Dell Encryption Personal

Technical Advisories v11.9

January 2024
Rev. A01

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.

Contents

1

Technical Advisories

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

See KB 301500 to view FIPS compliance status for the data security line of products.

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, see Dell ProSupport International Phone Numbers.

New Features and Functionality v11.9

- Bug fixes to improve user experience.
- Upgraded all server and client ISMs to Installshield 2023 R2.

Resolved Security Advisories v11.9

- Earlier Dell Encryption allows any user to access application install directory during the installation. This issue is resolved by setting the Access Control List on application install directory in the start of the installation or upgrade process. [DDPC-13786]

Resolved Technical Advisories v11.9

Encryption v11.9

- An issue is resolved where a temp folder is created during the Dell Encryption installation as the Access Control List is not configured properly. [DDPC-13619]
- An issue is resolved where the Symlink error is not displayed after the installation is complete. [DDPC-13821[

Pre-boot Authentication v11.9

- No technical advisories exist.

SED Manager v11.9

- No technical advisories exist.

Technical Advisories v11.9

Encryption v11.9

- The Symlink is not getting detected in the C:\custom folder of your system. [DDPC-13822]

Pre-boot Authentication v11.9

- No technical advisories exist.

SED Manager v11.9

- No technical advisories exist.

New Features and Functionality v11.8.1

- Bug fixes to improve user experience.

Resolved Security Advisories v11.8.1

- An issue is resolved where the Dell Encryption Installer does not verify if Symlink is available in the ProgramData folder, resulting in creation of random files. [DDPC-13644]

Resolved Technical Advisories v11.8.1

Encryption v11.8.1

- No technical advisories exist.

Pre-boot Authentication v11.8.1

- No technical advisories exist.

SED Manager v11.8.1

- No technical advisories exist.

Technical Advisories v11.8.1

Encryption v11.8.1

- For Dell Precision 7875 workstations, Dell Technologies recommend to use the Dell Encryption client version 11.6 or earlier to avoid the possible black or blue screen problem. [DDPSUS-3295]

Pre-boot Authentication v11.8.1

- No technical advisories exist.

SED Manager v11.8.1

- .No technical advisories exist.

New Features and Functionality v11.8

- Integrated Package Key Destruction Utility tool in the latest installer of Dell Encryption.

Resolved Security Advisories v11.8

- No security advisories exist.

Resolved Technical Advisories v11.8

Encryption v11.8

- An issue that results in cmgshieldsvc.exe crash after user logs on is resolved. [13098]
- An issue that results in system BSOD when a composite device is disconnected from VirtualBox is resolved. [13535]
- An issue that results in application service not getting removed from machine using uninstall command is resolved. [11770]

Pre-boot Authentication v11.8

- An issue that results in PBA not loaded on computers protected by SED Manager when multi-disk encryption is enabled and an additional unencrypted disk is added or replaced is resolved. [DDPC-13358]

SED Manager v11.8

- An issue that results in PBA not loaded on computers protected by SED Manager when multi-disk encryption is enabled and an additional unencrypted disk is added or replaced is resolved. [DDPC-13358]

Technical Advisories v11.8

Encryption v11.8

- No technical advisories exist.

Pre-boot Authentication v11.8

- No technical advisories exist.

SED Manager v11.8

- .No technical advisories exist.

New Features and Functionality v11.7.1

- The internal Windows feature providing user information from Windows to Dell Encryption is scheduled for deprecation but an exact date for the removal is unknown. The Dell Encryption client v11.7 includes a feature to address the loss of this functionality in Windows by implementing a custom Credential Provider. An issue was encountered in cases when other installed products were using a custom Credential Provider on the computer. In these instances, the Windows login process could be disrupted.

  To address this, Dell Encryption 11.7.1 returns to use the previous internal Windows function to avoid any potential custom Credential Provider conflicts. If you require the use of custom Credential Providers for third-party applications and updated to Encryption Personal v11.7, it is recommended that you update Encryption Personal v11.7.1.

Resolved Security Advisories v11.7.1

- No security advisories exist.

Resolved Technical Advisories v11.7.1

Encryption v11.7.1

- No technical advisories exist.

Pre-boot Authentication v11.7.1

- No technical advisories exist.

SED Manager v11.7.1

- No technical advisories exist.

Technical Advisories v11.7.1

Encryption v11.7.1

- No technical advisories exist.

Pre-boot Authentication v11.7.1

- No technical advisories exist.

SED Manager v11.7.1

- SED Manager requires the use of the Dell custom Credential Provider to synchronize Windows password changes and data encryption keys. If you require use of third-party applications that use custom Credential Providers running on computers protected SED Manager, you must initiate Windows password changes through the Data Security Console. For information about changing your password in the Data Security Console, see the *Password* chapter in the Data Security Console User Guide.

New Features and Functionality v11.7

- Windows 7 is no longer supported.
- Windows 10 2016 LTSB is no longer supported.

Resolved Security Advisories v11.7

- Encryption Personal third-party components have been updated.

Resolved Technical Advisories v11.7

Encryption v11.7

- Files that are required for installation are now properly removed after Encryption is uninstalled. [DDPC-12745]
- A message no longer displays and prompts for restart as a result of a Windows 10 upgrade after running WSDeactivate. [DDPC-12755]
- If Hibernation is enabled, the Hibernation option in the Windows Power menu now displays as expected. [DDPC-13376]
- The 32-bit and 64-bit Dell Encryption child installers details now display the following: **Dell Encryption Installer** [DDPC-13510]
- An issue resulting in inaccessible System Data Encryption keys and boot loop on computers protected by Policy-Based Encryption is resolved. [DDPC-13515, DDPSUS-3205]
- An issue resulting in incomplete and repeated encryption sweeps is resolved. [DDPC-13521, DDPSUS-3207, DDPSUS-3244]

Pre-boot Authentication v11.7

- An issue resulting in failure to sync passwords if using a third-party credential provider is resolved. [DDPC-13414, DDPSUS-3168]
- The PBA environment now displays the correct error if an incorrect password is entered. [DDPC-13454]

SED Manager v11.7

- An issue resulting in failure to sync passwords if using a third-party credential provider is resolved. [DDPC-13414, DDPSUS-3168]
- The PBA environment now displays the correct error if an incorrect password is entered. [DDPC-13454]

Technical Advisories v11.7

Encryption v11.7

- No technical advisories exist.

Pre-boot Authentication v11.7

- The PBA currently does not load on computers protected by SED Manager when multi-disk encryption is enabled and an additional unencrypted disk is added or replaced. As a workaround, bypass the PBA using Recovery. For more information, see *Perform a SED Recovery* in Encryption Recovery. [DDPC-13358]

SED Manager v11.7

- The PBA currently does not load on computers protected by SED Manager when multi-disk encryption is enabled and an additional unencrypted disk is added or replaced. As a workaround, bypass the PBA using Recovery. For more information, see *Perform a SED Recovery* in Encryption Recovery. [DDPC-13358]

New Features and Functionality v11.6

- DiagnosticInfo now collects additional logging information for the following:
  - Carbon Black Endpoint Detection and Response
  - Carbon Black AppDefense
- Encryption Personal now supports Windows 10 22H2.

Resolved Security Advisories v11.6

- No security advisories exist.

Resolved Technical Advisories v11.6

Encryption v11.6

- No technical advisories exist.

Pre-boot Authentication v11.6

- No technical advisories exist.

SED Manager v11.6

- No technical advisories exist.

Technical Advisories v11.6

Encryption v11.6

- After uninstalling Dell Encryption, Hibernation may not display in Windows advanced power settings. As a workaround, start command prompt as an administrator then run the following command:

  powercfg.exe /hibernate ON

  [DDPC-13376]

Pre-boot Authentication v11.6

- Computers protected by the PBA environment may not display the PIN authentication option after an operating system upgrade. As a workaround, use password authentication. [DDPC-13453]

SED Manager v11.6

- No technical advisories exist.

New Features and Functionality v11.9

- Bug fixes to improve user experience.
- Upgraded all server and client ISMs to Installshield 2023 R2.

Resolved Security Advisories v11.5

- No security advisories exist.

Resolved Technical Advisories v11.5

Encryption v11.5

- A message no longer displays and prompts for restart as a result of a Windows 10 upgrade after running WSDeactivate. [DDPC-12755]
- Verbose logging no longer decreases encryption and decryption sweep speed. [DDPC-13159]
- An issue resulting in accessible files if Fast User Switching is enabled is resolved. [DDPC-13161]
- A database issue resulting in intermittent computer crashes is resolved. [DDPSUS-3105]

Pre-boot Authentication v11.5

- The Legacy boot mode PBA environment now displays the correct URL for Dell Support. [DDPC-12536]

SED Manager v11.5

- A rare issue resulting in encryption status not displaying in the Data Security Console after a reboot is resolved. [DDPC-13101]

Technical Advisories v11.5

Encryption v11.5

- Encryption Personal currently does not provision as expected after installation and restart on VMWorkstation running Windows 11 with TPM enabled. As a workaround, reboot the computer a second time. [DDPC-12771]
- In-place OS upgrade from Windows 10 21H1 to Windows 11 22H2 is not currently supported for Encryption Personal installed on VMWorkstation. [DDPC-13292]

Pre-boot Authentication v11.5

- No technical advisories exist.

SED Manager v11.5

- No technical advisories exist.

New Features and Functionality v11.4

- Diagnostic Info now collects logging and troubleshooting data for Absolute Device and Data Security.
- DiagnosticInfo now collects logging and troubleshooting data for Dell Threat Defense.
- Dell Encryption now supports Windows 10 LTSC 2021.

Resolved Security Advisories v11.4

- The log4net component in the Data Security Uninstaller has been updated. [DDPC-13088]

Resolved Technical Advisories v11.4

Encryption v11.4

- The Dell End User License Agreement (EULA) has been updated to 2022 for all products and pages. [DDPC-12052]
- Encryption Personal now displays the following message if a user inputs the incorrect Encryption Administrator Password three times: **Maximum attempts reached. Please try after 15 Min.** [DDPC-12618]
- The Dell Encryption vault file, a secure container that stores policy and key information, is now located in C:\ProgramData\Dell\Dell Data Protection\Encryption\Vault. [DDPC-13005]
- Child installers and master installers are now install the Encryption Management Agent components to C:\Program Files\Dell\Client Security Framework. [DDPC-13006]
- An issue resulting in computer crash and incorrect designation of internal drives as external on computers protected by Encryption External Media is resolved. [DDPSUS-3109]
- An issue resulting in computer crash after updating Encryption Personal to v11.3 and applying Encryption External Media policies is resolved. [DDPSUS-3123]

Pre-boot Authentication v11.4

- If a Windows Feature update is blocked, the DellAgent.log file now includes entries detailing the block. [DDPC-12598]
- An issue resulting in unprinted outputs due to Caps Lock being enabled is resolved. [DDPC-13084]

SED Manager v11.4

- During uninstallation, SED Manager filter drivers are now properly unmounted. [DDPC-12461, DDPSUS-2925, DDPSUS-3054]
- A rare issue resulting in encryption status not displaying in the Data Security Console after a reboot is resolved. [DDPC-13101]

Technical Advisories v11.9

Encryption v11.9

- The Symlink is not getting detected in the C:\custom folder of your system. [DDPC-13822]

Pre-boot Authentication v11.9

- No technical advisories exist.

SED Manager v11.9

- No technical advisories exist.

New Features and Functionality v11.3

- DiagnosticInfo collects additional information including:
  - Class filter drivers in use
  - Dell Data Security product versions
  - Hardware serial numbers
  - Installed servers and their availability status
  - Windows build versions
  - Logs for the following:
    - Component-Based Servicing
    - Installed applications
    - Deployment Image Servicing and Management
    - Security Management Server installation
    - Server Configuration Tool and server migration
    - Threat Defense
    - VMware Carbon Black
    - Windows Updates

Resolved Security Advisories v11.3

- No security advisories exist.

Resolved Technical Advisories v11.3

Encryption v11.3

- DiagnosticInfo now identifies mishandled Command Line entries when run with the /silent option. [DDPC-10244]
- Uninstalling Dell Encryption now removes all Windows 10 Feature Update supporting folders as expected. [DDPC-12039]
- An issue resulting in an errant directory displaying in Dell Encryption logs is resolved. [DDPC-12854]
- When accessing the Recovery Keys or Advanced Settings in the Local Management Console, the following informational text now displays if Caps Lock is enabled: **Caps Lock is on** [DDPC-12661]
- Users can now navigate through Advanced Settings in the Local Management Console after inputting the correct password. [DDPC-12673]
- An issue resulting in the Local Management Console displaying a Sweep in Progress notification to unmanaged users is resolved. [DDPC-12674]

- Encryption Personal now displays the following error if the incorrect password is entered when changing the the Administrator Password in the Local Management Console: Password change failed. You do not have permission or the password you entered is invalid. [DDPC-12691]

Pre-boot Authentication v11.3

- An issue resulting in delays in the Pre-boot Authentication environment when using the TB16 dock is resolved. [DDPC-8147, DDPSUS-1923]
- An issue resulting in a freeze in the The Pre-boot Authentication environment is resolved. [DDPC-12758]
- A driver issue resulting in network cards being unavailable in the Pre-boot Authentication environment is resolved. [DDPC-12835, DDPSUS-2959, DDPSUS-2977]

SED Manager v11.3

- No technical advisories exist.

Technical Advisories v11.3

Encryption v11.3

- Encryption Personal currently fails to uninstall when using the Data Security Uninstaller and selecting the *Do not install Encryption Removal Agent* option. As a workaround, uninstall using the child installers. [DDPC-12771]
- Encryption Personal is not currently supported on VMware Workstation running Windows 11. [DDPC-12771]
- Encryption Personal currently mislabels some local accounts in the Local Management Console. [DDPC-12869]
- Windows Hello for Business authentication requires the following registry key if you install using the child installers:

  HKLM\SYSTEM\CurrentControlSet\Services\DellMgmtAgent\Parameters

  REG_SZ: NoDDPETray

  Value: 0 [DDPC-13001]
- When installed with the master installer, the directory in which Client Security Framework components are installed does not currently align with the directory created during installation with the child installers. [DDPC-13006]

Pre-boot Authentication v11.3

- No technical advisories exist.

