on and allow the encryption sweep to complete. After encryption sweeps are complete for all users, run WSScan to ensure that no files are still encrypted with the User Roaming key. Migration can now be performed. [DDPC-606]
- Pausing encryption is not reflected in the local console if the menu option "Process Encryption Only When Screen is Locked" is enabled. [DDPC-620]
- After migrating a computer running Windows 8 or Windows 8.1 and using Windows' Fast Startup feature with the Managed Migration Utility, a second restart is required for the migration to complete successfully. This is due to Windows' Fast Startup feature, which logs off and hibernates the user, rather than restarting the computer. A second reboot completes the migration. [DDPC-725]
- 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]
- The computer does not single sign-on after resuming from Sleep-to-Hibernate. 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 Security Tools and Encryption do not support Sleep-to-Hibernate and single sign-on. Disable Sleep-to-Hibernate when using Preboot Authentication if your organization intends to use single sign-on. [MMW-841]

Advanced Authentication

- After migrating with the Managed Migration Utility, a user may not be able to authenticate with enrolled fingerprints. To work around this issue, change the policy to require only password authentication. The user should log on and re-enroll fingerprints. After re-enrollment, the user will be able to log on with fingerprints. [MMW-573]
- Password Manager does not support Google Chrome v35 and later, due to a change in the way Chrome handles extensions. [MMW-619, MMW-754]
- Password Manager does not support importing credentials from Internet Explorer 10 and 11 (because the interface is not published by Microsoft). [MMW-770]
- On computers running ActivClient 7, single sign-on may not function properly. Also, multiple smart card icons may display in the Windows credential provider screen. [MMW-837]
- When Preboot Authentication is activated on a computer with more than one user and with only fingerprint authentication enabled, if two or more users enroll with the same fingerprint, at authentication for second and subsequent users an error message may display, "The fingerprint is not verified." However, the first user is able to authenticate successfully. [MMW-848]

- Eikon external fingerprint readers do not function properly on Windows 8.1 without the latest drivers. To work around this issue, when using an external fingerprint reader, download and install the latest drivers required for your specific reader. [MMW-880]

Preboot Authentication

- When upgrading from pre-v8.2 Enterprise Edition, Preboot Authentication must be deactivated before beginning the upgrade. After the upgrade, the PBA is activated normally. [DDPC-636]
- On a UEFI laptop computer with the PBA activated, when the computer is docked or attached to an external monitor, the laptop lid must remain open in order for the PBA to function properly. [DDPUP-507]
- On a computer with multiple users the Windows Power Option, Require a password on wakeup, must be enabled. If this option is not enabled, when the computer resumes from hibernation, it resumes in the user account in which hibernation occurred. This behavior is typical of Windows hibernation. [MMW-761]
- After activating Preboot Authentication on a UEFI computer, when the computer resumes from hibernation for the first time following PBA activation, the process becomes a cold boot. After the first hibernation, the computer resumes from hibernation normally. To work around this issue, restart the computer a second time after PBA activation. [MMW-844]

Enterprise Edition for SED

- During an update to Intel Rapid Storage Technology Drivers, the self-encrypting drive may become undetectable. To resolve this issue, reboot the computer a second time after the update has been applied. [MMW-633]

Cloud Edition

- When using the master installer to install Cloud Edition and installing using the interactive UI mode, the Encryption client is automatically selected in the list of features to install and, therefore, two licenses are consumed. There are three ways to work around this issue:

1 Use the command line mode to install the software. Only the master installer in interactive UI mode exhibits the issue.

