Dell Data Security

Endpoint Security Suite Enterprise Technical Advisories v1.7.1

Notes, cautions, and warnings

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

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

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

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

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

Endpoint Security Suite Enterprise Technical Advisories

2018 - 01

Rev. A03

Contents

1

Technical Advisories

Endpoint Security Suite Enterprise offers advanced threat protection at the operating system and memory layers, authentication, and encryption, all centrally-managed from the Security Management Server or Security Management Server Virtual. With centralized management, consolidated compliance reporting, and console threat alerts, businesses can easily enforce and prove compliance for all of their endpoints. Security expertise is built in with features such as pre-defined policy and report templates, to help businesses reduce IT management costs and complexity.

Contact Dell ProSupport

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

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

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

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

New Features and Functionality v1.7.1

- FDE is now supported with smartcard preboot authentication on supported Dell computers running in UEFI boot mode
- FDE is now supported on non-English operating systems:
  - EN - English
  - JA - Japanese
  - ES - Spanish
  - KO - Korean
  - FR - French
  - PT-BR - Portuguese, Brazilian
  - IT - Italian
  - PT-PT - Portuguese, Portugal (Iberian)
  - DE - German
- FDE is available for beta testing in non-production environments on Dell computers running legacy boot mode.
- FDE encryption drivers are now compatible with HVCI .
- Web Protection and Client Firewall features are now supported with Windows 10 Fall Creators Update (Redstone 3 release).

Resolved Technical Advisories v1.7.1

Encryption Client v8.17.1

- Italian translations have been corrected for the Home/Advanced tab names. [DDPC-5825, DDPC-5826]
- An issue that resulted in a the computer becoming unresponsive when Dell Encryption and Symantec Endpoint Protection were installed on the same device has been resolved. [DDPC-7808]

- An issue causing the smart card login to fail when the smart card certificate information in the registry missing has been resolved. [DDPC-7904]
- An issue resulting with an error message of "Unable to generate catalog" after an upgrade from Redstone 2 to Redstone 3 with encryption client installed has been resolved. [DDPC-7946]

Preboot Authentication v8.17.1

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

Full Disk Encryption v1.1

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

Technical Advisories v1.7.1

Encryption Client v8.17.1

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

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

Preboot Authentication v8.17.1

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

SED Management v8.17.1

- Currently, an error message of "Unhandled exception has occurred in your application" appears during an upgrade of Digital Persona's Auth when the Dell Data Security Console is also open during the upgrade. [DDPC-7836]
- The Oberthur chip only smart card ID-One COSMO V7.0 is read by the PBA but fails to log in on a UEFI machine. [DDPC-7985]
- In some cases, Smart card readers are not detected on legacy machines. [DDPC-8030]

Full Disk Encryption v1.1

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

Legacy Boot Mode FDE

For beta testing in non-production environments

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

Bitlocker Manager v8.17.1

- Currently, an error message of "Unhandled exception has occurred in your application" appears during an upgrade of Digital Persona's Auth when the Dell Data Security Console is also open during the upgrade. [DDPC-7836]
- The policy line of: <PasswordUse MinimumPasswordLength="8" PasswordComplexity="Allow" Usage="Allow" />

  is forcing a secondary drive, which the D: drive is being seen at, to unlock with a password. Before the password unlock, this volume is not mount-able. It seems that once this is unlocked, the shield is not properly seeing this drive being mounted as a "Fixed disk", even though PCS is classifying it as:

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

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

New Features and Functionality v1.7

- Added 01/2018- Dell's Preboot Authentication environment for Self-Encrypting Drive and Full Disk Encryption now has built-in resiliency. If the data-store for user credentials in the PBA becomes corrupted, it will revert to a known-good database. This can be manually initiated by holding the Control and Alt keys, and then pressing 'b' on the keyboard.
- The Encryption client is now supported with Windows 10 Fall Creators Update (Redstone 3 release). Upgrades to Fall Creators Update are now supported.
- SED Management and Bitlocker Manager are now supported with Windows 10 Fall Creators Update (Redstone 3 release). Upgrades to Fall Creators Update are supported, except for upgrades from Windows 7.
- Full Disk Encryption is now supported with Windows 10 Fall Creators Update (Redstone 3 release). Upgrade to Fall Creators Update will be supported in v8.17.1. In 8.17, PBA deactivation/decryption are required in order to upgrade to Fall Creators Update.
- The Encryption client local console now shows status of "In Compliance" when there are no pending policies and an initial sweep is complete, regardless whether the Encryption policy is enabled on the Dell Server.
- System-created files in the \Windows folder are no longer encrypted, regardless of policy settings. This behavior can be changed by adding a Category 3 inclusion to SDE Encryption Rules.

Resolved Technical Advisories v1.7

Encryption Client v8.17

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

Preboot Authentication v8.16.1

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

Technical Advisories v1.7

All Clients

- No Technical Advisory exists for all clients

Dell Encryption v8.17

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

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

[DDPC-7794]

Preboot Authentication v8.16.1

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

SED Management v8.16.1

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

Full Disk Encryption v1.1

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

BitLocker Manager v8.16.1

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

New Features and Functionality v1.6

- Added 12/2017 - Advanced Threat Prevention is now supported with Windows 10 Fall Creators Update (Redstone 3 release), build 1441 or later. Upgrades to Fall Creators Update are supported with build 1441 or later. Fall Creators Update is supported with OneDrive; however, OneDrive files that have been stored to the computer before the initial ATP scan are not scanned until they are opened.
- Added 12/2017 - In future version of v8.17.1, Web Protection and Client Firewall features will be supported with Windows 10 Fall Creators Update (Redstone 3 release).
- Endpoint Security Suite Enterprise now supports TLS 1.2 when used with a Dell Server v9.9 or newer.
- Endpoint Security Suite Enterprise now supports IPv6.
- Web Protection and Client Firewall features are now supported with Windows 10 Creators Update (Redstone 2).
- Full Disk Encryption is now optionally available with Endpoint Security Suite Enterprise for Dell computers running in UEFI boot mode with non-SED drives. Full Disk Encryption provides administrators central management of Preboot Authentication in addition to disk encryption, with the capability to remotely disable endpoint login and lock the device. Keys are protected with the Trusted Platform Module (TPM), preventing access to encrypted data in the event that the hard drive is removed from the computer.
- Web Protection and Client Firewall features can now be installed independently of Dell Encryption.
- A new policy enables Advanced Threat Prevention to detect and address malicious payloads with the following options:
  - Ignore - No action is taken against identified memory violations.
  - Alert - Record the violation and report the incident to the Dell Server.
  - Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run.
  - Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call.
- 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.
- Endpoint Security Suite Pro has reached End of Life. For information, see http://www.dell.com/support/article/us/en/19/sln305349.