SED Manager v11.3

- No technical advisories exist.

New Features and Functionality v11.2

- Encryption Personal v11.2 now supports Windows 11 v21H2.
- Encryption Personal v11.2 now supports Windows 10 v21H2.
- Dell Encryption now displays the following message in the notification area if a user attempts to upgrade to an unsupported version of Windows: **Dell Encryption is preventing an upgrade to an unsupported version of Windows. Contact Dell ProSupport for Software for assistance.**

Resolved Security Advisories v11.2

- No security advisories exist.

Resolved Technical Advisories v11.2

Encryption v11.2

- An issue that is caused by hardlink mapping mishandling resulting in high CPU use on computers that are protected by Dell Encryption is resolved. [DDPC-12407, DDPSUS-2983]
- Encryption External Media now honors policies more than 500 lines. [DDPC-12553, DDPSUS-2980]
- Files in OneDrive folders now decrypt as expected. [DDPC-12444]
- CMGAu no longer crashes when loading the Recovery Bundle for Encryption Personal. [DDPC-12735]
- An issue resulting in computer crash if abnormally large amounts of data were being processed by the file I/O buffer is resolved. [DDPC-12746, DDPSUS-3021]
- An issue resulting in computer crash due to coinciding high file transmission rates and file lock requests is resolved. [DDPC-12753, DDPSUS-3025]
- An issue resulting in locked user accounts due to incorrect credentials being processed during Fast User Switching is resolved. [DDPC-12780, DDPSUS-3026]

Pre-boot Authentication v11.2

- An issue resulting in delays in the Pre-boot Authentication environment is resolved. [DDPC-12758]

SED Manager v11.2

- No technical advisories exist.

Technical Advisories v11.2

Encryption v11.2

- After running WSDeactivate on a computer, a message incorrectly displays and prompts for restart as a result of a Windows 10 upgrade. This message should be ignored. [DDPC-12755]
- The following error message incorrectly displays when following the workflow to change Advanced Encryption settings in the Local Management Console and canceling before changes are made: **The username or password is incorrect**

  ⓘ **NOTE:** This error persists if you access Advanced Encryption settings following the previous workflow. [DDPC-12763]

- If a computer crash occurs before Dell Encryption activates, the vault is corrupted and automatic repair is not attempted. As a workaround, run WSDeactivate on the affected computer. [DDPC-12779]
- WinPE run on Windows 11 does not automatically mount the target disk. As a workaround, use the following steps:
  1. Type **x** and press Enter to exit to Command line.
  2. To open the Diskpart utility, type **diskpart** and press Enter.
  3. Type **list vol** and press Enter to list the available volumes.
  4. Type **select volume x** where **x** is the volume number.
  5. Use the **assign** command to assign a drive letter to that volume. For example, `assign C` and press Enter.
  6. Type **exit** to leave Diskpart.

  The target disk is mounted, and recovery can be performed. [DDPC-12848]

Pre-boot Authentication v11.2

- Dell platform BIOS from mid-2020 and earlier may not align with EFI-based certificate handling recently updated by Microsoft. This may result in the Dell Pre-boot Authentication environment failing to boot. To work around this incompatibility, ensure that the BIOS on your computer is updated. See this KB article 129365 for more information. [DDPC-12834]

SED Manager v11.2

- No technical advisories exist.

New Features and Functionality v11.1

- Installs and upgrades to Windows 11 and Windows 10 21H2 are not blocked with Encryption Personal v11.1. Dell does not support preview versions of operating systems and using unsupported operating systems may result in data loss. Go to KB article 156050 for additional Information on Windows operating system compatibility.
- The Encryption Administrator Password now protects against brute-force attacks with a cooldown timer that invokes a 15 minute lockout if the password is entered incorrectly three times.

Resolved Security Advisories v11.1

- The icon and verbiage for failed login attempts in the PBA environment have been aligned. [DDPC-12662]

Resolved Technical Advisories v11.1

Encryption v11.1

- An issue resulting in corruption of hard link files after new data is written is resolved. [DDPC-12079]
- An issue caused by policies with large character counts in a single policy resulting in the Local Management Console not properly displaying policies and displaying a 100 error code is resolved. [DDPC-12326]
- Files in OneDrive folders now decrypt as expected. [DDPC-12444]
- Interactive user detection no longer blocks all removable media if multiple users rapidly log in and out of the computer. [DDPC-12561]
- The child installers now extract from the master installer as expected on computers that have the Security Framework installed. [DDPC-12571]
- The Encryption Management Agent now provides the following error when unsupported Windows Feature Updates fail to install: **Dell Encryption is preventing an upgrade to an unsupported version of Windows. Contact Dell ProSupport for Software for assistance.** [DDPC-12597]
- A rare issue resulting in partial file corruption with files containing hard link based on their naming convention in tandem with rapid superceding updates is resolved. [DDPC-12693]

Pre-boot Authentication v11.1

- No technical advisories exist.

SED Manager v11.1

- No technical advisories exist.

Technical Advisories v11.1

Encryption v11.1

- The following error may display if you inspect a policy that exceeds nine KB of data:

  Invalid Value for 100 [DDPSUS-2980]
- When opening the **Advanced** pane in the Local Management Console, if the Encryption Management Password is entered incorrectly, the resulting error message displays multiple times. [DDPC-12677]
- Deleted users incorrectly display in the **Applies to** menu in the Local Management Console. [DDPC-12682]
- Modification of Encryption Personal policies now must be performed simultaneously, or an error displays. If multiple policies require modification, between each policy save, return to the home screen then reopen the **Advanced** pane of the Local Management Console. [DDPC-12683]
- When changing the password for removable media protected by Encrypted External Media, **Password Accepted** displays incorrectly. [DDPC-12721]
- The Data Security Console does not currently display information for protected removable media. [DDPC-12722]
- The Data Security Uninstaller currently does not uninstall properly if using the **Encryption Removal Agent - Import Keys from a File** option. As a workaround, use the **Encryption Removal Agent - Download Keys from Server** option, or uninstall by running the Dell Encryption child installer using the predownloaded key. [DDPC-12723]
- System Data Encryption validation failures on boot do not currently cause a computer crash as expected. An infinite boot logo displays instead. A System Data Encryption recovery should be performed for resolution. [DDPC-12725]
- Using Fast User Switching between inactivated users on a device running Encryption Personal may initiate an encryption sweep. [DDPC-12674]
- In rare instances, providing an incorrect current password to a device protected by Encryption External Media through the Local Management Console may result in a failed password update. As a workaround, recover the device using the Recovery Guide. [DDPC-12685]

Pre-boot Authentication v11.1

- External smart card readers do not currently function properly when used in the Pre-Boot Authentication environment on Dell models that are generated in calendar year 2020 or later due to a change in the BIOS of these computers. [DDPC-12730]

SED Manager v11.1

- No technical advisories exist.

New Features and Functionality v11.0

- Encryption Personal is now supported with Windows 10 v21H1 (May 2021 Update/21H1)
- The Kioxia BG4 NVMe is now supported with SED Manager.
- Encryption Personal now supports Microsoft and Office 365 Accounts.

Resolved Security Advisories v11.0

- The Encryption Personal signing certificate is updated.

Resolved Technical Advisories v11.0

Encryption v11.0

- External Media Encryption's installation description is updated to clarify functionality of the product. [DDPC-12367, DDPC-12368]
- Copyrights are updated. [DDPC-12378]
- With a global shift to inclusive language, several terms and expressions have been updated. [DDPC-12398]

Pre-boot Authentication v11.0

- No technical advisories exist.

SED Manager v11.0

- The Encryption Management Agent now performs additional checks during installation and uninstallation to detect if the computer was rebooted. This prevents an inaccessible boot drive. [DDPC-12390, DDPSUS-2925]

Technical Advisories v11.0

Encryption v11.0

- The Dell Encryption Removal agent may not decrypt hydrated OneDrive files. To decrypt these files, either unlink OneDrive, or decrypt these files before uninstall through policy. [DDPC-12444]
- WSDeactivate currently displays a non-functional progress bar. [DDPC-12502]

Pre-boot Authentication v11.0

- Computers leveraging Microsoft-based accounts and protected by SED Manager with the *Sync Users at PBA Activation* policy enabled currently cannot use single sign-on after rebooting. As a workaround, at the Windows sign-in screen, select **Other User** and log in using your user name and password. Single sign-on is functional for the local users and Active Directory domain users if the system is domain-joined. [DDPC-12089]

SED Manager v11.0

- Computers leveraging Microsoft-based accounts and protected by SED Manager with the *Sync Users at PBA Activation* policy enabled currently cannot use single sign-on after rebooting. As a workaround, at the Windows sign-in screen, select **Other User** and log in using your user name and password. Single sign-on is functional for the local users and Active Directory domain users if the system is domain-joined. DDPC-12089

New Features and Functionality v10.10

- No technical advisories exist.

Resolved Security Advisories v10.10

- The Encryption Personal signing certificate is updated.

Resolved Technical Advisories v10.10

Encryption v10.10

- The decryption agent now properly decrypts Cloud-based files regardless of hydration status. [DDPC-11556, DDPSUS-2895]
- The Encryption External Media service now starts as expected on computers that do not have Dell Encryption installed. [DDPC-12101, DDPC-12196]
- An issue resulting in double-encrypted files with superseding file versions is resolved. [DDPC-12302]

Pre-boot Authentication v10.10

- No technical advisories exist.

SED Manager v10.10

- No technical advisories exist.

Technical Advisories v10.10

Encryption v10.10

- No technical advisories exist.

Pre-boot Authentication v10.10

- No technical advisories exist.

SED Manager v10.10

- No technical advisories exist.

New Features and Functionality v10.9

- Encryption Personal is now supported with Windows 10 v20H2 (October 2020 Update/20H2).
- Encryption Personal now supports disks with 4k sector formats.
- The Dell Encryption PBA now supports Brazilian ABNTv2 keyboards.

Resolved Security Advisories v10.9

- No security advisories exist.

Resolved Technical Advisories v10.9

Encryption v10.9

- If a duplicate user attempts to activate with Deferred Activation, the following message displays: **Activation Failed & the user is already activated on this computer.** [DDPC-7456]
- An issue resulting in a memory leak due to file name length is resolved. [DDPC-7569]
- Encryption Personal logs now display the correct product name. [DDPC-11637]
- An issue resulting in the Dell DiagnosticInfo utility detecting a client operating system as a server operating system is resolved. [DDPC-11762]
- Encryption External Media now displays on the component selection screen when upgrading Dell Encryption. [DDPC-11998]
- An issue resulting in the inability to use smart card login from a remote location is resolved. [DDPC-12068, DDPC-12290, DDPSUS-2821]
- An issue resulting in incomplete feature installation when installing with the master installer using command-line or interactively is resolved. [DDPSUS-2870, DDPSUS-2908, DDPC-12090]
- Block SID functionality with multiple disks is improved. [DDPC-12183]
- An issue resulting in inaccessible data and unresponsive Start menu after Windows 10 Feature Update failure is resolved. [DDPC-12121, DDPSUS-2844, DDPSUS-2854]
- An issue resulting in inaccessible data due to mishandling of System Disk Encryption keys is resolved. [DDPC-12123, DDPSUS-2850]
- An issue resulting in encryption sweep failures on computers protected by Dell Encryption and VMWare Carbon Black Cloud or many anti-virus solutions is resolved. [DDPC-12205, DDPSUS-2883]
- An issue resulting in failed provisioning for computers protected by Dell Encryption is resolved. [DDPC-12289, DDPSUS-2893, DDPSUS-2906]
- An issue resulting in nonfunctional shortcuts after completing an encryption sweep is resolved. [DDPC-12265]
- An issue resulting in failed Dell Encryption reactivation due to a corrupt System Disk Encryption key vault is resolved. [DDPC-12255]
- An issue resulting in failed Windows 10 Feature Updates and computer crash due to a corrupt System Data Encryption key vault is resolved. [DDPSUS-2862]
- An issue resulting in inaccessible files due to System Data Encryption key handling is resolved. [DDPSUS-2867]

Pre-boot Authentication v10.9

- The Pre-boot Authentication environment now displays the correct version in the *About* section. [DDPC-11995]

SED Manager v10.9

- No technical advisories exist.