2 Manually de-select the Encryption client in the interactive UI mode installation.

3 Use the child installer to install Cloud Edition. Only the master installer in interactive UI mode exhibits the issue.

[DDPC-140]

- With Dropbox v2.10.30 and later, a permission denied error occasionally occurs when syncing files created by internal users within folders that have been created by external users. [DDPCE-834]

BitLocker Manager

- Amended 06/2015 - If a user suspends then turns off BitLocker through the BitLocker dialogs, decryption begins and continues for five minutes after the user suspends BitLocker at which point BitLocker Manager reverts decryption. If the volume fully decrypts within five minutes after BitLocker is suspended, at five minutes, encryption begins and may require user interaction. [CSF-253]

New Features and Functionality v8.4.1

- Multi-certificate Common Access Cards are now supported.
- Enterprise Edition for Windows now supports Windows Embedded 8.1 Industry Enterprise Edition.
- Cloud Edition for Windows now supports Dropbox 2.11 and Dropbox 2.12.

Resolved Technical Advisories v8.4.1

Enterprise Edition for Windows

- 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]
- Dell Data Protection | Encryption has added logic to better detect self-encrypting drives, including the Samsung SM841. [DDPC-248]
- 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

- When Preboot Authentication is configured to use smart cards for authentication, if the **Options > Server Sync** menu option is selected, the Windows password authentication screen no longer displays. Smart card authentication proceeds normally. (DDPLP-135]
- 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]

Cloud Edition

- The compatibility issue that previously occurred when linking Dropbox for Business with Internet Explorer 8 is now resolved, and the SuppressOAuth registry setting is no longer required. [DDPCE-571]
- With Firefox running on Windows 8.1, an encrypted file that is downloaded through the browser now decrypts as expected when opened with Cloud Edition. [DDPCE-580, DDPCE-704]
- After uninstalling Cloud Edition, registry keys are now removed as expected. [DDPCE-595, DDPCE-636, DDPCE-646]
- When downloading files using the web browser, file icons now properly display in the Save As dialog box, and the user-permissions error that previously occasionally occurred no longer occurs. [DDPCE-630, DDPCE-631]
- The sync client no longer attempts to index synced, encrypted files that are deleted locally. [DDPCE-632]
- Occasional issues with folder uploads through the web browser are resolved. [DDPCE-650]
- Subfolders now inherit protection levels of their parent folders when uploaded to the cloud. [DDPCE-662]
- Synced files and folders that are deselected from Selective Sync then reselected now decrypt from the cloud into the local sync client folder as expected. [DDPCE-668]
- External users' files that are not shared with internal users are no longer encrypted into the cloud. [DDPCE-670]

Technical Advisories v8.4.1

Enterprise Edition for Windows

- After installing External Media Edition, the tray icon menu does not display the option, "Check for Policy Update." Because of this, users cannot manually poll for policy changes. However, at computer start-up, Dell Data Protection | Encryption automatically polls for policy updates. [DDPS-281]
- 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, MMW-724]

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]
- UPN name is not supported by PBA. The correct usage would be to login with a non-UPN user name, domain\username, or enter the username independently and select the domain from the drop-down menu. [DDPLP-167, DDPC-80, MMW-591]
- 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]

New Features and Functionality v8.4

- When using Cloud Edition and Dropbox for Business, the following features are now available:
  - Remote wipe user accounts
  - Multi-account support, including new policies that distinguish between Dropbox for Business and Dropbox personal accounts
  - Dropbox for Business context menus for quick access to frequently used operations
- Cloud Edition now offers expanded protection and management options, as well as an enhanced user experience with Dropbox:
  - Secure one-click sharing
  - Ability to view files that are encrypted with Cloud Edition using the native Dropbox mobile application
- Cloud Edition now supports Windows 8.1. (OneDrive is not supported on Windows 8.1 when using Cloud Edition.)