Resolved Technical Advisories v1.6

All Clients

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

Advanced Threat Prevention v1.6

Resolved Customer Issues

- The Advanced Threat Prevention selection now remains selected during installation on a server operating system if the check box for the Web Protection and Firewall option is cleared. [DDPC-6319]

Encryption Client v8.16

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

Resolved Customer Issues

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

SED and FDE Preboot Authentication v8.16

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

Resolved Customer Issues

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

SED Management v8.16

Resolved Customer Issues

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

BitLocker Manager v8.16

No Resolved Technical Advisories exist.

Technical Advisories v1.6

Advanced Threat Prevention v1.6

- Added 12/2017 - If users attempt to run the optional Web Protection and Firewall features with Windows 10 Fall Creators Update (Redstone 3 release), the following occur:
  - If a user attempts to install Advanced Threat Prevention and optional Web Protection and Firewall features on Windows 10 Fall Creators Update (Redstone 3 release), only Advanced Threat Prevention is installed.
  - If a user attempts to upgrade to Fall Creators Update with Advanced Threat Prevention and optional Web Protection and Firewall features installed, Windows 10 Setup prompts the user to uninstall Client Firewall and Web Protection.
  - In some circumstances, the Web Protection and Client Firewall tile displays in the Data Security Console following a failed install.
- In the Data Security Console, in the Advanced Threat Prevention Tile, "Protection" is incorrectly translated to "Disabled" in Italian. [DDPC-7455]

- Command line upgrade for Client Firewall and Web Protection requires the installers to be run in a specific order. Failure to install the components in the proper order results in upgrade failure. Run the installers in the following order:
  - **\Threat Protection\EndPointSecurity**

    The following installs Web Protection and Client Firewall with default parameters (silent mode, install Client Firewall and Web Protection, override Host Intrusion Prevention, no content update, no settings saved).

    ```
    EPSetup.exe ADDLOCAL="fw,wc" /override"hips" /nocontentupdate /nopreservesettings /l"C:
    \ProgramData\Dell\Dell Data Protection\Installer Logs\McAfee" /qn
    ```

  - **\Threat Protection\ThreatProtection\WinXXR**

    The following example installs the client with default parameters (suppress the reboot, no dialogue, no progress bar, no entry in Programs list).

    ```
    DellThreatProtection.msi /qn REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1 /l*v "<C:
    \ProgramData\Dell\Dell Data Protection\Installer Logs\Dell> Data Protection - Threat
    Protection.msi.log"
    ```

  - **\Threat Protection\SDK**

    The following command line loads certificate default parameters.

    ```
    "Threat Protection\SDK\EnsMgmtSdkInstaller.exe" -LoadCert >"C:\ProgramData\Dell\Dell Data
    Protection\Installer Logs\McAfeeSDKInstallerBeforeEndPoint.log"
    ```

  - **\Threat Protection\SDK**

    The following example installs the SDK.

    ```
    EnsMgmtSdkInstaller.exe "C:\Program Files\Dell\Dell Data Protection\Threat Prevention
    \DellAVAgent.exe" -InstallSDK -RemoveRightClick -RemoveMcTray > "C:\ProgramData\Dell\Dell
    Data Protection\Installer Logs\McAfeeSDKInstallerAfterEndPoint.log"
    ```

Dell Encryption v8.16

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

PBA Advanced Authentication v8.16

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

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" = DWORD:1

  0=Enabled (default)

  1=Disabled

  [DDPC-7019]

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

Preboot Authentication v8.16

SED Management v8.16

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

Full Disk Encryption v1.0

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

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

BitLocker Manager v8.16

- No Technical Advisories exist.

New Features and Functionality v1.5

- A new policy in Security Management Server/Security Management Server Virtual v9.8 allows administrators to block more than 100 specific categories of information on the Internet, when the optional Web Protection feature is installed.
- A new policy in Security Management Server/Security Management Server Virtual v9.8 allows the administrator to enable or disable users' ability to select **Remember Me** on the PBA login screen and customize Support dialog text.
- The Encryption client drivers pass the Hypervisor Code Integrity (HVCI) checks.

- Operating system downgrade is now supported with the Encryption client.
- SSL is no longer supported with Advanced Authentication, SED Management, or BitLocker Manager. TLS 1.0, 1.1, or 1.2 should be used rather than SSL.
- The Security Tools Mobile application has reached End of Life. For more information, see www.dell.com/support/article/us/en/19/sln305349.
- Windows 10 Creators Update is not yet supported with the optional Web Protection and Firewall features. For this reason, installation of these features is prevented on Windows 10 Creators Update.

Resolved Technical Advisories v1.5

All Clients

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

Advanced Threat Prevention v1.5

- Decryption performance is improved on a computer running Advanced Threat Prevention after policy is set to decrypt. [DDPC-5365]
- File cleanup during uninstallation is improved. [DDPC-5594]

Resolved Customer Issues

- A second license is no longer consumed when the optional Web Protection and Firewall features are installed. [DDPC-6407]

Resolved Technical Advisories - Auto-Updates

For information about periodic Advanced Threat Prevention updates for enterprises enrolled for Agent Auto Update on the Dell Server, see http://www.dell.com/support/article/us/en/19/SLN305419/dell-data-protection-endpoint-security-suite-enterprise-and-dell-data-protection-threat-defense-release-notes?lang=EN. Select the **Saas Updates** tab.