Technical Advisories v10.9

Encryption v10.9

- Devices with multiple disks may not display the status of disks immediately when selecting the Encryption tab in the Data Security Console . [DDPC-11346]
- If Policy-Based Encryption is installed before the Encryption Management Agent, computer crash may occur. This issue is caused by failure to load the encryption Sleep driver which is used to manage the PBA environment. As a workaround, use the master installer or ensure that Policy-Based Encryption is installed after the Encryption Management Agent. [DDPC-12239]

Pre-boot Authentication v10.9

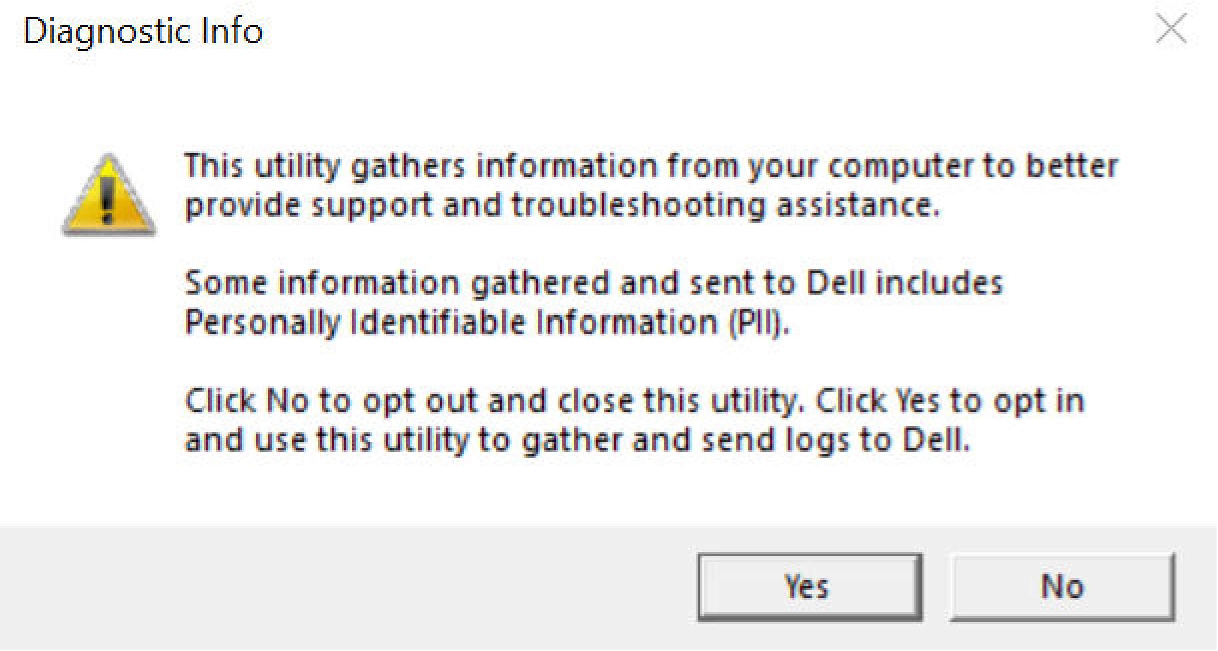
- No technical advisories exist.

SED Manager v10.9

- No technical advisories exist.

New Features and Functionality v10.8

- The DiagnosticInfo utility is now installed when the Encryption Management agent is installed.
- The DiagnosticInfo utility now queries additional registry entries.
- The master installer's detection of UEFI and Legacy boot modes is improved.
- The Dell Encryption WinPE recovery environment verbiage is updated for Self-Encrypting Drives .
- The DiagnosticInfo utility now displays the following prompt for Personally Identifiable Information:



Diagnostic Info

This utility gathers information from your computer to better provide support and troubleshooting assistance.

Some information gathered and sent to Dell includes Personally Identifiable Information (PII).

Click No to opt out and close this utility. Click Yes to opt in and use this utility to gather and send logs to Dell.

- If Encryption is not activated on the computer, Encryption Personal now displays a **Don't Ask Again** checkbox. If the user intends to activate Encryption later and selects this option, change the following registry value:
  - HKCU\Software\Dell\Dell Data Protection\Encryption

    "HidePasswordPrompt"=DWORD

    1 = disables the password prompt for Encryption Personal activation

    0 = enables the password prompt for Encryption Personal activation
- SED Manager now supports the following platforms:
  - Latitude 9510
  - Latitude 9510 2-in-1
  - XPS 15 9500

Resolved Security Advisories v10.8

- Additional files used during the installation of Encryption Personal are now signed. [DDPC-6827]

- Dell has released additional fixes for an improper access control vulnerability in Encryption Personal (CVE-2020-5358). See the Dell Security Advisory (DSA-2020-113) at https://www.dell.com/support/security/ for affected products, versions, and additional information. [DDPC-11877]

Resolved Technical Advisories v10.8

Encryption v10.8

- Custom Support Dialog is now properly consumed against a Security Server with nondefault ports when set. [DDPC-8060]
- Deferred activation now activates properly against a Security Server with nondefault ports. [DDPSUS-2762]
- Unsupported languages no longer display in help directories after installing Encryption Personal. [DDPC-10746]
- Encryption Personal logs now display the correct product name. [DDPC-11637]
- Nonadministrator users now receive the following error when attempting to change the backup location for Disk Encryption keys: **Local Administrator rights are required to specify an alternate backup location for the Dell Encryption recovery bundle.** [DDPC-11756]
- Reboot prompts no longer display on the login screen after decryption. [DDPC-11940]

Pre-boot Authentication v10.8

- When using Recovery Questions to log in through the PBA, the password reset prompt now only appears for the first 90 seconds after login. [DDPC-11671]
- Right-clicking the username, password, smart card, pin or recovery answer field in the PBA no longer yields a menu. [DDPC-11795]
- An issue resulting in third-party authentication providers being disabled by default is resolved. [DDPC-12057, DDPSUS-2818]

SED Manager v10.8

- No technical advisories exist.

Technical Advisories v10.8

Encryption v10.8

- During reboot and shutdown, a .NET error may display due to simultaneous shutdown of a Dell Encryption service and Windows WMI service. [DDPC-12054, DDPC-12098, DDPSUS-2807, DDPSUS-2812]
- In rare scenarios, the DiagnosticInfo utility does not collect all logs after Command-line installation and failed exportation errors display in the Command-line window. [DDPC-12090]
- Administrators are currently unable to change disk encryption keys' escrow location after encryption sweeps are complete. [DDPC-12100]

Pre-boot Authentication v10.8

- No technical advisories exist.

SED Manager v10.8

- No technical advisories exist.

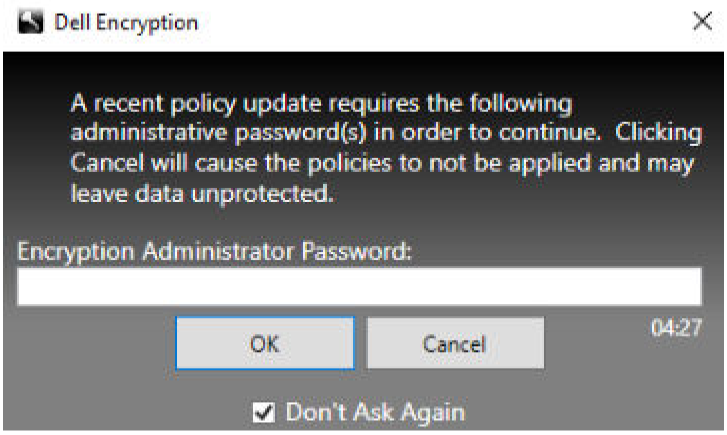
New Features and Functionality v10.7

- Encryption Personal is now supported with Windows 10 v2004 (May 2020 Update/20H1).
- Encryption Personal now can locate and escrow encryption keys to mapped network drives.
- The Dell DiagnosticInfo utility logging is improved.
- Boot order logging is improved.
- A new RAID controller driver is added to the Dell Encryption Recovery WinPE environment. This enables recovery of disks in newer platforms configured in RAID ON mode.
- Dell Encryption performs a re-analysis of encrypted volumes on key backups to ensure policy is correctly applied to the entire drive. This will appear as a re-sweep of encryption of the disk, which may lead to a temporary increase in system resource use.
- Encryption Personal now displays a **Don't Ask Again** again checkbox if Encryption is not activated on the computer. If the user intends to activate Encryption at a later date and selects this option, delete the following registry value:

  HKEY_Current_User\Software\Credant\CMGShield\

  REG_SZ (string) - PasswordPromptKey

  Value = HidePasswordPrompt



Dell Encryption

A recent policy update requires the following administrative password(s) in order to continue. Clicking Cancel will cause the policies to not be applied and may leave data unprotected.

Encryption Administrator Password:

- The Encryption Personal Data Security Console now displays the following message if a user attempts to add a new user before enabling the PBA:

  Note: Protection must be enabled to add users.

- Encryption Personal now prompts the user to reboot their computer after the Encryption Removal Agent finishes its final state in the decryption process. This prompt can be disabled by configuring the following registry value.

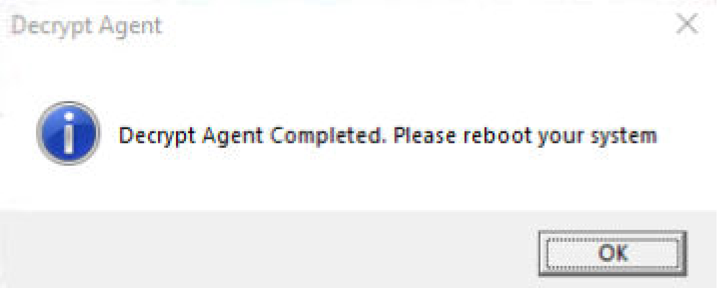
  HKLM\Software\Dell\Dell Data Protection

  "ShowDecryptAgentRebootPrompt"=DWORD

  Default = enabled

  1 = enabled (displays prompt)

  0 = disabled (hides prompt)



Decrypt Agent

Decrypt Agent Completed. Please reboot your system

- SED Manager now supports the following platforms:
  - Latitude 5411
  - Latitude 5511

  - Latitude 9410 2-in-1
  - OptiPlex 5480 All-in-One
  - OptiPlex 7480 All-in-One
  - OptiPlex 7780 All-in-One
  - Precision 3440
  - Precision 3551
  - Precision 7550
  - Precision 7750
  - XPS 15 9500

Resolved Technical Advisories v10.7

Encryption v10.7

- Dell Encryption files are now properly cleaned up during uninstallation. [DDPC-866, DDPC-2548, DDPC-11094, DDPC-11497]
- A rare issue resulting in the DiagnosticInfo utility failing to generate a temporary directory for data collection before packaging is resolved. [DDPC-4981]
- An issue resulting in installation files being improperly flagged as threats is resolved. [DDPC-6827, DDPC-11573, DDPC-11844. DDPC-11846]
- The Encryption Personal installation logs now display the correct error message when the registry value located at HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order is missing during installation. [DDPC-8397, DDPSUS-2171]
- Installed versions of Encryption Personal that are not activated no longer fail to upgrade to newer versions. [DDPC-10973]
- The Data Security Uninstaller now accepts upper case and lower case entries of the *silent* Command-line switch (*Silent* and *silent*). [DDPC-11092]
- An issue resulting in failed activation on computers leveraging multiple domains and users is resolved. [DDPC-11479, DDPC-11840, DDPSUS-2648]
- The master installer now displays text correctly in German on the *InstallShield Wizard Complete* screen. [DDPC-11501]
- An issue resulting in computer crash after mounting and unmounting removal media is resolved. [DDPC-11555]
- The HCA driver is no longer installed when installing Encryption Personal. [DDPC-11576]
- Encryption Personal now requires that SED Manager is enabled and the PBA is active before additional users can be added. If a user attempts to add a user before satisfying these prerequisites, an error displays. DDPC-11669
- The Data Security Uninstaller no longer displays overlapping windows on the Latitude 7370. [DDPC-11791]
- An issue resulting in failed activation due to the inability to locate a user in the vault is resolved. [DDPC-11840, DDPSUS-2734]
- Encryption sweeps no longer yield an error due to a mishandled vault code. [DDPC-11849, DDPSUS-2759]
- Dell has released fixes for an improper access control vulnerability in Encryption Personal (CVE-2020-5358). See the Dell Security Advisory (DSA-2020-113) at https://www.dell.com/support/security/ for affected products, versions, and additional information. [DDPC-11877]
- An issue resulting in computer crash if the Encryption Management Agent is installed on a computer with Credant Mobile Guardian v7.x is resolved. [DDPC-11890, DDPSUS-2763]
- Files on Demand and .PST file types no longer fail to sync to Onedrive on computers protected by Dell Encryption. [DDPC-11963, DDPSUS-2799, DDPSUS-2800]
- Large recovery bundles no longer encounter a timeout and subsequently fail to download from the Dell Server. [DDPC-11972, DDPSUS-2713]

Pre-boot Authentication v10.7

- Keyboard mapping on Swiss French keyboards now function as expected on the Latitude 7490. [DDPC-11122, DDPSUS-2579]

SED Manager v10.7

- Selecting a username in the Data Security Console no longer results in an unhandled exception error. [DDPC-11642]

- An issue resulting in the Dell Credential provider resetting the password field as a user attempts to log in after logging off or unlocking the computer is resolved. [DDPC-11826, DDPSUS-2739]

Technical Advisories v10.7

Encryption v10.7

- Dell Encryption cannot be upgraded to v10.7.0 from versions earlier than v8.16.0. Endpoints running versions prior to v8.16.0 must upgrade to v8.16.0 then upgrade to v10.7.0 . [DDPC-11576]
- After decrypting a computer, a prompt to reboot the computer may display on the login screen. [DDPC-11940]
- In rare situations, upgrades using the DDSSetup installer fail and an error displays on subsequent update attempts detailing that the application is already updated. As a workaround, upgrade specific components using the child installers. [DDPC-11993]
- If updating an endpoint running Dell Encryption with the DDSSetup installer interactively, the External Media Encryption option may not display in the feature selection screen. [DDPC-11998]

Pre-boot Authentication v10.7

- The *About* section in the PBA environment currently lists the incorrect version number. [DDPC-11995]

SED Manager v10.7

- No technical advisories exist.

New Features and Functionality v10.6

- Dell's DiagnosticInfo utility now queries additional registry entries for more comprehensive results.
- SED Manager now supports the following platforms:
  - Latitude 7070 Tower

    Note: This platform was incorrectly listed as supported in v10.5 Technical Advisories.