Resolved Technical Advisories v8.4

Cloud Edition

- The Dropbox installer now functions properly with Cloud Edition. [DDPCE-81, DDPCE-385, DDPS-435]
- Overall stability is improved. [DDPCE-156, DDPCE-488, DDPCE-516]
- If Cloud Edition is left running and idle, an error no longer occurs and the system tray icon reconnects to the service as expected. [DDPCE-157]
- Downloading files through Google Chrome and Mozilla Firefox now proceeds as expected. [DDPCE-189, DDPCE-696, DDPCE-709]
- Cloud Edition now functions properly with proxies configured through Internet Explorer. [DDPCE-201]
- When the Cloud Edition client computer time setting differs from the time setting of the cloud storage web server by more than 12 hours, correct policy is now delivered without reactivation of Cloud Edition. [DDPCE-347]
- Performance is improved when using WebEx with Cloud Edition. [DDPCE-349, DDPCE-547]
- Folders that do not belong to a sync client no longer display in Cloud Edition Folder Management. [DDPCE-522]
- Syncing with OneDrive running on Windows 7 and Windows 8 now proceed normally. [DDPCE-523, DDPS-718, DDPS-777]
- The Cloud Edition icon now consistently displays on uploaded files. [DDPCE-541]

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

Cloud Edition

- The Dropbox preference, "Share screenshots using Dropbox", allows users to upload unencrypted screenshots to cloud storage. Administrators should consider putting a company policy in place that instructs users to not enable this Dropbox feature. [DDPCE-319]
- After a device is suspended from the system tray icon, the device can still access the Dropbox web site. [DDPCE-401]
- When the Cloud Edition Folder Management feature is used to deselect folders for encryption, parent folders in the same hierarchy are also deselected. [DDPCE-419]
- The user cannot move the default sync folder once the folder location is established. [DDPCE-535, DDPCE-545]

New Features and Functionality v8.3.2

- Enterprise 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]

Enterprise Edition for Windows

- 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]
- Security Tools now properly uninstalls without error when Cloud Edition is installed. [28959]

Enterprise Edition for SED

- 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]

Technical Advisories v8.3.2

Enterprise Edition for Windows

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

New Features and Functionality v8.3.1

- Enterprise Edition for Windows 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.
- Enterprise Edition for Windows now supports OneDrive on Windows 8.1. [28300, 28303, 28304]

Resolved Technical Advisories v8.3.1

Enterprise Edition for Windows

- 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]
- Inventory is now properly uploaded to the Dell Server after the completion of an SDE encryption sweep. [28844]
- 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
  - Network unlock
  - 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
- Enterprise Edition for SED now supports Windows 8 and Windows 8.1 using legacy boot mode for all computers configured with an SED.
- Cloud Edition now supports Box 4.0 and Dropbox 2.6 meta installer.

Resolved Technical Advisories v8.3

Enterprise Edition for Windows

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]
- Hard-coded SDE exclusions for the most common antivirus applications have been added to Enterprise Edition for Windows. Exclusions for Symantec Endpoint Protection, Symantec PGP, McAfee SafeBoot, McAfee Antivirus, and Trend Micro will help to prevent interaction complications between encryption processing and AV processing. [28375]
- 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]
- To improve performance and reduce excessive policy polling, an inventory upload will only occur if the recorded sweep times have changed. [28462]
- 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]

Enterprise Edition for SED

- On the Endpoint Details page, Cloud Device Control commands now correctly display when an SED is activated. [DDPS-379]
- The first time after activation of the PBA, if the computer is locked (CTRL+ALT+DEL) after the "System Shutdown Required" message displays and then the user unlocks the computer, the "System Shutdown Required" message now correctly displays again. A restart is no longer required. [28391]

Cloud Edition

- When an iOS device is moved to a different Enterprise Server, the local policy and cached keys are now correctly reset. [27765]
- 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.
- The new IP address range introduced by Box sync client is now represented in VE Server policies for Cloud Edition. [DDPS-88]
- On the Endpoint Details page, Cloud Device Control commands now correctly display when an SED is activated. [DDPS-379]

Technical Advisories v8.3

All Clients

- If Windows updates are not installed before the master installer runs, installation may fail. [28835]