For instructions on how to enroll for Agent Auto Update on the Dell Server, refer to *AdminHelp*, accessible from the Remote Management Console.

Encryption Client v8.15

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

Resolved Customer Issues

- An issue is resolved that resulted in unresponsiveness of the computer following hibernation. [DDPC-1475]
- An issue is resolved that caused the computer to become unresponsive, followed by a Windows bugcheck. [DDPC-2349, DDPC-3284]
- Two issues are resolved that led to errors in applications that were running during an encryption sweep. [DDPC-2751, DDPC-4444]
- After upgrade to Windows 10, a second restart is no longer required in certain cases for encryption to resume. [DDPC-4080]

- The computer now restarts after Port Control policies are enabled or updated. [DDPC-5255]
- Diagnostic Info performance and error messaging are improved. [DDPC-5559]
- File names on the Start menu are now correctly translated into French. [DDPC-5895]

Preboot Authentication v8.15

Resolved Customer Issues

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

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]

BitLocker Manager v8.15

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

Resolved Customer Issues

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

Technical Advisories v1.5

Advanced Threat Prevention v1.5

- In rare situations, new policies may not be properly enforced by the Advanced Threat Prevention client, although existing policies are enforced as expected. To work around this issue if it occurs, reinstall the Advanced Threat Prevention client. (CYL-611)
- To block all PowerShell scripts with Advanced Threat Prevention, both the PowerShell and PowerShell Console policies must be set to **Block** in the Dell Server Remote Management Console. When both policies are set to Block, no scripts can be run, either through the PowerShell console or the Cmd console. This ensures that PowerShell one-line scripts are not vulnerable to execution. To allow approved scripts to run through the Cmd console, select the Enable Approve Scripts in Folders (and Subfolders) policy, and add the approved scripts to the Approve Scripts in Folders (and Subfolders) policy.

  NOTE: The PowerShell Console policy applies to PowerShell v3 and later. Windows 7 includes PowerShell v2, by default. To upgrade to PowerShell v3 on Windows 7, see www.microsoft.com/en-us/download/details.aspx?id=34595.

  [CYL-619]
- After Auto-Update to v2.0.1441, the Advanced Threat Prevention tile may no longer display in the Dell Data Security Console. To work around this issue, run the following command:

  ```
  MSIEXEC.EXE /I "ATP_CSF_Plugins_x64.msi" APPFOLDER="C:\Program Files\Dell\Dell Data Protection
  \Advanced Threat Protection\Plugins" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer
  Logs\ATP_CSF_Plugins_x64.msi.log"
  ```

  The .msi file can be found in the following folder, extracted from the installation package: **\Advanced Threat Prevention\WinXXr**

  If the issue persists, contact ProSupport. [CYL-626]
- Enterprise policies for Advanced Threat Prevention running in Disconnected Mode can currently be managed by adding SHA256 values of threats directly to Endpoint Groups. [CYL-629]

- The Advanced Threat Prevention selection can become unselected during installation on a server operating system if the check box for the Web Protection and Firewall option is cleared. To work around this behavior, after clearing the Web Protection and Firewall check box, reselect **Advanced Threat Prevention**. [DDPC-5722]
- Windows 10 Creators Update is not yet supported with the optional Web Protection and Firewall features.

Technical Advisories - Auto-Updates

For information about periodic Advanced Threat Prevention updates for enterprises enrolled for Agent Auto Update on the Dell Server, see http://www.dell.com/support/article/us/en/19/SLN305419/dell-data-protection-endpoint-security-suite-enterprise-and-dell-data-protection-threat-defense-release-notes?lang=EN. Select the **Saas Updates** tab.

For instructions on how to enroll for Agent Auto Update on the Dell Server, refer to *AdminHelp*, accessible from the Remote Management Console.

Encryption Client v8.15

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

[DDPC-5521, DDPC-5670]

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

Advanced Authentication v8.15

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

Preboot Authentication v8.15

- A few keys on Canadian French and British/English keyboards behave differently than expected on computers running in UEFI mode. [DDPC-5369, DDPC-5969]
- An intermittent "System Failed" error may display after inserting a smart card for PBA login on the OptiPlex 3240 All-In-One. [DDPC-5907]
- A few keys on a Brazilian Portuguese keyboard behave differently than expected on the Dell Precision M4800 running in UEFI mode. [DDPC-5975]
- A delay in display of the PBA login screen has been observed on the following Dell computers: Optiplex 5055, Precision 5820T, Precision 7820T, and Precision 7920T. [DDPC-6375]
- Recovery of a SanDisk X300 drive with the Recovery All bundle succeeds but may require up to two minutes to complete. [DDPC-6389]
- The backslash/pipe (\ |) key on an Arabic behaves differently than expected. [DDPC-6529]
- SSL is no longer supported. TLS 1.0, 1.1, or 1.2 should be used rather than SSL.

SED Client v8.15

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

BitLocker Manager v8.15

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

New Features and Functionality v1.4

- Endpoint Security Suite Enterprise now includes the optional features, Client Firewall and Web Protection. The Client Firewall is a stateful firewall that checks all incoming and outgoing traffic against its list of rules. Web Protection monitors web browsing and downloads to identify threats and enforce action set by policy when a threat is detected, based on ratings for websites. Prior to upgrade to the new features, follow the instructions in Upgrade to Endpoint Security Suite Enterprise v1.4.
- Advanced Threat Prevention is now supported with Server 2016.
- The Encryption client is now supported with the Windows 10 Creators Update (Redstone 2 release).
- BitLocker Manager is now supported with Server 2016.
- Added 5/2017 - Remote PBA management of local user accounts is now available.
- Endpoint Security Suite Enterprise is **not** supported with Windows Server 2008 (non-R2 version).
- Users can now access ProSupport contact information from the About screen in DDP Console.