  - OpiPlex 7080 Tower

Resolved Technical Advisories v10.6

Encryption v10.6

- An issue resulting in the inability to decrypt and uninstall if multiple System Data Encryption keys were present in the registry is resolved. [DDPC-2428, DDPC-11662, DDPSUS-2208]
- An issue resulting in ERR files after changing policy to Single Overwrite Pass during a System Data Encryption sweep is resolved. [DDPC-2751, DDPC-5038, DDPC5148, DDPC-7708, DDPC-8019, DDPC-8116]
- The reboot prompt no longer displays off-screen after a policy requiring a reboot is updated. [DDPC-5374, DDPC-5376]
- The Data Security Uninstaller now removes all Dell Encryption registry entries as expected. [DDPC-5410]
- An issue resulting in the inability to configure encryption after installing Encryption Personal is resolved. [DDPC-11390, DDPC-11618]
- Encryption Personal can now be uninstalled through Control Panel and Apps & features as expected. [DDPS-11634]
- An issue that triggered System Data Encryption recovery after Windows updates is resolved. [DDPC-11667]
- An issue caused by corrupt vault entries that resulted in cmgshieldsvc.exe and computer crash is resolved. [DDPC-11720]

Pre-boot Authentication v10.6

- Smart cards leveraging compressed certificates now function as expected. [DDPC-11769]

SED Manager v10.6

- An issue resulting in domain-added users failing to authenticate when a third-party credential provider is in use after an administrator invoked password change is resolved. [DDPC-11654, DDPSUS-2506, DDPSUS-2695]
- An issue resulting in computers starting up automatically after hibernating or shutting down is resolved. [DDPC-11751]

Technical Advisories v10.6

Encryption v10.6

- In January 2020, SHA1 signing certificates are no longer valid and cannot be renewed. Devices running Windows 7 or Windows Server 2008 R2 must install Microsoft KBs https://support.microsoft.com/help/4474419 and https://support.microsoft.com/help/4490628 to validate SHA256 signing certificates on applications and installation packages.

  Applications and installation packages signed with SHA1 certificates will function but an error will display on the endpoint during installation or execution of the application without these updates installed.

Pre-boot Authenticationv10.6

- No technical advisories exist.

SED Managerv10.6

- No technical advisories exist.

New Features and Functionality v10.5

- Swedish keyboards are now supported by the Pre-boot Authentication environment.
- Dell Encryption now supports additional Windows smart card Credential Providers.
- Encryption Personal now supports Windows 10 v1909 (November 2019 Update\19H2).
- SED Manager now supports the following platforms:
  - Latitude 3310
  - Latitude 3310 2-in-1
  - Latitude 5401
  - Latitude 5403
  - Latitude 5501
  - Latitude 7220 Rugged Extreme Tablet
  - Latitude 7300
  - OptiPlex 3070 All-in-One
  - OptiPlex 5070 Tower, Small Form Factor, Micro
  - Optiplex 5270 All-In-One
  - OptiPlex 7070 Tower, Small Form Factor
  - Optiplex 7770 All-In-One
  - Precision 3431 Desktop Workstation
  - Precision 3540
  - Precision 3541

Resolved Technical Advisories v10.5

Encryption v10.5

- An issue resulting in corrupted files created by Notepad++ and Onenote is resolved. [DDPC-11440, DDPSUS-2385, DDPSUS-2642]
- An issue resulting in files not encrypting after a change in encryption algorithm is resolved. [DDPC-11460]
- A rare occurrence resulting in the Change Password option to not display at Windows login is resolved. [DDPC-11400]
- Installing Dell Encryption with older versions of Encryption Management Agent now creates independent system tray icons for each product. [DDPC-11052, DDPC-11279]

Pre-boot Authentication v10.5

- Boot time when the Pre-boot Authentication environment is present is improved. [DDPC-11042, DDPC-11422, DDPSUS-2471]
- Swiss French keyboard mapping now functions as expected in the Pre-boot Authentication environment. [DDPC-11122, DDPSUS-2579]

SED Manager v10.5

- No technical advisories exist.

Technical Advisories v10.5

Encryption v10.5

- Added 12/2019 - In January 2020, SHA1 signing certificates are no longer valid and cannot be renewed. Devices running Windows 7 or Windows Server 2008 R2 must install Microsoft KBs https://support.microsoft.com/help/4474419 and https://support.microsoft.com/help/4490628 to validate SHA256 signing certificates on applications and installation packages.

  Applications and installation packages signed with SHA1 certificates will function but an error will display on the endpoint during installation or execution of the application without these updates installed.
- In rare occurrences, computers leveraging eMMC drives will crash in Dell.SecurityFramework.Agent.exe, causing a Stop 0x74 CRITICAL_PROCESS_DIED BSOD, when restarting the computer after applying encryption. [DDPC-11461]
- The German installer contains improperly formatted text. [DDPC-11501]
- In rare cases, encryption sweeps yield an error due to a mishandled vault code. [DDPC-11849, DDPSUS-2759]

Pre-boot Authenticationv10.5

- When leveraging smart cards for PBA activation, the Sync Users at PBA Activation policy must be disabled in the Dell Server. [DDPC-11543]

SED Managerv10.5

- No technical advisories exist.

New Features and Functionality v10.4

- Dell Encryption's DDSSetup and DDSSuite installers have been updated to resolve CVE-2016-2542.
- Dell has added verbosity in the Policy-Based Encryption logs when performing Windows 10 Feature Updates.

- SED Manager now supports the following platforms:
  - Latitude 5403
  - Precision 5540
  - Precision 7540
  - Precision 7740
  - XPS 7390
  - XPS 7390 2-in-1
  - XPS 7590

Resolved Technical Advisories v10.4

Encryption v10.4

- LSARecovery files generated by Encryption Personal are now compatible with a 32-bit or 64-bit WinPE. [DDPC-1116]
- The master uninstaller now removes all files and folders as expected. [DDPC-9468]
- An issue resulting in the Encryption service failing after activation and, in rare occurrences, operating system crashes is resolved. [DDPC-11011, DDPC-10952, DDPC-10953, DDPSUS-2543]
- Multi-user and domain-based computers no longer invoke activation loss or fail to achieve policy compliance regardless of authentication method or sequence. [DDPC-11053, DDPC-11066]
- Encryption Personal now prompts local users to activate on reboot as expected. [DDPC-10825, DDPC-10974, DDPC-10975]
- A race condition resulting in an unusable system due to no Credential Providers available at the Windows login screen is resolved [DDPC-10936]
- The Local Management Console no longer crashes when accessed by a non-administrative user. [DDPC-11093, DDPC-11123, DDPSUS-2559]
- An issue resulting in the Encryption service crashing after attempting to take ownership of a TPM is *Cleared* state is resolved. [DDPC-11095, DDPSUS-2565]
- An issue resulting in failure to write the Encryption mode in use to registry is resolved. [DDPC-11125]
- An issue resulting in a crash if changing crypto libraries with HVCI enabled is resolved. This issue could present when upgrading from versions prior to v10.0 to v10.1 or later. [DDPC-11178, DDPC-11293, DDPC-11506, DDPSUS-2572, DDPSUS-2598]
- An issue resulting in a crash due to failed policy processing is resolved. [DDPC-11207, DDPSUS-2597]
- An issue in Dell Encryption resulting in untranslated text during a Windows 10 Feature Update is resolved. [DDPC-11381]
- An issue resulting in a crash after applying KB4512941 on a computer protected by Encryption is resolved. [DDPC-11320, DDPSUS-2662]
- An issue resulting in the inability to install Cadence, orCAD, and Allegro with Encryption present on the target computer is resolved. [DDPC-11420, DDPSUS-2630]
- An exception resulting in the Encryption service crashing is resolved. [DDPC-11425, DDPSUS-2629]
- An issue resulting in system crash caused by a new file classification starting in KB4515384 and KB4512941 is resolved. For more information, see KB article SLN318627. [DDPC-11505]
- An issue resulting in Encryption moving to an unmanaged state after a Windows Feature Update is resolved. [DDPC-10545, DDPC-10569]

Pre-boot Authentication v10.4

- An issue resulting in a delay if a Dell Server was unavailable at in the Pre-boot Authentication environment is resolved. [DDPC-4503, DDPC-8098, DDPSUS-2277]
- Challenge/Response Recovery now functions as expected in Legacy boot mode when multiple user certificates are in use. [DDPC-4503, DDPC-10816]
- The Pre-boot Authentication environment no longer freezes when authenticating a user with cached smart-card credentials. [DDPC-8072, DDPC-8696]
- Users can now enroll Recovery Questions using a mouse or keyboard. [DDPC-9143]
- Users can now enroll Recovery Questions as expected. [DDPC-9972, DDPC-10503]
- Legal Notice and Support Information fields in the Pre-boot Authentication environment now display text as expected. [DDPC-11026, DDPSUS-2545]
- The Pre-boot Authentication environment now properly displays copyright dates on the Network and Support pages. [DDPC-10740]

- Challenge/Response Recovery now functions as expected in UEFI boot mode. [DDPC-10815]
- An issue resulting in duplicate DHCP requests in the Pre-Boot Authentication environment is resolved. This fix reduces boot time. [DDPC-11366]

SED Manager v10.4

- An issue resulting in smartcard login being unavailable for devices protected by SED Manager after resuming from sleep is resolved. [DDPC-8284]

Technical Advisories v10.4

Encryption v10.4

- After installing Dell Encryption, the Support pane in the Data Security Console displays a blank page until the device activates, or an internet connection is available. [DDPC-8059]
- When Policy Based Encryption and any technology managed by the Encryption Management Agent is installed, removable media may not consistently appear as removable in the Data Security Console and the Security Management Server. [DDPC-9736]
- The Encryption Management Agent no longer outputs policies by default. To output current and newly consumed policies, create the following registry key:

  HKLM\Software\Dell\Dell Data Protection\

  DWORD: DumpPolicies

  Value=1

  Note: a reboot is not required for this change to take effect. [DDPC-9786]
- When using Policy-Based Encryption with a version prior to v10.0 and the Encryption Management Agent with v10.0 or newer, Policy Based Encryption's status does not properly display in the Data Security Console. [DDPC-11052]
- The following registry key prevents lock screen applications from properly functioning until a user has logged into the device. This key is enabled by default to ensure that user activation and key unlock is not impeded.

  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

  DWORD: DisableAutomaticRestartSignOn

  Value: 1 [DDPC-10825]
- The master uninstaller currently requires all lower-case characters with the /silent command. Running with camel-case or upper case characters will prevent the uninstaller from running. [DDPC-11092]
- Before a reboot, Dell recommends properly closing any files open in applications that leverage temporary files to store changes. Failure to properly close these files could result in data loss. [DDPC-11440]

Pre-boot Authenticationv10.4

- The XPS 7390 touchpad functions improperly after the Pre-boot Authentication environment is created. After logging into Windows, the touchpad functions properly. To work around this issue, use the Tab key to transition between dialog boxes and options. [DDPC-11306]
- In rare occurrences, when the Pre-boot Authentication environment is created, the boot order may be set incorrectly on reboot. [DDPC-11504]

SED Managerv10.4

- No technical advisories exist.

New Features and Functionality v10.3

- Pre-boot Authentication now supports block SID features.
- Dell Encryption now supports Micron 1300 self-encrypting drives.
- Dell Encryption now supports the following platforms:
  - Latitude 5300
  - Latitude 5500
  - Latitude 7200 2-in-1
  - Latitude 7400
  - Latitude 7400 2-in-1

Resolved Technical Advisories v10.3

Encryption v10.3

- An issue resulting in failed user activation when a smart card is in use with Policy Based Encryption is resolved. [DDPC-9686, DDPC-9808, DDPC-10592, DDPC-10592, DDPSUS-2402, DDPSUS-2425, DDPSUS-2450]
- An issue resulting with Windows 10 Work Folders failing to sync when attempting to sync encrypted files is resolved. [DDPC-10400, DDPSUS-2269, DDPSUS-2394, DDPSUS-2407]
- Decryption of EMS devices from any endpoint is now enabled. [DDPC-10564, DDPC- 10781, DDPSUS-2421, DDPSUS-2467]
- An issue resulting in the Encryption Management Agent and Policy Based Encryption installers failing to determine the installation status of newer VC++ 2017 versions is resolved. These prerequisites may be bypassed through MSI installation. Contact Dell ProSupport to acquire MSI installers. [DDPC-10654, DDPC-10888]
- Encryption sweeps now function as expected after upgrading a computer protected by Dell Encryption in Encryption External Media mode. [DDPC-10828, DDPSUS-2508]
- An issue resulting in a crash if Microsoft's .Net Framework is corrupted on a computer protected by Dell Encryption is resolved. [DDPC-10871, DDPSUS-2519]
- A rare issue resulting in a crash during a Policy Based Encryption upgrade with Secureboot enabled is resolved. [DDPC-10954, DDPSUS-2572, DDPSUS-2534]
- Devices protected by Encryption External Media and white-listed no longer require a manual recovery of the encrypted files on the drive. [DDPC-10957]

Pre-boot Authentication v10.3

- When enabling the Pre-Boot Authentication environment for Dell Encryption, the boot order no longer reverts to PXE boot when it is enabled in BIOS. [DDPC-4334, DDPC-8377, DDPC-8378, DDPC-10961, DDPSUS-2176, DDPSUS-2456]
- An issue resulting in the Pre-boot Authentication environment failing to properly recognize some keys on non-English keyboards is resolved. [DDPC-8154, DDPC-10713, DDPSUS-1656, DDPSUS-2415]

  NOTE: This fix requires the BIOS update launched in late April 2019 or in May 2019. The BIOS revision and release date will vary based on the platform affected. If the BIOS update is applied before Dell Encryption is installed on devices with US English keyboards, the Pre-boot Authentication environment may not properly translate all characters.

- An issue that resulted in the *Challenge Response* screen displaying in place of the password authentication screen after exceeding recovery questions attempts on a Legacy computer with PBA active is resolved. [DDPC-9426]
- An issue resulting in sleep mode failing on an Optiplex 7060 when Dell Encryption and SED management are both activated after an upgrade to Windows 10 October 2018 update is resolved. [DDPC-10410]
- An issue resulting in a malformed Pre-boot Authentication database due to incorrect updates to the Pre-boot Authentication environment's datastore is resolved. Primary and secondary datastores now properly validate data and rotate. [DDPC-10757, DDPSUS-2482]
- A delay during login when selecting the option to run as a different user in Windows with Pre-boot Authentication enabled is resolved. [DDPC-10956] [DDPSUS-2531]

SED Management v10.3

- Dell Encryption now allows registry-based overrides to prevent disabling third-party credential providers after the Pre-boot Authentication environment is enabled. To prevent Dell Encryption from disabling third-party credential providers, create the following registry key:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0=Disabled (default)

  1=Enabled

  [DDPC-10542, DDPSUS-2410, DDPSUS-2412, DDPSUS-2506]

Technical Advisories v10.3

Encryption v10.3

- In rare occurrences, when the TPM is in a cleared state in BIOS, Dell Encryption may attempt to take ownership of the TPM and receives a null value. In this situation the Dell Encryption service may crash, resulting in an operating system crash. As a work around, if the TPM is in a cleared state, fully disable the TPM. [DDPC-11095, DDPSUS-2565]

Pre-boot Authentication v10.3

- No technical advisories exist.
- In rare instances, when using Recovery Questions in the Pre-Boot Authentication environment, the expected workflow of a password reset is not properly presented once the device transitions into Windows. [DDPC-11660]

SED Management v10.3

- After logging in through the PBA, the Data Security Console may appear when hotkeys are leveraged within the operating system to close applications. [DDPC-9344]

New Features and Functionality v10.2.1

- No technical advisories exist.