Enterprise Edition for Windows

- 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]
- 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]
- During Preboot Authentication activation, if the computer is not connected to the network with access to the Enterprise Server, the Encryption client does not enforce required shutdown and Preboot Authentication activation is not completed. If Dell Data Protection | Encryption cannot access the Enterprise Server to back up encryption keys and other critical data, PBA activation is not completed and the required shutdown does not occur. To work around this issue, ensure that the computer has access to the Enterprise Server during the installation of Dell Data Protection | Encryption and policy deployment to back up encryption keys and other critical data, complete PBA activation, and enforce required shutdown. [28787/DDPC-37]
- 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]
- Upgrade from External Media Edition (EME) to Enterprise Edition (EE) fails, and a dialog that requests the Personal Edition Entitlement displays. During the upgrade, EME will be uninstalled. However, the installer is attempting to deploy a DLL that is in use by the EMS Service and requires a reboot to complete the deletion of the file. To work around this issue, uninstall the EMS service using SCedit from the command line before upgrading to EE. [28853, 28854, 28855]
- 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]
- After a user is suspended in the Remote Management Console, the Shield ID is blank rather than indicating that the Shield is unmanaged. On the client computer, the Dell Data Protection | Encryption local console does not open properly. [28893]
- 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]

Enterprise Edition for SED

- 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 (this also uninstalls EE for SED)

  Uninstall Security Tools Authentication

  [28791]
- Amended 05/2014 - Attempting to upgrade from 8.0.0 or 8.0.1 to the latest release fails and an error message is displayed saying that the computer has not been modified. This issue occurs because the installer cannot deactivate the PBA and, therefore, uninstallation of the earlier version is blocked. To work around this issue, deactivate the PBA and reboot the computer before attempting to upgrade to the new version. [28817]
- The Dell Optiplex XE2 computer intermittently does not display the Windows logon or credential provider screen after waking from sleep. To work around this issue, upgrade to the latest applicable BIOS version, which is A05 as of 03/2014. In the BIOS screen, locate the option for Deep Sleep and disable it. [28862]
- Hybrid Sleep is not supported on Windows 8.1 with SED drives on the Precision M6800/M4800 platform. [28897]
- 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:

  - SED with Dell Data Protection | Security Tools installed
  - SED with Dell Data Protection | Encryption installed
  - SED with Dell Data Protection | Security Tools and Dell Data Protection | Encryption installed
  - 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 legacy boot mode, the computer must be re-imaged.

[28790]

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

- Enterprise Edition for Windows (software encryption only) now supports Microsoft Windows 8.1.

Resolved Technical Advisories v8.2.1

Enterprise Edition for Windows

- Enterprise Edition for Windows 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]

Advanced Authentication

- When using Microsoft Windows 8.1, the Security Console screen will no longer be blank after minimizing and re-opening the window. [28044]

- Amended 03/2014 - Password Manager pre-train icons are now supported with Google Chrome and Mozilla Firefox as well as Internet Explorer when using Microsoft Windows 8.1. However, 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.

[28329]

Technical Advisories v8.2.1

Enterprise Edition for Windows

- The Shield is intermittently sending invalid XML characters in the event bundle. The result is that event logs from endpoints are occasionally not parsed or logged for compliance reporting at the Enterprise Server. [28321]

Advanced Authentication

- 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

- Enterprise Edition for Windows (software encryption only) now supports Microsoft Windows 8.1 on Dell Venue Pro 11, Dell Venue Pro 8, and Dell OptiPlex 3020.

Resolved Technical Advisories v8.2

Enterprise Edition for Windows

- Rijndael128 and Rijndael256 encryption algorithms are changed to AES128 or AES256 respectively when using EMS. This change occurs during an Enterprise Server migration to v8.2. Virtual Edition is unaffected, as Rijndael128 and Rijndael256 are not supported. Changing the algorithms to AES128 or AES256 fixes the issue of occasional file corruption when using EMS and taking an encrypted device to a non-Shielded computer and attempting to open the files through EMS Explorer. [27597]

Enterprise Edition for SED

- The PBA authentication process times on Samsung drives have been improved. [27318]
- A message that reads "Please do not turn off or unplug your computer" persists on the Dell Latitude E6440 running Microsoft Windows 7 (32-bit). [28245]

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

Enterprise Edition for Windows

- 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.