Resolved Technical Advisories v1.4

Advanced Threat Prevention v1.4

Resolved Customer Issues

- The system tray icon is now interactive as expected when running Disconnected Mode. [DDPC-5263]

Resolved Technical Advisories - Auto-Updates

For information about periodic Advanced Threat Prevention updates for enterprises enrolled for Agent Auto Update on the Dell Server, see http://www.dell.com/support/article/us/en/19/SLN305419/dell-data-protection-endpoint-security-suite-enterprise-and-dell-data-protection-threat-defense-release-notes?lang=EN. Select the **Saas Updates** tab.

For instructions on how to enroll for Agent Auto Update on the Dell Server, refer to *AdminHelp*, accessible from the Remote Management Console.

Encryption Client v8.13

- 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]
- VDI client activation error handling is improved. [DDPC-4474]
- Log files are now collected when Diagnostic Info is run on a server OS. [DDPC-5206]
- Changes to Common Encryption exclusions are now enforced while the user is logged in. [DDPC-5213]

Resolved Customer Issues

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

  Set the EnableNGMetadata registry entry in the following location:

  [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CmgShieldFFE]

  "EnableNGMetadata" = dword:1

  0=Disabled (default)

  1=Enabled

  [DDPC-694, DDPC-794, DDPSUS-863]
- An issue is resolved that resulted in access denial errors for non-domain users. [DDPC-854]
- Decryption performance is improved when SDE Encryption is enabled. [DDPC-3577, DDPSUS-975]
- An issue is resolved that occasionally caused the Encryption client to become unresponsive with warnings in the log files. [DDPC-5311]

Advanced Authentication v8.13

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

Resolved Customer Issues

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

Preboot Authentication v8.13

- Preboot Authentication is supported on the following computers:
  - Latitude 5280
  - Latitude 5480
  - Latitude 5580

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

SED Client v8.13

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

BitLocker Manager v8.13

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

Technical Advisories v1.4

Advanced Threat Prevention v1.4

- Setting an Action in a Client Firewall rule to Block IPv4 traffic prevents client connectivity with the Dell Server. Do not set such an Action when running in Connected Mode. [DDPC-5716]
- During migration from Enterprise Edition to Endpoint Security Suite Enterprise the optional features, Web Protection and Firewall, are not selected by default in the installer and must be manually selected for installation. [DDPC-5888]
- The Client Firewall and Web Protection features of Endpoint Security Suite Enterprise v1.4 require Dell Enterprise Server or VE v9.7 or later. Before upgrading clients to use these features, Dell Server v9.7 or later must be installed and the policy, Memory Action: Exclude executable files, must be ***enforced*** on pre-v1.4 clients. Prior to client upgrade to the new features, refer to Upgrade to Endpoint Security Suite Enterprise v1.4 for the policy's new default value. Do not begin client upgrade before the new policy is enforced on the client. [DDPS-5112]
- Endpoint Security Suite Enterprise will be supported with the Windows 10 Creators Update (Redstone 2 release) in a later release.

Technical Advisories - Auto-Updates

For information about periodic Advanced Threat Prevention updates for enterprises enrolled for Agent Auto Update on the Dell Server, see http://www.dell.com/support/article/us/en/19/SLN305419/dell-data-protection-endpoint-security-suite-enterprise-and-dell-data-protection-threat-defense-release-notes?lang=EN. Select the **Saas Updates** tab.

For instructions on how to enroll for Agent Auto Update on the Dell Server, refer to *AdminHelp*, accessible from the Remote Management Console.

Encryption Client v8.13

- Pausing encryption from the system tray icon does not pause the encryption sweep. [DDPC-5372]
- After policy update that requires reboot, the reboot prompt occasionally displays off-screen on the Dell Latitude 7280. [DDPC-5376]
- Encryption overlay icons display on unmanaged users' files when overlay icons are enabled for managed users on the same computer. [DDPC-5415]

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

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

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 http://www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/drivers.

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

  [DDPC-5941, DDPC-6219]

BitLocker Manager v8.13

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

New Features and Functionality v1.3

- Endpoint Security Suite Enterprise now supports persistent and non-persistent VMware and Citrix VDI clients with Dell Data Protection Server v9.6 and later.
- Added 4/2017 - The Encryption client is now supported with Windows Server 2016 - Standard Edition, Essentials Edition, and Datacenter Edition.
- Added 4/2017 - BitLocker Manager is now supported with Server 2012 and Server 2012 R2 - Standard Edition and Enterprise Edition (64-bit).
- The PBA user interface has a new look and feel.
- New policies allow the administrator to configure the maximum number of Dell Server connection attempts and the retry interval for the Encryption client running on a server OS.
- A standalone version of Encrypt for Sharing, Encrypt4Share.exe, is now added to the <installation folder>\Dell Data Protection \Encryption folder at installation and can be accessed from the Windows Start menu.

Resolved Technical Advisories v1.3

Advanced Threat Prevention v1.3

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

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

  "MaxPoliciesStored" =dword:00000010

  Valid range = 0 - 100

  [DDPC-4583]

Added 4/2017 - Resolved Technical Advisories v2.0.1421

The following issues are resolved in v1.3.1421, available when an organization is enrolled for Agent Auto Update on the Dell Server. For instructions on how to enroll, refer to *AdminHelp*, accessible from the Remote Management Console.

- Fixed an issue where the Agent communicated using SSL 3.0 or TLS 1.0 only.
- Fixed an issue with a Windows device failing to generate a fingerprint.
- Resolved issue with Microsoft Word template file not being recognized when added to the whitelist.
- Fixed an issue with the Windows OS version incorrectly being reported to the Console.
- Fixed an issue with the false detection of Nsight drivers on Windows devices.
- Fixed an issue on Windows x64 devices where a malicious payload detection was causing crashes upon exit.
- Fixed an issue with 64-bit Java applications crashing.
- Fixed an issue where the CPU would spike with integration service on a Windows device.