Resolved Technical Advisories v10.2.1

Encryption v10.2.1

- An incompatibility issue with Windows 10 March Cumulative Update that resulted in UI errors and missing activation information is resolved. [DDPC-10944, DDPSUS-2537]

Pre-boot Authentication v10.2.1

- No resolved technical advisories exist.

Technical Advisories v10.2.1

Encryption

- No technical advisories exist.

Pre-boot Authentication v10.2.1

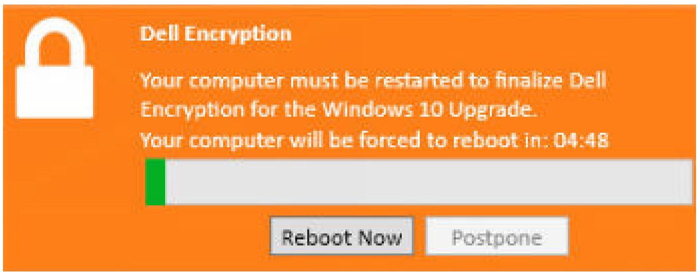
- No technical advisories exist.

SED Management v10.2.1

- No technical advisories exist.

New Features and Functionality v10.2

- Following Windows 10 feature upgrade, a restart is **required** to finalize Dell Encryption. The following message displays in the notification area after Windows 10 feature upgrades:



Dell Encryption

Your computer must be restarted to finalize Dell Encryption for the Windows 10 Upgrade.

Your computer will be forced to reboot in: 04:48

Resolved Technical Advisories v10.2

Encryption v10.2

- An issue that caused operating system crash following an Windows update is resolved.[DDPC-5664, DDPC-9457, DDPSUS-1356, DDPSUS-1409, DDPSUS-2216]
- An issue with the Dell Authentication Service resulting in the inability to register recovery questions is resolved. [DDPC-9972, DDPC-10503, DDPC10528, DDPC-10620]
- Encryption sweeps now process as expected following upgrades. [DDPC-10168]
- An issue resulting in inaccessible files protected by Encryption External Media is resolved. [DDPC-10251, DDPSUS-2318, DDPSUS-2408]
- An issue resulting in loss of smart card functionality with previously activated users is resolved. [DDPC-10592, DDPSUS-2402, DDPSUS-2425]
- An issue that resulted in intermittently inaccessible Microsoft Office documents following an upgrade to Dell Encryption is resolved. [DDPC-10606, DDPSUS-2392]
- An issue that resulted in crashes following an update to Dell Encryption v10.1 is resolved. [DDPC-10676, DDPSUS-2469]
- An issue that resulted in excessive logging is resolved. [DDPC-10679, DDPSUS-2449]

Pre-boot Authentication v10.2

- An issue that resulted in a parity error after activating pre-boot authentication with Dell Encryption installed on a Latitude 7404, Latitude 7204, or a Latitude 5404 Rugged computer in Legacy boot mode is resolved. [DDPC-9493, DDPC-10748, DDPSUS-2225]
- The K13A Rugged dock (only compatible with Rugged computers) no longer requires the an open lid to display on external monitors. [DDPC-10093]
- Recovery question user experience is improved. [DDPC-10544, DDPC-10543, DDPC-10640]
- The **Sign In** button is no longer enabled following initial activation of the pre-boot authentication. [DDPC-10615]
- An issue in the pre-boot authentication environment that resulted in various keys on Japanese keyboards not displaying or displaying incorrectly on the Latitude E7280 is resolved. [DDPC-10639, DDPSUS-1656]
- Users logging in with recovery questions are now able to change their Windows password as expected. []

Technical Advisories v10.2

Encryption

- No technical advisories exist.

Pre-boot Authentication v10.2

- No technical advisories exist.

SED Management v10.2

- No technical advisories exist.

New Features and Functionality v10.1

- Added 12/2018 -
  - Dell Encryption is now supported with Windows 10 October 2018 Update (Redstone 5 release).
  - SED management and Bitlocker manager are now supported with Windows 10 October 2018 Update (Redstone 5 release).
- Dell Encryption v10.1 and later defaults to leveraging a new cryptographic library, provided by RSA, as well as multiple new options for cryptographic libraries. For more information, see http://www.dell.com/support/article/us/en/19/SLN301500.
- HP EliteBook 840 G4 and HP EliteBook 1040 G3 have been validated with SED when running in UEFI Boot mode. To ensure full functionality, set the following BIOS settings:
  - In BIOS, navigate to the Advanced tab, select *Secure Boot Configuration*, then select the check boxes labeled *Import Custom Secure Boot keys* and *Enable MS UEFI CA key*.
  - From the drop down menu, select *Legacy Support Disable* and *Secure Boot Enable.*
  - In BIOS, navigate to Advanced tab > Option ROM Launch Policy and select *All UEFI* from the drop down menu.

Resolved Technical Advisories v10.1

Encryption

- EMS Explorer is now working as expected when connecting an encrypted USB with EMS on a computer without Dell Encryption. [DDPC-5585, DDPSUS-2401]
- Resolved an issue that resulted in the loss of user activation on reboot. [DDPC-6572, DDPSUS-1844]

- Local users can now activate with Dell Encryption installed with Opt-in mode on a computer running Windows April 2018 update and not joined to a domain. [DDPC-9377, DDPSUS-2365, DDPSUS-2387,]
- The PBA Recovery Question authentication works as expected. [DDPC-9671]
- When child installers fail to install successfully, Dell Encryption will also fail to install and will log these errors. [DDPC-10110, DDPSUS-2379]
- LastSyncTime in the report results for Device Detail is now working as expected. [DDPC-10184, DDPSUS-2388]
- SDE plugins, PBE plugins and Encryption plugins now display the correct versions on the Management Console. [DDPC-10531, DDPSUS-2416]

Preboot Authentication

- An issue resulting with a computer running Windows 7 becoming unresponsive during decryption with PBA activated and FDE enabled has been resolved. [DDPC-9237, DDPC-10121]

Technical Advisories v10.1

Encryption

- Usernames with symbols may result with a "System Lock Required" pop-up message after a successful Single Sign On. To work around this issue, unlock and log back into the computer.[DDPC-10485]
- In rare occurrences, users may be unable to enroll in recovery questions due to an unresponsive Dell Authentication Service. To work around this issue, reboot the computer. [DDPC-10503]
- After installing Dell Encryption, an error in DellAgent.log stating "Could not locate saasManager plugin" may be safely ignored. [DDPC-10509]
- When attempting to upgrade Windows to a newer feature update, the feature update processes as expected, but registration is lost after the update. To work around this issue, reboot the computer. [DDPC-10569]

Preboot Authentication v10.1

- While using a K13A Rugged dock (only compatible with Rugged computers), an open laptop lid may be required for the operating system to populate on some monitors. [DDPC-10093]
- With the latest version of Encryption client installed, an Optiplex 7040 may not properly return from a hibernation or sleep. [DDPC-10181]
- Sleep mode may fail on an OptiPlex 7050 while Full Disk Encryption is in the process of encrypting. [DDPC-10261]

SED Management v10.1

- No technical advisories exist.

New Features and Functionality v10.0.1

- Resolved customer issues.

Resolved Technical Advisories v10.0.1

Encryption

- Added 12/2018 - Resolved an issue with Dell Encryption and Digital Persona credential providers conflicting. [DDPC-10120]

- The installation of Dell Encryption on a domain controller no longer changes the local machine policies set in the "Default Domain Policy" Group Policy Object. Dell Authentication can handle logging in with no password set when a 0 password length policy is enabled.

  For more information, see https://www.dell.com/support/article/us/en/19/sln313561/dell-encryption-enterprise-and-dell-endpoint-security-suite-enterprise-security-bulletin-082018?lang=en . [DDPSUS-2364]

Technical Advisories v10.0.1

Encryption

- No technical advisories exist.

Preboot Authentication v10.0.1

- Added 11/2018 - A password is required for all users added in the Add User panel. Zero-length password users will be locked out of the computer following activation. [DDPC-10114]

SED Management v10.0.1

- No technical advisories exist.

New Features and Functionality v10.0

- Improvements to Windows Update handling in Self-Encrypting Drive is supported.
- The following non-Dell computers have been validated with Preboot Authentication when running in Legacy Boot mode:
  - HP EliteBook 1040 G3
  - Lenovo ThinkPad T560
- The following non-Dell computers have been validated with Preboot Authentication when running in UEFI Boot mode:
  - HP EliteBook 840 G3
  - Lenovo ThinkPadP50
- Personal Encryption is versioned to 10.x to realign client and Server versioning.

Resolved Technical Advisories v10.0

Encryption

- Added 09/2018- Files synced via OneDrive with "Files On-Demand" enabled, work folders, and other technologies leveraging new APIs for file handling from Microsoft, introduced in a cumulative update for Windows 10 1709 and later, on a system running Dell Encryption are no longer displayed as erroneous text. For more information on OneDrive Files On-Demand, see https://www.dell.com/support/article/us/en/19/sln309779/dell-encryption-support-for-onedrive-files-on-demand?lang=en. [DDPC-8568]
- The "enroll' button no longer disappears for recovery questions with encryption client installed on a Windows 10 32-bit machine. [DDPC-8938, DDPC-9199]
- Added 09/2018-Resolved an issue with Dell Encryption and Symantec Endpoint Protection resulting in an intermittent Operating System failure [DDPC-9510]

Preboot Authentication

- The mouse now works during the PBA login screen on a Precision M4800 and Latitude 5290 computer with Windows 10 installed in UEFI mode and PBA enabled. [DDPC-6978, DDPC-7032, DDPC-8841]
- The mobile keyboard and touchpad work as expected during the PBA login screen on a Latitude 5290 2-in-1 machine with Windows 10 installed in UEFI mode and PBA enabled. [DDPC-7032]
- An issue resulting with the user name being changed to ''SYSTEM" while the password is in the process of being changed using Alt + Ctrl + Delete and PBA is active on a Windows 7 computer has been resolved. [DDPC-8948]
- Multiple "Other User" tiles are no longer created on the Windows 7 login screen after successfully answering Recovery questions and with PBA active. [DDPC-9343]
- An issue resulting with the message of "Username or password is incorrect" on the Windows screen when entering updated credentials after authenticating in PBA with a newly changed password has now been resolved.[DDPC-9483]
-
- Smartcard is no longer the default login option when password authentication is set for PBA and SmartCardEnabled is set within Windows. The default is PBA authentication. [DDPC-9497, DDPSUS 2301]

SED Management

- Machines with Coffee Lake-H Xeon processors activate with currently shipping enterprise-class or OEM Samsung drives. [DDPC-9348]

Technical Advisories v10.0

Encryption

- In some cases, after changing passwords in Windows, the computer may experience slower logins during the first login or auto-reactivation may occur. To work around this issue, run WSDeactivate after changing the password. [DDPC-9459]
- In rare occurrences, when updating to v10.0, an error may present if the user interface is used for the update. This can be safely closed with no impact to the install. [DDPC-9555]
- Multiple users are given the option to change the password on the Windows login screen when a user has logged into the computer after successfully completing the PBA Recovery Questions. If an account other than the one that authenticated through the PBA with recovery questions is selected, an error message displays "The specified network password is not correct." [DDPC-9650]
- Single Sign On fails when a user authenticates PBA after entering a password into the console using copy+paste with more than the allowed 32 characters for Windows. [DDPC-9700]
- Added 11/2018 - Dell Encryption may introduce changes to how data is protected on your device. To ensure your endpoints are protected, running the "WSProbe" application that is included with Dell Encryption will perform a validation that all files on the computer are properly encrypted. This may result in a slight performance degradation, but it is generally unnoticed. [DDPC-10168]
- Added 11/2018 - Windows 10 Work Folders may fail to sync when attempting to sync encrypted files. To work around this issue, manually sync each file. [DDPC-10400, DDPSUS-2269, DDPSUS-2394, DDPSUS-2407]

Preboot Authentication v10.0

- In some cases, the touchpad becomes unresponsive during the PBA login screen on a Precision 7520 and Precision 7720 computer with Windows 10 or Windows 7 installed in legacy mode and PBA enabled. To work around this issue, attach an external mouse or use the tab key to switch through fields. [DDPC-8646]
- Added 11/2018 - Password resets after a local PBA user answers recovery questions is disabled after a minute, 30 seconds. [DDPC-9707]
- In some cases, non-Dell devices have to manually import the Microsoft SecureBoot certificates when these devices are configured for UEFI boot mode with SecureBoot enabled. This process may vary based on the manufacturer and is recommended to refer to the device's documentation for instructions on performing this process. [DDPC-9828]

SED Management v10.0

- No technical advisories exist.