Enterprise Edition for SED

- This release resolves an incompatibility between an Intel Network Interface Card and Enterprise Edition for SEDs. This issue was discovered on Dell hardware, but may also exist on other vendor's hardware.

New Features and Functionality v8.1

- Enterprise Edition for Windows adds class level port controls to block data leakage to smartphones
- Enterprise Edition for SED adds PBA support for smart card and smart card + PIN on Windows 7
- Enterprise Edition for Windows adds Windows XP support for software encryption (excludes Advanced Authentication, SED, HCA)

Resolved Technical Advisories v8.1

All Products

- Windows Vista is no longer a supported operating system.

Enterprise Edition for Windows

- 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
- VPN connection events are now reported to the Shield. The use of CREDActivate for remote user activation is no longer required. [27143]
- The prompt to enter an EAP and escrow keys when remotely managed no longer displays. [27600]
- If a user has the *Secure Windows Credentials* policy enabled, they can now log in using cached credentials following the use of WSDeactivate. [27612]
- 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]

Enterprise Edition for SED

- SED recovery question for v7.3 and earlier have been added back to the Enterprise Server.

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

Enterprise Edition for Windows

- 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]

Enterprise Edition for SED

- Amended 03/2014 - 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. [27496, 25785]
- When using a Precision M6800, Single Sign-On will fail if a USB device is currently plugged into the computer. [27595]
- Added 03/2014 - With Windows 8, after a computer automatically moves from the sleep to hibernate state, when the computer resumes, Single Sign-On is not functioning properly. [27888]

Advanced Authentication

- The fingerprint reader on Latitude 10, Latitude 5530, and Latitude 5430 for OS logon does not work with Dell Data Protection | Encryption Enterprise Edition.

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]

BitLocker Manager

- When BitLocker is encrypting, if the PBA is turned on, the error message "createdatabase failed" may be received. To work around the issue, dismiss the dialog and allow BitLocker encryption to finish. [26540]
- When running on a Latitude E5430 and leaving the TPM in a cleared state and relying on EMAgent to activate and take ownership, a "GetPhysicalPresenceRequest - PpiAcpiFailure" error message displays. To work around the issue, have the TPM on and activated in the BIOS and enable the "TPM ACPI Support" check box in the BIOS. [26708]
- Using the GUI to upgrade from 8.0.1 to 8.1 does not function. Upgrading from 8.0.1 to 8.1 from the command line works as expected. Upgrading from the master installer also works as expected. [27664]

Resolved Technical Advisories v8.0.1

Enterprise Edition for Windows

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

New Features and Functionality v8.0

- Enterprise Edition for Windows now supports Microsoft Windows 8 for software encryption and legacy HCA.

Resolved Technical Advisories v8.0

Enterprise Edition for Windows

- As of v8.0, Shield and PCS events are turned off by default. The events can be re-enabled by configuration changes. EMS events remain as they have been in previous versions.
- To reduce the chances of DPAPI authentication failure, the registry is now notified of cached credential changes.
- Inventory times no longer display future times after a reboot when using SDE. [26233]
- 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

Enterprise Edition for Windows

- 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.
- Advanced Authentication cannot be installed when Dell Data Protection | Access is present on the computer. Follow the steps in the *Dell Data Protection | Enterprise Edition Administrator Guide* to uninstall DDP|A. [27073]
- When uninstalling Dell Data Protection | Encryption, 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.

Enterprise Edition for SED

- SED v7.3 cannot be directly upgraded to SED v8.0. To move to v8.0 issue a policy to deprovision the SED and re-provision after the upgrade.