- Resolved an issue with an inconsistency on start-up on a Windows device.
- Resolved BSOD due to exception issue with Device Control when using display port.
- Resolved an issue with the Auto-Quarantine feature preventing the EventPro application user-interface from launching on a Windows device.
- Resolved an issue with the Agent sending duplicate Syslog events to the Console.
- Fixed an issue where the Agent could cause 32-bit Java applications to crash on Windows devices.
- Fixed Script Control to not block a Microsoft Windows 10 script.
- Fixed an issue where installing the Agent MSI package using the command line without including the installation token resulted in the Agent requiring an uninstall password and the Agent could not be uninstalled.
- Fixed an issue where a USB device was not being blocked upon first use on Windows XP and Windows Server 2003 devices when Device Control was enabled and set to Block.
- Fixed an issue with WMI errors occurring on Windows devices during startup and shutdown.
- Fixed an issue with Device Control events to generate a serial number when a USB mass storage device is disabled then enabled on a Windows device.
- Fixed duplication of Device Control events for iOS USB connection to a Windows device.
- Fixed duplication of Device Control events for Android USB connection to a Windows device.
- Fixed an issue with the event log on a Windows device to include the device serial number for iOS devices.
- Fixed an issue with the Application Control folder exclusions to prevent portable executable (PE) files from manually being moved on a Windows device.
- Fixed an issue that was causing threat files to be quarantined from a macOS Samba SMB mounted drive.
- Fixed an issue with the ability to recognize a trailing backslash in Application Control folder exclusions on a Windows device.
- Fixed an Application Control issue with the ability to copy a file from a non-excluded folder to an excluded folder on a Windows device.
- Fixed an issue with the Optics to only upload Windows logs that have not been uploaded before.
- Fixed an issue with the ability to downgrade the local cloud model on macOS devices.
- Fixed an issue with Device Control events to include the detection of USB floppy drives on Windows devices.
- Fixed an issue with duplicated Device Control events being generated when connecting a USB drive to a Windows device.
- Fixed an issue with the event log on a Windows device to include the device serial number when connecting a USB device to a VMware Workstation instance.
- Fixed an issue with the event log on a Windows device to include the device serial number for an Apple iPad.
- Fixed an issue with the event log on a Windows device to include the serial number for Canon cameras.
- Fixed an issue with scanning folders externally mounted to a macOS device, where the file is not local.
- Fixed an issue with the rate that the Agent checks the status of the cloud model when the Console communication is not responsive.
- Fixed an issue with the Visual Studio App Simulator from being blocked as an exploit on macOS devices.
- Fixed an issue with the timer to add a random buffer for checking in to the Console after a connection is re-established.
- Fixed a Windows issue where memory allocated to fields in DEVFLT_CONTEXT are not freed.
- Fixed an issue where the uploader repeats when the upload limit is reached.
- Updated the localization files to ensure translations work on OS X El Capitan.
- Fixed a Windows boot issue when the Console is unavailable.
- Fixed an issue with the macOS Sierra Beta build crashing the Agent UI.

Added 4/2017 - Resolved Technical Advisories v1.2.1411

The following issues are resolved in v1.3.1411, available when an organization is enrolled for Agent Auto Update on the Dell Server. For instructions on how to enroll, refer to *AdminHelp*, accessible from the Remote Management Console.

- Resolved a compatibility issue between Memory Protection and Windows 10 Credential Guard.
- Fixed an issue where Windows Security Center registration fails when installing the Agent via GPO
- Fixed an issue where files added to the Global Safelist were not properly waived by the Agent.
- Fixed an issue to ensure quarantined files remain quarantined, even if multiple copies of the file in question get copied to the computer.
- Fixed an issue where the ScriptCache folder was consuming too much disk space if Script Control for Office Macros was enabled. Office documents are no longer cached as part of ScriptCache; only ActiveScript and PowerShell scripts are cached.
- Fixed an issue to ensure that on-demand scans are using both the Local model as well as Cloud lookups, as with background scans.

- Resolved a compatibility issue between Memory Protection and Remote Desktop on Windows 8 computers.
- Fixed an issue where the Agent does not attempt to re-deliver device system information to the Management Console if the send operation times out.
- Fixed an issue to allow Script Control exceptions for web-based locations.
- Fixed an issue to ensure that the Background Threat Detection status is accurately reported.
- Fixed an issue where the Agent may not properly send the file hash to the Management Console, resulting in an error in the Management Console.
- Fixed an issue where the Agent does not properly register with the Management Console if the Agent is installed without network access.
- Resolved a compatibility issue between Memory Protection and Passport.
- Resolved a compatibility issue between Memory Protection and NVIDIA Nsight.
- Fixed an issue where Agents deleted from the Management Console would still attempt to connect to the Management Console to upload Agent logs.
- Resolved a compatibility issue between Memory Protection, Auto-Quarantine (AQT) and Novell Zenworks Logger.
- Fixed an issue where the Advanced Threat Protection service was not properly starting on devices using .NET 4 Client Profile.
- Fixed an issue where the Windows installation would not accept the Installation Token if the device is offline.
- Fixed an issue where the Windows OS version was incorrectly reported, causing issues with Zone Rules.
- Fixed an issue to ensure Auto-Update properly updates both the Agent and Optics.
- Resolved an issue where the Agent was snot updating Optics with the Device ID if Optics was installed prior to Agent registration with the Management Console.
- Fixed an issue to ensure that Local models are fully loaded before scanning files.
- Fixed an issue to ensure that USB devices encrypted with BitLocker can be accessed.
- Fixed an issue where Optics was not properly updating the product version number in Add/Remove Programs.
- Fixed an issue where the Windows theme would crash when the device starts.
- Fixed an issue where certain files paths were causing issues for Script Control exclusions.
- Resolved an issue in Windows 8 where Advanced Threat Prevention would appear as expired under certain circumstances.
- Fixed an issue where the macOS Agent and Windows installation would not accept the Installation Token if the device is offline.
- Fixed an issue where the macOS Agent blocked the Xcode debugger from running.
- Fixed an issue where the macOS Agents will repeatedly try to upload a file to the Management Console, even if the file is too large to upload.
- Fixed an issue where Watch For New Files was not properly working for long file paths on macOS systems.
- Fixed an issue where Memory Protection was not working properly on macOS computers.
- Resolved a compatibility issue with macOS Sierra and Time Machine on non-Apple network attached storage.
- Fixed an issue where Watch For New Files was incorrectly scanning mounted network drives on macOS computers.