New Features and Functionality v8.18

- Encryption Client and SED Management is now supported with Windows 10 April 2018 Update (Redstone 4 release).
- The Windows 10 update process and compatibility with Windows Defender are improved when System Data Encryption is enabled . The encryption client can now identify and encrypt user files without the need to hardcode exclusion of system-generated files when System Data Encryption is enabled. This behavior is configurable and can be overridden by the administrator, if necessary. For more information on the Windows 10 Feature Update process, refer to http://www.dell.com/support/article/us/en/04/sln298382.
- The Encryption client can now identify and encrypt user files without the need to hardcode exclusion of system files.
- SED Manager is now compatible with HVCI.
- SED Manager has been qualified on the following non-Dell computers:
  - HP ProBook 450 G2 (Legacy)
  - HP ProBook 450 G5 (Legacy)
  - HP ProBook 840 G4 (Legacy)
  - HP Elitebook 840 G3 (Legacy)
  - HP Elitebook 840 G4 (UEFI)
  - Lenovo ThinkPad (Legacy)
  - Lenovo T560 (UEFI)
- Starting with the Encryption Client v8.18, the authentication provider component has been fully replaced. This installer will leverage a new Dell built-in credentials provider that is part of the Client Security Framework installer. The old Digital Persona credentials provider is set to a disabled state. If leveraging the fingerprint or smart card contact-less authentication, these will no longer work after an upgrade of Encryption Client v8.18.

Resolved Technical Advisories v8.18

Encryption

- Resolved an issue with longer than usual boot times when leveraging the Policy-Based Encryption client. [DDPSUS-1950, DDPSUS-2081]
- With Fast User Switching enabled and being leveraged no longer causes Dell Encryption to fail to communicate to the Dell Security Management Server. [DDPSUS-2163]
- Re-mapped libraries no longer cause an immediate failure during install. [DDPSUS-2166]
- USB external media provisioned with Dell Encryption can now be accessed on Windows or Mac computers interchangeably without loss of key material. [DDPC-6592]
- The Dell Data Security Console shows Protection and encryption status for Policy-Based encryption. [DDPC-7046]
- Resolved an issue with the inability to white-list a device with Dell Encryption. [DDPC-7717]
- Volumes now display during recovery. [DDPC-7794]
- A memory leak no longer occurs when inserting external devices to the computer. [DDPC-8297]

Preboot Authentication

- Resolved an issue with Thunderbolt based docking stations with the Dell Encryption Pre-Boot Authentication environment. [DDPSUS-1923]
- Resolved and issue with Pre-Boot Authentication displaying an initial access code, even though connectivity to the Dell Security Management Server is present. [DDPSUS-2198. DDPSUS-2200]
- An issue resulting with the backslash/pipe (\ |) key on an Arabic behaving differently than expected has been resolved. [DDPC-6529]
- The Windows 10 upgrade process with PBA activated is improved. [DDPC-8031]

SED Management

- An error message no longer displays during an upgrade of Digital Persona's Auth when the Dell Data Security Console is also open during the upgrade. [DDPC-7836]
- Oberthur chip only smart card ID-One COSMO V7.0 works as expected on a UEFI copmuter. [DDPC-7985]
- Smart card readers are now detected on legacy machines. [DDPC-8030]

Technical Advisories v8.18

Encryption

- Dell Encryption logs do not specify if insufficient disk storage caused installation failure. [DDPC-2994]
- In some cases, recovery questions are not available to the user after upgrade. To work around this issue, disable then re-enable recovery questions. If recovery questions were previously disabled after user enrollment, ensure that the option is disabled after upgrade. [DDPC-8880]
- Single Sign On is active for a 90 second period after PBA authentication on a computer in hibernation mode with the Encryption client installed. After 90 seconds, the OS user credentials must be used for authentication. [DDPC-9179]
- Upgrades to v8.18 may fail if Dell Encryption Personal has not been fully activated. To work around this issue, activate both Dell Encryption Personal through the Dell Data Security Console as well as the Dell Encryption Local Management Console. Once both products are activated, the upgrade will proceed normally. [DDPC-9346]
- Added 09/2018- An issue with Dell Encryption and Symantec Endpoint Protection may result in an intermittent operating system failure [DDPC-9510]
- Added 11/2018 - Occasionally, Dell Encryption is unable to connect to the local management console. This condition results in Dell Encryption not providing the dialog to enter the password for encrypted external media, it does not prompt to encrypt unprotected media, and the About box does not contain the correct information. A computer restart resolves the issue. [DDPC-10409]

Preboot Authentication v8.18

- Added 08/2018- After activating PBA with the Encryption Client installed on a Latitude 7404, Latitude 7204, or a Latitude 5404 Rugged computer in Legacy boot mode, an error message of "Parity Error" displays. To work around this issue, disable one of the two serial ports in BIOS.[DDPSUS-2225, DDPC-9493]
- A local user must log in through Windows at least once on the computer before the Preboot Authentication prompts for credentials at startup for that user. If users are manually added to the computer, they must be added through User Accounts, accessed through the Control Panel. [DDPC-8569]
- In some cases, the touchpad and mouse become unresponsive during the PBA login screen on a Precision 7520 machine with Windows 10 installed in legacy mode and PBA enabled. [DDPC-8646]
- In some cases, when user tries to login using PBA after changing hibernations settings, the Single Sign On feature fails. [DDPC-8683]
- Currently, when upgrading from Fall Creators update of Windows to the April 2018 update, the initial sync to PBA appears under the task bar. [DDPC-8798]
- In rare occurrences, when upgrading from Fall Creators Update of Windows to April 2018 Update, PBA is unable to resolve DNS/DHCP successfully. To work around this issue, the user must deactivate and activate PBA again. [DDPC-8814]
- In some cases, the mouse and keyboard become unresponsive during the PBA login screen on a M4800 with Windows 10 installed in UEFI mode and PBA enabled. [DDPC-8841]
- Added 08/2018- With the computer lid closed, a black screen displays after the PBA login screen when a TB16 docking station is attached to a Precision 5530 or Precision 7730/7530 Mobile Workstation with 1.0.0 BIOS and Windows April 2018 update. To work around this issue, the computer must be reverted back to Windows 10 Fall Creators Update until an update to the BIOS has been promoted. The Precision 7730/7530 can also be attached to a TB18 docking station to resolve this issue regardless of the Windows update version. [DDPC-8945]
- Added 11/2018 - When a user logs into Windows using a password or a smart card after upgrading to v8.18, the user may be prompted to re-enroll the smart card credentials through the PBA. If the policies have changed and smart card authentication is no longer allowed, smart card re-enrollment will not be possible. If the prompt to enroll credentials continues, deactivate the PBA and then reactivate again. [DDPC-9313]

SED Management v8.18

- When a NVME is used as a data drive with a standard 2.5" Self Encrypting Drive, a "Device Locked" message will display on the PBA screen. [DDPC-9256]

New Features and Functionality v8.17.2

- SED Manager includes a security update addressing the Spectre and Meltdown vulnerabilities CVE-2017-5754. Customers and field teams should take v8.17.2 and all sustaining releases as a best practice.

Resolved Technical Advisories v8.17.2

Encryption

- The following hard-coded exclusions have been added for improved interoperability with Windows Defender and Microsoft Credential Vault:
  - C:\ProgramData\
  - C:\Program Files\
  - C:\Program Files (x86)\
  - C:\Users\<user>\AppData\Local\Microsoft\Vault\

  Due to these changes, a re-sweep will be performed to ensure that these folders are properly protected by Dell Encryption.

  This sweep decrypts files that are system-generated files, but will ensure that user-generated data within these folders will stay protected as either Common encrypted or SDUser encrypted data based on currently set policies. These changes can be overridden by adding a Category 3 inclusion to SDE Encryption Rules. [DDPC-8037, DDPC-8147]
- Resolved an issue that resulted in an Operating System failure when Dell Encryption is installed and a Thunderbolt docking station is used.

  NOTE: This is a temporary fix, and will be corrected in the next release of Dell Encryption. New drivers for thunderbolt based docking stations may be required for a final resolution.

Preboot Authentication

- The username text is now displayed in French on the PBA screen after FDE has been installed on a UEFI machine. [DDPC-8012]
- An issue where the Lock/Unlock commands were not immediately enforced even though the "check for PBA commands" policy was enabled has been resolved. [DDPC-8021]

Technical Advisories v8.17.2

Encryption

- After installing the encryption client and opening a report of the file with WSScan, unencrypted files have " \\?\" characters at the beginning of their directories. Only a cosmetic issue and has no effect on the system or files." [DDPC-8190]
- In some cases, after installing or upgrading encryption client, a message results of "Backup keys operation still not performed successfully..." once policies have been set. The current workaround is to reboot the machine. [DDPC-8316]

Preboot Authentication

- No technical advisories.

SED Management v8.17.2

- No technical advisories.

New Features and Functionality v8.17.1

- There are no new features for Personal Edition v8.17.1.

Resolved Technical Advisories v8.17.1

Encryption

- 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]

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]

Technical Advisories v8.17.1

Encryption

- In some cases, a device may not show in compliance after sweep completes. The current workaround is to reboot the device. [DDPC-7977]

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 a network cable is unplugged after loading the PBA, there is no IP address captured which causes the server sync to fail. [DDPC-7936]
- Added 05/2018- In some cases, the touchpad becomes unresponsive during the PBA login screen on a M300 machine with Windows 10 installed in UEFI mode and PBA enabled. [DDPC-8206]

SED Management v8.17.1

- 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]

New Features and Functionality v8.17

- 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.

Resolved Technical Advisories v8.17

Encryption

- 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]
- Added 03/2018- The following hard-coded exclusions have been added for improved interoperability with Windows updates. This sweep decrypts files that are system-generated files, but will ensure that user-generated data within these folders will stay protected as either Common encrypted or SDUser encrypted data based on currently set policies. These changes can be overridden by adding a Category 3 inclusion to SDE Encryption Rules.

  - %SystemRoot%

  - %SystemRoot%\\CbsTemp

  [DDPC-7881]

Preboot Authentication

- Added 05/2018 - The touchpad is now functional at the PBA login screen on non-UEFI computers. [DDPC-5362]
- Added 05/2018 - The touchpad is now functional after the computer resumes from sleep on non-UEFI Dell Latitude computers. [DDPC-5363]
- 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]
- Added 05/2018 - With Preboot Authentication enabled for Full Disk Encryption or Self Encrypting Drive technologies, booting into the preboot environment or manually syncing server communication no longer fail if the Dell Security Management Server is unavailable. [DDPC-7181]
- 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

Dell Encryption v8.17

- No Technical Advisories exist.

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

New Features and Functionality v8.16

- 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

Encryption

- 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]
- Added 05/2018 - An issue causing the local management console to become unresponsive or file explorer filename sorting to not function after an encryption sweep the Secure Post-Encryption Cleanup policy set to an overwrite value has now been resolved. [DDPC-5764]

Resolved Customer Issues

- Windows now properly resumes from hibernation when the Secure Windows Hibernation File policy is enforced. [DDPSUS-1346]
- Registry keys are now properly removed at uninstall. [DDPC-5410]
- 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]
- Added 03/2018- The following hard-coded SDE exclusions have been added for improved interoperability with Windows upgrades. This sweep decrypts files that are system-generated files, but will ensure that user-generated data within these folders will stay protected as either Common encrypted or SDUser encrypted data based on currently set policies. These changes can be overridden by adding a Category 3 inclusion to SDE Encryption Rules.

  - %SystemDrive%_SMSTaskSequence

  [DDPC-6932}
- 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]

Technical Advisories

Dell Encryption v8.16

- Added 11/2018 - When attempting to uninstall Dell Encryption Personal with the Dell Data Security Uninstaller, ensure that the LSARecovery executable being used for the uninstall is stored locally. If the LSARecovery being used for the uninstall is stored on a network share, an error may be seen, which causes the uninstall to fail. [DDPC-7535]

PBA Advanced Authentication v8.16

- 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]

SED Management v8.16

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

New Features and Functionality v8.15

- Added 03/2018-Dell has introduced a change to how built-in encryption exclusions are being handled. Previously, built-in exclusions would prevent the encryption of any file that was created, or copied into a folder that was defined within these exclusion lists. Future hard-coded exclusions introduced in 8.15 and later will be protected in a way that only system generated files will no longer be encrypted, all user generated data will still be encrypted that enters these folders through a file create or a file copy action. As always, file move operations will retain the encryption status of the source folder until an encryption sweep or a change to the file is enacted.
- The Encryption client drivers pass the Hypervisor Code Integrity (HVCI) checks.
- Activation performance is improved, and capability is now available to enter the entitlement key within the installation command.
- Operating system downgrade is now supported with the Encryption client.
- Personal Edition is rebranded to Encryption Personal.
- 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

Encryption

- The "Invalid Password" message now displays when the user enters the wrong password into the Encryption Removal Agent. [DDPC-1313]
- Performance of Encryption client upgrade that begins during an encryption sweep is improved. [DDPC-4261]
- 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]

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]
- Added 05/2018 - When the Encryption client is installed on Windows Server 2016 Standard Edition, the OS/Version field for the Endpoint now reads "Microsoft Windows Server 2016 Datacenter/10.0.14393" in the Dell Server. [DDPC-4836]
- Diagnostic Info performance and error messaging are improved. [DDPC-5559]
- File names on the Start menu are now correctly translated into French. [DDPC-5895]

Advanced Authentication

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

SED Client v8.15

- 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]

Technical Advisories v8.15

Encryption

- 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]
- Policy updates are not received following a user security identifier (SID) change. [DDPC-6374]
- 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]
- On rare occasion, the Local Management Console becomes unresponsive. To work around this issue if it occurs, add the following exclusion to the SDE Encryption Rules policy: -^3C:\Windows\Globalization [DDPC-6547]
- Command-line uninstallation with the Encryption Removal Agent parameter fails. To work around this issue, uninstall with the master installer or by double-clicking the child installer executable file. Dell recommends storing a copy of the LSARecovery file locally before running a scripted uninstallation with decryption. [DDPC-6568]

Advanced Authentication

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

SED Client v8.15

- 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).

- Users can now access ProSupport contact information from the About screen in DDP Console and through the About option from the system tray icon.

Resolved Technical Advisories v8.13

Encryption

- 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]
- All text now displays as expected in Japanese Encryption Removal Agent dialogs. Previously, some text did not display in one dialog. [DDPC-4159]

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]
- 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]

Technical Advisories v8.13

Encryption

- 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]
- 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]

- 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 v8.13

- 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]

SED Client v8.13

- 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 .