Advanced Authentication

- Advanced Authentication cannot be installed when Dell Data Protection | Access is present on the computer. Follow the steps in the *Dell Data Protection | Enterprise Edition Administrator Guide* to uninstall DDP|A. [27073]

New Features and Functionality v7.7

Enterprise Edition for Windows

Enterprise Edition for Windows and External Media Edition now update the Dell Enterprise Server to change the status to *Unprotected* at the beginning of a client uninstall process. See the *Enterprise Edition Administrator Guide* for details.

Technical Advisories v7.7

Enterprise Edition for Windows

- 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

Enterprise Edition for Windows

- 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.
- When using Self-Service Recovery for External Media Edition, text entry fields to enter an access code no longer display. The access code entry field now only displays during Help Desk Assisted Recovery, as expected.
- Improvements have been made to the Dell Data Protection | Encryption upgrade process.
- 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]
- The Dell Admin Utilities can now use Kerberos to download encryption keys from the Enterprise Server. [23042]
- 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 attempting External Media Edition device recovery, errors related to new passwords not being compliant have been resolved. [23726]
- External Media Edition policies are now applied properly when the user is roaming. [23739]
- When uninstalling External Media Edition, all External Media Edition system files are properly removed. [23768]
- Previously, if a device was encrypted by External Media Edition, then encryption was disabled by policy, when the device was re-inserted into a computer, it would re-encrypt the device. This issue has been resolved. [23780]
- Corruption errors no longer occur when encrypting a file through EMS Explorer and then attempting to read the file on a computer with the full Shield installed. [23806]
- Previously, when an auto-authenticated External Media Edition user changed their password and then attempted help desk assisted recovery, manual authentication would fail. This issue has been resolved. [24025]
- Improvement have been made to user activation, slotted activation, and other delayed user activation scenarios so that Dell Data Protection | Encryption can slot multiple users in Fast User Switching more reliably. [24026, 24034, 24043]
- 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]
- When activating External Media Edition using slotted or network activation, the Dell Enterprise Server would license the client as a full Shield. This issue has been resolved. [24288]
- 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]
- The ADDLOCAL parameter in the Dell Data Protection | Encryption installer has been disabled, as all features are required for Dell Data Protection | Encryption. [24544]
- 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

Enterprise Edition for Windows

- 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]

BitLocker Manager

- Encryption Status Reports will not exactly match the Windows BitLocker encryption dialog window. BitLocker Manager updates encryption status every 30 seconds, therefore there will be a 30 second delay in BitLocker Manager encryption status.
- If a user with local Admin rights uses the Microsoft Control Panel to turn off BitLocker encryption before the volume has been completely encrypted, the preset user authentication (PIN or Startup key) will be removed and the system will revert back to TPM only. To avoid this issue, local Admin users should not use the Microsoft Control Panel to change encryption status when two-factor authentication is set by policy.

Resolved Technical Advisories v7.2.1

Enterprise Edition for Windows

- The "keys" icon no longer displays in the local console when remotely managed. [21874]

Technical Advisories v7.2.1

Enterprise Edition for Windows

- 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

Enterprise Edition for Windows

- 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]

Resolved Technical Advisories v7.0.1

Enterprise Edition for Windows

- The communication between the Shield and the Policy Proxy is now encrypted. This prevents exposure to the command channel and data transported to the Dell Enterprise Server. This is being done in response to increased availability of tools capable of observing wireless network traffic in the clear. Dell recommends the use of a VPN for all communication with Dell Enterprise Servers (our own and otherwise), but the additional protection now included offers an encrypted channel for Dell Enterprise Server contact in the absence of any other measures.
- Windows 7 SP1 has introduced several changes to elements of the Windows operating system that Dell monitors for malicious behavior. Changes to the Shield have been made in order to prevent potential SDE recovery cases, and to ensure that performance is not impacted by the volume of file activity caused by the update.