Resolved Technical Advisories v1.2.1401.84

The following issues are resolved in v1.2.1401.84, available when an organization is enrolled for Agent Auto Update on the Dell Server. For instructions on how to enroll, refer to *AdminHelp*, accessible from the Remote Management Console.

- Increased the detail available in the debug logs.
- Fixed an issue to properly waive files contained within archives.
- Fixed an issue where files whitelisted by certificate were incorrectly labeled as "catalog."
- Fixed an issue where a portable executable (PE) file was able to be copied onto a device with Application Control enabled.
- Fixed an issue where threats are blocked but not properly terminated (killed) in some OS X environments.
- Updated Memory Protection to include support for Metro Apps.
- Fixed an issue that caused a crash on the Windows Vista operating system.
- Fixed an issue where the user-interface notifications were not properly working for archived files.
- Fixed an issue with updating the Agent.
- Fixed an issue where Alternate Data Streams (ADS) filenames were not properly handled.
- Fixed an issue where some Memory Protection and Script Control events were not properly sent to the Console..
- Fixed an issue where the Agent UI would display erroneous text caused by the localization language folders not deploying correctly to the Cylance directory and being absent from the directory.

NOTE: Agent version 1401 supports Windows 10 Anniversary Edition but does not support Device Guard or Credential Guard, optional Windows 10 security features. If these features are enabled, disable them before using the Agent.

Added 4/2017 - Resolved Technical Advisories - Auto-Updates

For information about additional periodic Advanced Threat Prevention updates for enterprises enrolled for Agent Auto Update on the Dell Server, see http://www.dell.com/support/article/us/en/19/SLN305419/dell-data-protection-endpoint-security-suite-enterprise-and-dell-data-protection-threat-defense-release-notes?lang=EN. Select the **Saas Updates** tab.

For instructions on how to enroll for Agent Auto Update on the Dell Server, refer to *AdminHelp*, accessible from the Remote Management Console.

Encryption Client v8.12

- Debug-level logging is improved. [DDPC-2307]
- Administrative Download Utility (CMGAd) and Administrative Unlock Utility (CMGAu) are now functioning as expected with non-domain users. [DDPC-4109]
- Upgrade to Windows 10 now proceeds as expected when the installation media is stored in a folder that is encrypted with the User or Common key. [DDPC-4146]
- The Secure Windows Hibernation File and Prevent Unsecured Hibernation policies are now enforced after upgrade. [DDPC-4786]
- The WSScan **Unencrypted file in Violation** option now initiates a sweep of unencrypted files as expected, without the files having to be selected or accessed. [DDPC-4790]
- 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 v8.12

- The Enroll Credentials window no longer occasionally displays after a computer with fingerprint or smart card enrolled credentials resumes from sleep. [DDPC-4269]
- Effective policies from the Dell Server are now automatically exported and stored in C:\ProgramData\Dell\Dell Data Protection\Policy \Policy-xxxxxxxx.xml, where "xxxxxxxx" is the sequence number of the policy. By default, the last 10 policies received from the Server are stored. To change the default number of policies stored, change the value of the following registry key. The valid range is 0 - 100.

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

  "MaxPoliciesStored" =dword:00000010

  Valid range = 0 - 100

  [DDPC-4583]

Preboot Authentication v8.12

- Amended 4/2017 - Preboot Authentication is supported ***only*** with UEFI mode (with and without SecureBoot) on the following computers:
  - OptiPlex 3050 All-In-One
  - OptiPlex 5250 All-In-One
  - OptiPlex 7450 All-In-One

- OptiPlex 3050 Tower, Small Form Factor, Micro
- OptiPlex 5050 Tower, Small Form Factor, Micro
- OptiPlex 7050 Tower, Small Form Factor, Micro
- Latitude 3180
- Latitude 3189
- Latitude 3380
- Latitude 3480
- Latitude 3580
- Latitude 5285
- Latitude 5289
- Precision 7520
- Precision 7720
- Precision 5720 All-in-One

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

SED Client v8.12

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

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

  "MaxPoliciesStored" =dword:00000010

  Valid range = 0 - 100

  [DDPC-4583]

BitLocker Manager v8.12

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

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

  "MaxPoliciesStored" =dword:00000010

  Valid range = 0 - 100

[DDPC-4583]

Technical Advisories v1.3

All Clients

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

Advanced Threat Prevention v1.3

- Persistent and non-persistent clients' Protected status differs in the Dell Server Remote Management Console:

  Persistent - Following the first restart after activation, the client status is Protected.

  Non-Persistent - The client status does not change to Protected after activation, since the virtual machine does not retain the client instance after restart.

Encryption Client v8.12

- 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]
- When the Encryption client is installed on Windows Server 2016 Standard Edition, the OS/Version field for the Endpoint reads "Unknown/null" in the Dell Server. [DDPC-4836]
- When encryption or decryption is paused, the Compliance/Provisioning status may not be accurately indicated in the Local Management Console. [DDPC-5063]

Preboot Authentication v8.12

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

Resolved Technical Advisories v1.2

Advanced Threat Prevention v1.2

Added 4/2017 - Resolved Technical Advisories v2.0.1421

The following issues are resolved in v1.2.1421, available when an organization is enrolled for Agent Auto Update on the Dell Server. For instructions on how to enroll, refer to *AdminHelp*, accessible from the Remote Management Console.