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

  [DDPC-5941, DDPC-6219]

New Features and Functionality v8.12

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

Resolved Technical Advisories v8.12

All Products

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

Encryption

- On Windows 10, the Encryption icon now displays as expected on encrypted files in File Explorer. [DDPC-1186, DDPC-2817, DDPMTR-1864]
- Debug-level logging is improved. [DDPC-2307]
- Upgrade to Windows 10 now proceeds as expected when the installation media is stored in a folder that is encrypted with the User or Common key. [DDPC-4146]

- The Secure Windows Hibernation File and Prevent Unsecured Hibernation policies are now enforced after upgrade. [DDPC-4786]
- The WSScan **Unencrypted file in Violation** option now initiates a sweep of unencrypted files as expected, without the files having to be selected or accessed. [DDPC-4790]
- An issue is resolved that resulted in Windows Update failures with Office and Windows 10 feature updates. [DDPSUS-1323]

Resolved Customer Issues

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

Advanced Authentication

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

Technical Advisories v8.12

Encryption

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

  [HKEY_LOCAL_MACHINE\SYSTEMCurrentControlSet\ServicesCmgShieldFFE]

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

  [DDPC-4185]
- If Personal Edition is uninstalled before activation, an error message displays: "EmbeddedServer service is in a pending delete state. error 0z430." To work around this issue, before uninstalling, allow the client to activate and then restart the computer before beginning uninstallation. [DDPC-4886]
- When encryption or decryption is paused, the Compliance/Provisioning status may not be accurately indicated in the Local Management Console. [DDPC-5063]
- Added 04/2018- Currently, users have to manually delete old files individually on Encrypt4Share. The current workaround is to press **Ctrl+Shift+Click all the files** and then select remove. [DDPC-8943]

Resolved Technical Advisories v8.11

Encryption

- An issue is resolved that resulted in the Local Management Console appearing unresponsive while the Encryption client performed tasks in the background. [DDPC-2769]
- The WSScan user interface now opens to the option of Unencrypted Files, as expected, when commands `-ua-`, `-ua`, and `-uav` are used to launch the user interface. [DDPC-3473]
- An issue is resolved that caused the Shield service to occasionally crash when the user logged out. [DDPC-3939]
- Added 05/2018 - Aventail Access Manager is now supported with Encryption client on Windows 10 computers. [DDPC-4335]

Resolved Customer Issues

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

Technical Advisories v8.11

Encryption

- Cumulative encryption exclusions are now automatically applied when the Encryption client is upgraded. This will require an encryption sweep for each user upgraded to v8.11 or later. However, subsequent updates will require a sweep only if the update includes new exclusions. [DDPC-1334, DDPC-5138]
- Activation fails after attempting to roll back an External Media Edition upgrade. [DDPC-4449]
- The user receives an access denied error when attempting to access removable media, although policy is set to allow full access to unShielded media. [DDPC-4523]
- After upgrade to Windows 10 Fall Update using WSProbe -E on a computer with Hardware Crypto Accelerator, during re-encryption with WSProbe -R, the Local Management Console freezes and a message displays regarding HCA key backup and provisioning. [DDPC-4645]

Advanced Authentication

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

New Features and Functionality v8.10.1

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

Resolved Technical Advisories v8.10.1

Encryption

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

Technical Advisories v8.10.1

Encryption

- 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]
- 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]

New Features and Functionality v8.10

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

Resolved Technical Advisories v8.10

Encryption

- Installer logging of launch conditions is improved. [DDPC-918]
- An issue that resulted in a computer occasionally becoming unresponsive after reboot is now resolved. [DDPC-1255]
- The Encryption Removal Agent no longer crashes during decryption of HCA- or SDE-encrypted files if the key bundle is missing or inaccessible to the Agent. Instead, a message displays that files could not be decrypted. [DDPC-1359]
- An issue that caused the Shield Service to crash is now resolved. [DDPC-2189]
- An issue that led to unresponsiveness after restarting a Windows 10 computer running Advanced Threat Protection is now resolved. [DDPC-2336]
- An issue that caused a restart and lock at the Windows startup screen on Windows 7 computers running Bitdefender Antivirus is resolved. [DDPC-2561, DDPSUS-842]
- Default SDE Encryption Rules have been refreshed. [DDPC-2689]
- SDE encryption now proceeds on computers with HCA or a SED, and a log entry stating SDE policies are blocked due to FVE or a SED disk no longer displays. SDE Encryption is now enabled by default in new installations and upgrades, based on the registry entry HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMgShield\AlwaysApplySDE set to "1." [DDPC-3273]
- Encryption handling of files that are always in use is improved. [DDPC-3331, DDPC-3333, DDPC-3334]
- Additional data is now provided to Dell Data Protection Server for endpoint status reporting. [DDPC-3332, DDPC-3335]
- Users with common access card authentication can now successfully activate Personal Edition. [DDPSUS-807]
- Windows logon with a smart card now proceeds as expected. [DDPSUS-855]
- Encryption sweep performance is improved on Windows 10 computers running Sophos. [DDPSUS-866]
- An issue that led to an error when EnCase attempted to access encrypted files is resolved. [DDPSUS-923]
- An issue that resulted in occasional computer unresponsiveness after installation but before activation is resolved. [DDPSUS-1037]
- An issue that led to multiple restarts is now resolved. [DDPSUS-1087]

Advanced Authentication

- On Dell Latitude 3450 and 3550 computers running Windows 10, fingerprint authentication now proceeds as expected. [DDPC-1598/CSF-772]
- After restoring credentials in Password Manager, a second authentication prompt no longer displays. [DDPC-1617]
- Password Manager logon now functions as expected with Dell Remote Management Console logon. [DDPC-2356]

- Occasionally after the computer hibernates or restarts, enrolled fingerprints must be re-enrolled. [DDPC-2812]

Technical Advisories v8.10

Encryption

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

Preboot Authentication

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

Resolved Technical Advisories v8.9.1

Encryption

- A Dell Data Protection-encrypted Windows 10 computer can now be upgraded to the Windows 10 Fall Update, after a few prerequisites are met. The prerequisites must be met, due to a change Microsoft has made to the Windows update process beginning with Windows 10. For more information, see Upgrade to the Windows 10 Anniversary Update. [DDPC-928, DDPC-1146, DDPC-1443]
- Corrected a misspelling of szRegValueLoginTimeout in the registry override variable and log message. [DDPC-966]
- The computer now boots as expected after Intel Rapid Storage Technology drivers are installed. [DDPC-1246]
- The HideOverlayIcons registry setting that is used to hide the encryption icons for all managed users on a computer after the original installation now works as expected. The HideOverlayIconsOverlay registry setting now effectively hides Dell Data Protection Encryption overlay icons when File Explorer is refreshed or reopened. [DDPC-1267, DDPC-1327]
- External Media Shield Explorer now launches properly after more than one incorrect password entry when accessing media that has been provisioned on a Mac. [DDPC-1273]
- A few WSProbe options have been deprecated to improve security. The WSProbe utility no longer supports the following options: -u (enable or disable Application Data Encryption), -x (exclude application from Application Data Encryption), and -i (revert an excluded application back to included in Application Data Encryption). [DDPC-1279]
- All characters of the 32-character Endpoint Code now fully display in the External Media Shield manual authentication dialog. [DDPC-1295]
- Excess logging of file-create operations no longer occurs. [DDPC-1339]
- An issue that caused excessive memory consumption has been resolved.[DDPC-1468]
- On a Windows computer, External Media Shield now successfully opens files and folders named with accented characters that are stored on external media and provisioned using a Mac computer. [DDPC-1517]
- When encryption models are changed (SDE to HCA) after an encryption sweep has completed, the computer no longer experiences a temporary blue screen. Previously, this occurred while key types were swapped, and allowing the computer to reboot typically restored functionality. [DDPC-1536]
- External Media Shield no longer displays Access Denied errors when the Windows Media Encryption and Windows Port Control policies are set to Off and Disabled. [DDPC-1572]

- After upgrade from Security Tools v1.3.1, the computer shuts down normally. [DDPC-1606]
- Processes related with pop-up notifications during the encryption sweep have been streamlined, reducing CPU usage. [DDPC-2115]
- Decryption with the Encryption Removal Agent at uninstallation now succeeds. Previously, in a few cases, decryption began but did not finish sweeping the entire volume. [DDPSUS-751]
- An issue that caused multiple reboots during installation or upgrade on some computers is resolved. [DDPSUS-766]

Advanced Authentication

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

Preboot Authentication

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

Resolved Technical Advisories v8.9

Encryption

- The Encryption client uninstaller now defaults to the uninstall/decrypt option instead of uninstalling but leaving files encrypted. When the option to uninstall without decrypting is selected, the Encryption Removal Agent is no longer installed. [DDPC-857, DDPC-1455]
- Silent uninstallation now supports decryption with pre-download key material on locally and remotely managed clients. [DDPC-930]
- The Shield Service no longer crashes during an HCA encryption sweep when the Volumes Targeted for Encryption policy is set to All Fixed Volumes. [DDPC-955]
- Files larger than 64Kb that are encrypted with the User or Common key on computers with HCA cards are no longer corrupted after decryption during uninstallation. [DDPC-1000]
- Upgrades now succeed, and an error no longer occurs with the message, "Error 1303: The installer has insufficient privileges to access this directory." [DDPC-1178]
- An issue that resulted in rare crashes of the local console when the console was open during an encryption sweep is resolved. [DDPC-1199]
- A default SDE Encryption Rules policy which caused problems with Windows updates has been resolved. The issue resulted from encryption of \System32 executable files. [DDPC-1207]
- Restarting or shutting down a computer during an encryption sweep no longer causes a Shield Service crash. [DDPC-1233]
- External Media Shield is now updated on a non-Shielded computer when that computer is used to access an encrypted removable media that has been updated. [DDPC-1259]
- The issue that prevented the Managed Migration Utility from converting Personal Edition to Enterprise Edition when attempting to obtain the User Principal Name (UPN) from the operating system is resolved. [DDPC-1260]
- An issue that allowed re-encryption of encrypted files when an encryption sweep started and ended during a single user login session is resolved. [DDPC-1262]
- An issue that occasionally caused a computer to become unresponsive during an encryption sweep is resolved. [DDPC-1275]
- Files stored in redirected folders on computers running HCA encryption are no longer corrupted. Previously, the last 4Kb of such files could be corrupted. [DDPC-1282]
- The Encrypt for Sharing context menu option is now present when the user right clicks a file or folder in Windows Explorer. [DDPC-1291]
- An issue that led to the computer becoming unresponsive during the reboot following installation is resolved. [DDPS-1328]
- The issue that flagged services as suspicious or offline injection attacks and blocked them from starting is resolved. Previously, this issue led to restart failures. [DDPC-1346, DDPC-1463]

Preboot Authentication

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

Technical Advisories v8.9

All Products

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

Encryption

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

Advanced Authentication

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

Preboot Authentication

- After recovering PBA access through recovery questions, the password change page displays a message that, if no action is taken, the user will be automatically logged in to the Windows session, although no automatic login occurs. [CSF-1083]
- Added 04/2018- When a user tries to sync to the server while using a Latitude 7204 Rugged Machine on an XFR dock with Windows 10 x32 and the Encryption client installed, the options

  Sync and Network are not available at the PBA Log in screen. [DDPC-1638]
- 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

Encryption

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

Advanced Authentication

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

Preboot Authentication

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

New Features and Functionality v8.7

- The Windows USB selective suspend feature is now supported.

Resolved Technical Advisories v8.7

Encryption

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

Advanced Authentication

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

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

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

Technical Advisories v8.7

Encryption

- If the HCA algorithm is changed during encryption, SDE encryption rather than HCA re-encryption begins. To work around this issue, restart the computer. After log in, HCA encryption begins normally. [DDPMTR-406]
- Reinstallation may fail with an error such as a file or folder access error or an EMSService crash, if the \temp folder was previously encrypted with the Common Encryption Key and files were not fully decrypted before uninstallation. To work around this issue, before reinstalling, remove files from the \temp folder. [DDPMTR-1647, DDPMTR-1782]
- When the Encryption Removal Agent is used to decrypt and uninstall, if an invalid Encryption Administrator Password is entered, an incorrect error message displays: "Failed to deserialize the specific file" [DDPMTR-1649]
- Running Diagnostic Info results in a file archiving error if run when files that must be accessed are locked or in use. [DDPMTR-1830]
- When running the Setup Wizard after WSDeactivate, access to Common and User encrypted data is lost. To work around this issue, after running WSDeactivate, do not run the Setup Wizard. Instead, perform File/Folder Encryption recovery as explained in the *Recovery Guide*. Select the option, My system does not allow me to access encrypted data.... Reboot the computer then run the Setup Wizard to re-activate the user. [DDPMTR-1831]

- When the EMS Access Code Failure Action policy is set to Apply Cooldown, the cooldown is not applied. To work around this issue, after the allowed number of password attempts, the user must manually authenticate to the device. For more information, see "EMS Authentication Failure" in *AdminHelp*, accessible from the Remote Management Console. [DDPMTR-1859]
- 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]

Advanced Authentication

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

Preboot Authentication

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

New Features and Functionality v8.6.1

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

Resolved Technical Advisories v8.6.1

Encryption

- During an upgrade, the following error no longer displays: "error Opendatabase,Databasepath,Openmode/error 80004005, (MSI API error)." This error occurred intermittently and the upgrade successfully completed after the user acknowledged the error. [DDPC-882]
- An issue that previously occurred on some Dell Latitude E5540 computers with USB external drives connected that resulted in a blue screen has been resolved. [DDPMTR-955, DDPSUS-259]
- An issue that resulted in occasional SDE key load and unlock failures is now resolved. [DDPMTR-1278]
- During upgrade, when Encryption Removal Agent is installed in order to proceed with uninstall, after the user selects the backup key location and enters the password, the following error no longer displays: "Error trying to verify the key bundle is for this machine. Continue without verifying the key bundle?" The installation now proceeds as expected. [DDPMTR-1366]
- Upgrades from pre-v8.5 no longer fail due to encryption notifications being sent during the upgrade. [DDPMTR-1404]
- On computers with more than one version of Apache log4net installed and registered with the Global Assembly Cache, uninstallation now proceeds as expected. [DDPMTR-1519, DDPMTR-1536]
- The issue with continued rebooting on a computer with the number of users nearing 300 has been resolved. [DDPSUS-37]
- The issue that caused upgrade to fail with the logged error, "CInstallInf::ProcessInf - Error calling SetupInstallServicesFromInfSection," is now resolved. [DDPSUS-283]
- Encryption of the \Regback folder after a scheduled backup no longer requires a reboot for encryption to begin. [DDPSUS-302, DDPSUS-342]