Technical Advisories v7.0/7.0.1

Enterprise Edition for Windows

- Windows Update Issue - This issue is applicable when running 32-bit Windows XP, Windows Vista, and Windows 7. When using a policy template other than Basic Protection for System Drive Only and when encryption is managed by the Dell Enterprise Server, Windows updates may fail and cause Windows to roll back to a previous version update. To resolve this issue, apply the Basic Protection for System Drive Only template, commit the changes, and re-initiate the Windows update.

2

Workarounds

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

- To host EMS, external media must have 55 MB available, plus open space on the storage that is equal to the largest file to be encrypted. To work around the issue, free up space on the storage or use media with more storage capacity. [DDPC-243]
- 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]
- When one user attempts to access data encrypted for another user on a multi-user Windows device, the Windows software involved, including the operating system itself, may or may not handle this error condition gracefully. If this happens: 1) Review the *User Encrypted Folders* policy involved to see whether the folder should be moved to the *Common Encrypted Folders* policy. 2) See whether an upgrade for your third-party software is available.

Software and Hardware Compatibility

Enterprise 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 Creators Update

- To upgrade a computer running the Encryption client to the Windows 10 Creators 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]

Symantec Protection Agent

- Instability issues (primarily lock ups) have been seen on Shielded computers which have Symantec Protection Agent installed. The only way to recover from this state is to press the power button and manually restart the computer.

  Symantec has acknowledged that this is an issue with the Symantec Protection Agent and the sysguard.sys driver. This known issue affects the following Symantec products:

  - Symantec Protection Agent 5.1.9.7275
  - Symantec AntiVirus Corporate Edition 10.1.6.6010
  - Symantec DLP 10.5.1020.02002

  To work around this issue, Symantec recommends disabling the Buffer Overflow Protection component in the SPA console. To do this, open the OS Protection policy for the group and de-select the Buffer Overflow Protection option. For more information, see http://www.symantec.com/business/support/index?page=content&id=TECH103259. [SF31904]

Symantec Workspace Virtualization

- After installing the Encryption client, shortcuts for programs deployed through Symantec Workspace Virtualization are no longer displayed. The issue has been identified as an incompatibility between Symantec Workspace Virtualization and the Microsoft Swap Buffer Driver. The Encryption client is related to this issue only in that it uses the Microsoft Swap Buffer Driver in its driver technology stack. Customers experiencing this issue should raise a case with Symantec customer support. [28734]

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.

Proventia Desktop Agent

- Proventia Desktop Agent prevents the Shield from accessing the network. Activation will fail unless the Encryption client is added as a known application in Proventia Desktop Agent. Follow the steps below to add CMGShieldSvc.exe as trusted application in Proventia Desktop Agent:

1 Select Tools > Edit Settings.

2 Select Application Control Tab > Known Applications.

3 Browse to CMGShieldSvc.exe. Ensure that Let it Run and Let it Connect (the network) are selected.

PartitionMagic

- If the Encrypt Temporary Files policy is Selected, the Encryption client is compatible with PartitionMagic only when it is run from Rescue Disks.

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.

ePocrates Rx Pro

- Because its databases contain only formulary reference information, if your organization uses ePocrates Rx Pro, we recommend that you exclude certain databases from encryption using the Databases to Exclude from Encryption policy. See the following table for the databases to exclude.

Databases to Exclude		
abbreviations-nc-2	eula-nc-2	PrefsDB
altclin-nc-2	formdetails-nc-2	pricing-nc-2
cfg-nc-2	formsortorder-nc-2	prostrings-nc-2
classes-nc-2	formstatus-nc-2	SmshEULA-nc-2
clientnames-nc-2	groupid-nc-2	sort-nc-2
clinical-nc-2	lasths-nc-2	status-nc-2
druginteractions-nc-2	p002-nc-2	strings-nc-2
drugs-nc-2	p011-nc-2	utilities-nc-2
duse-nc-2	p120-nc-2	version-nc-2

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.