- Fixed an issue where the Agent communicated using SSL 3.0 or TLS 1.0 only.
- Fixed an issue with a Windows device failing to generate a fingerprint.
- Resolved issue with Microsoft Word template file not being recognized when added to the whitelist.
- Fixed an issue with the Windows OS version incorrectly being reported to the Console.
- Fixed an issue with the false detection of Nsight drivers on Windows devices.
- Fixed an issue on Windows x64 devices where a malicious payload detection was causing crashes upon exit.
- Fixed an issue with 64-bit Java applications crashing.
- Fixed an issue where the CPU would spike with integration service on a Windows device.
- Resolved an issue with an inconsistency on start-up on a Windows device.
- Resolved BSOD due to exception issue with Device Control when using display port.
- Resolved an issue with the Auto-Quarantine feature preventing the EventPro application user-interface from launching on a Windows device.
- Resolved an issue with the Agent sending duplicate Syslog events to the Console.
- Fixed an issue where the Agent could cause 32-bit Java applications to crash on Windows devices.
- Fixed Script Control to not block a Microsoft Windows 10 script.
- Fixed an issue where installing the Agent MSI package using the command line without including the installation token resulted in the Agent requiring an uninstall password and the Agent could not be uninstalled.
- Fixed an issue where a USB device was not being blocked upon first use on Windows XP and Windows Server 2003 devices when Device Control was enabled and set to Block.
- Fixed an issue with WMI errors occurring on Windows devices during startup and shutdown.
- Fixed an issue with Device Control events to generate a serial number when a USB mass storage device is disabled then enabled on a Windows device.
- Fixed duplication of Device Control events for iOS USB connection to a Windows device.
- Fixed duplication of Device Control events for Android USB connection to a Windows device.
- Fixed an issue with the event log on a Windows device to include the device serial number for iOS devices.
- Fixed an issue with the Application Control folder exclusions to prevent portable executable (PE) files from manually being moved on a Windows device.
- Fixed an issue that was causing threat files to be quarantined from a macOS Samba SMB mounted drive.
- Fixed an issue with the ability to recognize a trailing backslash in Application Control folder exclusions on a Windows device.
- Fixed an Application Control issue with the ability to copy a file from a non-excluded folder to an excluded folder on a Windows device.
- Fixed an issue with the Optics to only upload Windows logs that have not been uploaded before.
- Fixed an issue with the ability to downgrade the local cloud model on macOS devices.
- Fixed an issue with Device Control events to include the detection of USB floppy drives on Windows devices.
- Fixed an issue with duplicated Device Control events being generated when connecting a USB drive to a Windows device.
- Fixed an issue with the event log on a Windows device to include the device serial number when connecting a USB device to a VMware Workstation instance.
- Fixed an issue with the event log on a Windows device to include the device serial number for an Apple iPad.
- Fixed an issue with the event log on a Windows device to include the serial number for Canon cameras.
- Fixed an issue with scanning folders externally mounted to a macOS device, where the file is not local.
- Fixed an issue with the rate that the Agent checks the status of the cloud model when the Console communication is not responsive.
- Fixed an issue with the Visual Studio App Simulator from being blocked as an exploit on macOS devices.
- Fixed an issue with the timer to add a random buffer for checking in to the Console after a connection is re-established.
- Fixed a Windows issue where memory allocated to fields in DEVFLT_CONTEXT are not freed.
- Fixed an issue where the uploader repeats when the upload limit is reached.
- Updated the localization files to ensure translations work on OS X El Capitan.
- Fixed a Windows boot issue when the Console is unavailable.
- Fixed an issue with the macOS Sierra Beta build crashing the Agent UI.

Added 4/2017 - Resolved Technical Advisories v1.2.1411

The following issues are resolved in v1.2.1411, available when an organization is enrolled for Agent Auto Update on the Dell Server. For instructions on how to enroll, refer to *AdminHelp*, accessible from the Remote Management Console.

- Resolved a compatibility issue between Memory Protection and Windows 10 Credential Guard.
- Fixed an issue where Windows Security Center registration fails when installing the Agent via GPO
- Fixed an issue where files added to the Global Safelist were not properly waived by the Agent.
- Fixed an issue to ensure quarantined files remain quarantined, even if multiple copies of the file in question get copied to the computer.
- Fixed an issue where the ScriptCache folder was consuming too much disk space if Script Control for Office Macros was enabled. Office documents are no longer cached as part of ScriptCache; only ActiveScript and PowerShell scripts are cached.
- Fixed an issue to ensure that on-demand scans are using both the Local model as well as Cloud lookups, as with background scans.
- Resolved a compatibility issue between Memory Protection and Remote Desktop on Windows 8 computers.
- Fixed an issue where the Agent does not attempt to re-deliver device system information to the Management Console if the send operation times out.
- Fixed an issue to allow Script Control exceptions for web-based locations.
- Fixed an issue to ensure that the Background Threat Detection status is accurately reported.
- Fixed an issue where the Agent may not properly send the file hash to the Management Console, resulting in an error in the Management Console.
- Fixed an issue where the Agent does not properly register with the Management Console if the Agent is installed without network access.
- Resolved a compatibility issue between Memory Protection and Passport.
- Resolved a compatibility issue between Memory Protection and NVIDIA Nsight.
- Fixed an issue where Agents deleted from the Management Console would still attempt to connect to the Management Console to upload Agent logs.
- Resolved a compatibility issue between Memory Protection, Auto-Quarantine (AQT) and Novell Zenworks Logger.
- Fixed an issue where the Advanced Threat Protection service was not properly starting on devices using .NET 4 Client Profile.
- Fixed an issue where the Windows installation would not accept the Installation Token if the device is offline.
- Fixed an issue where the Windows OS version was incorrectly reported, causing issues with Zone Rules.
- Fixed an issue to ensure Auto-Update properly updates both the Agent and Optics.
- Resolved an issue where the Agent was snot updating Optics with the Device ID if Optics was installed prior to Agent registration with the Management Console.
- Fixed an issue to ensure that Local models are fully loaded before scanning files.
- Fixed an issue to ensure that USB devices encrypted with BitLocker can be accessed.
- Fixed an issue where Optics was not properly updating the product version number in Add/Remove Programs.
- Fixed an issue where the Windows theme would crash when the device starts.
- Fixed an issue where certain files paths were causing issues for Script Control exclusions.
- Resolved an issue in Windows 8 where Advanced Threat Prevention would appear as expired under certain circumstances.
- Fixed an issue where the macOS Agent and Windows installation would not accept the Installation Token if the device is offline.
- Fixed an issue where the macOS Agent blocked the Xcode debugger from running.
- Fixed an issue where the macOS Agents will repeatedly try to upload a file to the Management Console, even if the file is too large to upload.
- Fixed an issue where Watch For New Files was not properly working for long file paths on macOS systems.
- Fixed an issue where Memory Protection was not working properly on macOS computers.
- Resolved a compatibility issue with macOS Sierra and Time Machine on non-Apple network attached storage.
- Fixed an issue where Watch For New Files was incorrectly scanning mounted network drives on macOS computers.