Advanced Authentication

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

Preboot Authentication

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

New Features and Functionality v8.6

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

Resolved Technical Advisories v8.6

Encryption

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

Advanced Authentication

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

Preboot Authentication

- The System Shutdown Required message that displays before PBA activation begins can now be properly minimized and maximized by clicking the system tray icon. [CSF-195]
- On a German operating system, the PBA logon button text is now sized correctly and fully visible. [DDPLP-276]
- On a UEFI computer with PBA activated and with default Title, Legal Notice, and Support Information for the PBA logon screen, selecting **Options > System Information** no longer returns the message “Support Information is not enabled.” [DDPUP-510]
- On a UEFI computer running a Japanese or Korean operating system with PBA activated, the PBA logon screen now loads and functions as expected. [DDPUP-547]
- On the Dell Precision T1700 and OptiPlex XE2, enabling Secure Boot and activating the PBA no longer results in the error, "No bootable devices found." [DDPUP-614, DDPUP-615]

Technical Advisories v8.6

Encryption

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

Advanced Authentication

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

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

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

[CSF-349]

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

Preboot Authentication

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

Resolved Technical Advisories v8.5.1

All Products

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

Encryption

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

Advanced Authentication

- When using Security Tools, the enrollment credentials wizard summary page now shows the chosen login option in the summary. [CSF-93]
- When using Security Tools' One-time Password feature, for devices that are already enrolled, enrollments are now properly deleted when the policy “Mobile Device Require Password” is changed from Off to On. [CSF-94]
- When using Security Tools' One-time Password feature, null reference pointers have been resolved. [CSF-98]
- The issue of using Security Tools, Windows 8.1, and the GPO "Do Not Display Last Username", causing single sign-on to fail has been resolved. [CSF-100]
- Improvements have been made to make user login and start-up more reliable. [CSF-114, CSF-116]
- Issues related to the "DellMgmtAgent" service failing to start or starting slowly have been resolved. These issues presented in the Windows System Event Viewer under the Service Control Manager with a message similar to the following: "The

DellMgmtAgent service failed to start due to the following error: The service did not respond to the start or control request in a timely fashion." [CSF-116]

- Encryption statistics now properly display in the Security Tools Console. [CSF-121]
- The issue of “Security Tools - Setup” being incorrectly translated in Chinese to “Security Tools - Installation” has been resolved. [CSF-128]
- When running Security Tools, “DDP Console – Admin Settings” is now properly displayed in the All Programs menu instead of NewShortCut3. [CSF-129]
- The size of the Security Tools Console now stays constant, unless it is manually enlarged or reduced. [DCF-2]
- The issue of some special unicode characters, particularly German language umlaut characters, failing to be recognized during entry of password recovery questions, is resolved. [DDPLP-202]

Resolved Technical Advisories v8.5

Encryption

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

Advanced Authentication

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

Technical Advisories v8.5

Encryption

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

New Features and Functionality v8.4.1

- Multi-certificate Common Access Cards are now supported.

Resolved Technical Advisories v8.4.1

Encryption

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

Advanced Authentication

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

Preboot Authentication

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

Technical Advisories v8.4.1

Encryption

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

Advanced Authentication

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

Preboot Authentication

- Single Sign-on intermittently fails on computers with self-encrypting drives on which Preboot Authentication is activated. [DDPLP-144]
- When replacing a provisioned self-encrypting drive (with the Preboot Authentication environment active) with a *new* self-encrypting drive and provisioning the Preboot Authentication environment, after the new SED is provisioned, the old SED can no longer be recovered. [DDPLP-150, MMW-581]
- On the Dell Latitude Rugged Extreme, the user is able to detach the tablet from the dock. However, the dock is needed to log in through the PBA. Detach the tablet only after the PBA authentication step is complete. [DDPLP-162, DDPLP-163]

- After successfully authenticating to the Preboot Authentication environment, the computer will not complete Single Sign-on. Instead, the computer halts at the Windows Logon screen for another user. Microsoft Windows 8.1 defaults to the Logon screen for the previously authenticated user. To complete logon, return to the User Tiles screen by selecting the back arrow in the top right of the screen and then selecting the correct user tile for the user authenticated in the PBA. SSO data captured by the PBA may still be present and once the user tile is selected, Windows authentication may be completed automatically. [MMW-564]

Resolved Technical Advisories v8.4

Advanced Authentication

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

Technical Advisories v8.4

Encryption

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

New Features and Functionality v8.3.2

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

Resolved Technical Advisories v8.3.2

All Products

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

Encryption

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

Advanced Authentication

- Fingerprint credentials are now retained when upgrading from v8.2.1 or earlier. [28457, 28766]

- Upgrade failures related to a USH fingerprint sensor configuration file error have been resolved. [28845]
- Attended enrollment is no longer needed when the Authentication Policy is set to Fingerprints + Contactless Smart Cards. [28873]

Technical Advisories v8.3.2

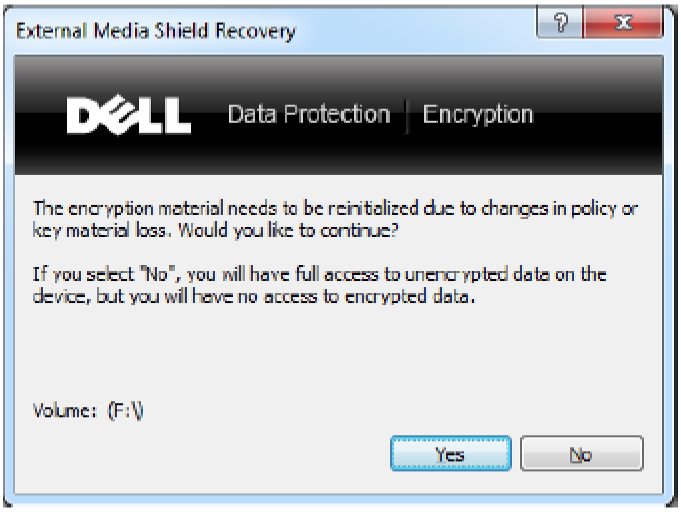
Encryption

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

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

  Instructions

  1. Insert the external media into a computer without Dell Data Protection | Encryption installed (a clean computer, WinPE image, Windows boot disc, etc.).
  2. Manually delete the hidden *_Encryption_Data_Do_Not_Delete_* folder. If running this from a command prompt you may need to remove the hidden attributes first (i.e. attrib -r -h -s _Encryption_Data_Do_Not_Delete_).
  3. Manually delete the *Access Encrypted Files (Mac).dmg, AccessEncrytpedFiles.exe*, and *autorun.inf* files from the root of the device.
  4. Login to a computer running Dell Data Protection | Encryption with the same user account that originally encrypted the external media. Older versions of Dell Data Protection | Encryption will also require both the same user **and** same computer that originally encrypted the external media.
  5. Insert the EMS-encrypted external media.
  6. You are prompted to perform a recovery. Click **Yes**.



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

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

Volume: (F:\)

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

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

New Features and Functionality v8.3.1

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

Resolved Technical Advisories v8.3.1

Encryption

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

New Features and Functionality v8.3

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

Resolved Technical Advisories v8.3

Encryption

Revised 04-2014

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

- Previously, after full HCA encryption and then hibernating, the computer would fail to retain the system state after returning from hibernation. This issue has been resolved. [28738]

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

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

Advanced Authentication

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

Cloud Edition

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

Technical Advisories v8.3

Encryption

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

  Dell Data Protection | Security Tools and Dell Data Protection | Encryption do not support Hybrid Sleep states and SSO when Preboot Authentication (PBA) is Active. Disable Hybrid Sleep when using Preboot Authentication if your organization intends to use SSO. [25785]

- During a command line uninstall, the installer will not download the encryption keys for the computer unless Silent mode is specified using the parameter CMGSILENTMODE=1. To work around this issue, specify CMGSILENTMODE=1 in the command. [27979]
- All registry keys and installation files are not removed after uninstallation. [28219]
- After uninstallation, logon with cached credentials occasionally fails when the computer is not connected to the network. During uninstallation, the cached credentials are decrypted. If this decryption fails for any reason, the user will not be able to login while disconnected from the network. To work around this issue, reconnect to the network and log on to cache the credentials. [28277]
- The encryption icon that indicates that a drive is encrypted does not display when a drive has been encrypted using HCA. [28400]
- During an attended (non-silent) upgrade from v8.1, the installer does not prompt the user to confirm that the upgrade is desired before continuing the installation. [28574]
- Preboot Authentication uses a "Basic" disk partition and cannot be converted to "Dynamic" partition (for RAID arrays). Attempts to convert the partition will result in the PBA not being created or the PBA not starting. [28587]
- After partial decryption recovery on a computer with an HCA card, the local Dell Data Protection | Encryption console may display duplicate information about local disks. To work around this issue, reboot the computer. After the restart, disk information displays properly. [28656]
- After installation of Enterprise Edition, the Microsoft Usbccid Smartcard Reader is intermittently reported as being in a problem state in Device Manager. However, smart cards and fingerprints seem to function normally. Dell ControlVault relies on the Microsoft Usbccid drivers. A premier case has been opened with Microsoft regarding this issue. [28697]
- Decryption on computers with HCA cards removes Preboot Authentication, which must be reinstalled. At the next logon, both an Encryption Administrator Password prompt and a Security Tools shutdown message display. When the computer is shut down, PBA activation begins. However, provisioning will be completed only after a subsequent reboot and entry of the Encryption Administrator Password. [28722]
- Infrequently, after HCA policy is set, the Preboot Authentication screen does not display until the computer is restarted a second time. [28762]
- Support for migrating the Personal Edition HCA preboot environment into Enterprise Edition is not available in v8.3. [28794]
- After encryption is enabled, the computer intermittently logs a Critical System Event 41 in the System Event Logs with this description: "The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly." The issue occurs only during a reboot and does not impact the security of the data or the performance of the computer. [28795]
- Amended 12/2014 - Secure Boot is a Unified Extensible Firmware Interface (UEFI) protocol that Windows 8 and 8.1 users can enable in the computer's BIOS to ensure that the computer boots using trusted firmware signed by the computer manufacturer. The feature is not supported when the following conditions are met:

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

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

    Instructions:

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

   [28790]

- When running Windows 7, a computer that is HCA encrypted may not boot in Windows Safe Mode. [28819]
- When using EMS Explorer, cutting and pasting a file does not remove the file from its original location. [28848]
- After an upgrade from v8.2 to v8.3, the v8.2 Dell Data Protection | Encryption installer remains on the computer. [28885]
- During an SDE encryption sweep, although the disk is only partially encrypted based on the progress of the sweep, the Security Console Encryption screen shows the disk as Protected. [28888]
- Fingerprints and smart cards stop working after the Port Control System policy to disable USB ports is applied. Broadcom USH hardware is a USB-attached device. When the policy to disable USB ports is applied, it prevents data transmission to and from the Broadcom USH hardware, which prevents users from logging on with fingerprints or smart cards. The

problem can be resolved by applying a combination of policies that restrict access to USB external media by setting Windows Portable Device and External Storage Device class policy to Read Only. This policy combination allows the Broadcom USH hardware to function properly but prevents data from being transferred from the computer to external media such as USB flash drives and smart phones. [28895]

Advanced Authentication

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

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

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

   [28528, 28678, 28719]

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

  Deactivate the PBA

  Uninstall Security Framework

Uninstall Security Tools Authentication

[28791]

Cloud Edition

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

New Features and Functionality v8.2.1

- Personal Edition now supports Microsoft Windows 8.1.

Resolved Technical Advisories v8.2.1

Encryption

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

Technical Advisories v8.2.1

Advanced Authentication

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

New Features and Functionality v8.2

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

Technical Advisories v8.2

Advanced Authentication

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

Resolved Technical Advisories v8.1.1

Encryption

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

New Features and Functionality v8.1

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

Resolved Technical Advisories v8.1

All Products

- Windows Vista is no longer a supported operating system.

Encryption

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

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]
  AlwaysApplySDE=REG_DWORD:1
  ```

- If an SDE encrypted file is moved (not copied) to a Common or User encrypted folder, the Shield now properly applies the Common or User encryption policy, rather than remaining SDE encrypted. [27752]

Advanced Authentication

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

Technical Advisories v8.1

Encryption

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

Cloud Edition

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

Resolved Technical Advisories v8.0.1

Encryption

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

Resolved Technical Advisories v8.0

Encryption

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

Cloud Edition

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

Technical Advisories v8.0

Encryption

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

Cloud Edition

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

2

Workarounds

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

- 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 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.
- If a user adds or removes smart card reader hardware without rebooting the Windows smart card, Dell Encryption may not properly recognize authentication. If this happens, the Dell Encryption prompts for alternate authentication. To work around this issue, reboot the Windows device. [9135]

3

Software and Hardware Compatibility

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

Upgrade to the latest Windows 10 Feature Update

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

Aventail Access Manager

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

Norton 360

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

Norton Ghost

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

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

AVG Antivirus Protection

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

Kaspersky Anti-Virus Protection

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

Windows Devices

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

McAfee Host Intrusion Detection

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

Webroot

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

Hacks and Utilities

- Hacks or utilities that alter device manufacturer performance specifications are not supported.