Added 2/2017 - Resolved Technical Advisories v1.2.1401

The following issues are resolved in v1.2.1401, available when an organization is enrolled for Agent Auto Update on the Dell Server. For instructions on how to enroll, refer to *AdminHelp*, accessible from the Remote Management Console.

- Increased the detail available in the debug logs.
- Fixed an issue to properly waive files contained within archives.
- Fixed an issue where files whitelisted by certificate were incorrectly labeled as "catalog."

- Fixed an issue where a portable executable (PE) file was able to be copied onto a device with Application Control enabled.
- Fixed an issue where threats are blocked but not properly terminated (killed) in some OS X environments.
- Updated Memory Protection to include support for Metro Apps.
- Fixed an issue that caused a crash on the Windows Vista operating system.
- Fixed an issue where the user-interface notifications were not properly working for archived files.
- Fixed an issue with updating the Agent.
- Fixed an issue where Alternate Data Streams (ADS) filenames were not properly handled.
- Fixed an issue where some Memory Protection and Script Control events were not properly sent to the Console..
- Fixed an issue where the Agent UI would display erroneous text caused by the localization language folders not deploying correctly to the Cylance directory and being absent from the directory.

NOTE: Agent version 1401 supports Windows 10 Anniversary Edition but does not support Device Guard or Credential Guard, optional Windows 10 security features. If these features are enabled, disable them before using the Agent.

Resolved Technical Advisories v1.2.1391

The following issues are resolved in v1.2.1391, available when an organization is enrolled for Agent Auto Update on the Dell Server. For instructions on how to enroll, refer to *AdminHelp*, accessible from the Remote Management Console.

- Added support for detecting 32-bit PowerShell and Active Script processes on 64-bit operating systems.
- Fixed an Agent installation error when the Installation Token contains spaces.
- Reduced the frequency of WMI state logs in Not Verbose mode.
- Include archive files in the Daily Upload Limit and only log one upload limit exceeded message per day, once the threshold is met.
- Fixed an issue with Memory Protection incompatibilities with BeyondTrust PowerBroker and AppSense.
- Fixed an issue with Microsoft PowerPoint 2016 not launching on a Windows 10 system when Memory Protection is enabled.
- Fixed an issue with Citrix users unable to logon after installing Advanced Threat Prevention on a server.
- Addressed an issue where enabling Memory Protection on Windows Server 2012 with vShield resulted in a black screen on Remote Desktop (RDP) login/logout.
- Increased the details for Memory Protection events for Verbose logging.
- Fixed an issue where no event was reported to the Server for remote script execution.
- Addressed conflicts with the Luminex driver.
- Fixed an issue where enabling Memory Protection would cause a black screen to display when a user logged in to the device.
- Addressed an issue to handle a corrupt local Advanced Threat Prevention database gracefully.
- Fixed an issue to prevent file execution before the Advanced Threat Prevention service starts up and that renaming the installation directory cannot be used as a method to prevent Advanced Threat Prevention from starting.
- Fixed an issue with MiraCast Wi-Fi Direct on a Microsoft Windows 10 system running the Agent.
- Fixed an issue when removing a Logitech webcam from a system running the Agent.
- Fixed an issue with the Microsoft Windows 10 Anniversary Edition (build 1607) and the Agent.
- Increased the wait time for Advanced Threat Prevention services to stop during the update process.
- Addressed an issue where attaching Microsoft Word files to emails took longer than expected when Watch for New Files was enabled.
- Fixed an issue to properly report the Background Threat Detection status in the Agent UI and Console.
- Addressed an issue to better normalize file paths for Memory Protection.
- Improved the signature verification process.
- Fixed an issue where changing the Copy File Samples path in a policy in the Server would not update the path in the Agent.
- Fixed an issue where enabling Memory Protection would cause a black screen to display when a user logged in to the device

Added 4/2017 - Resolved Technical Advisories - Auto-Updates

For information about additional periodic Advanced Threat Prevention updates for enterprises enrolled for Agent Auto Update on the Dell Server, see http://www.dell.com/support/article/us/en/19/SLN305419/dell-data-protection-endpoint-security-suite-enterprise-and-dell-data-protection-threat-defense-release-notes?lang=EN. Select the **Saas Updates** tab.

For instructions on how to enroll for Agent Auto Update on the Dell Server, refer to *AdminHelp*, accessible from the Remote Management Console.

Encryption Client v8.11

- An issue is resolved that resulted in the Local Management Console appearing unresponsive while the Encryption client performed tasks in the background. [DDPC-2769]
- Slotted activation now proceeds as expected for users who change their passwords before activation. [DDPC-3279]
- The WSScan user interface now opens to the option of Unencrypted Files, as expected, when commands `-ua-`, `-ua`, and `-uav` are used to launch the user interface. [DDPC-3473]
- An issue is resolved that caused the Shield service to occasionally crash when the user logged out. [DDPC-3939]

Resolved Customer Issues

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

Preboot Authentication v8.11

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

Technical Advisories v1.2

Advanced Threat Prevention v1.2

- Added 8/2017 - The Advanced Threat Prevention tile displays Not Protected until the computer is restarted a second time. Occasionally, it is necessary to restart the DellMgmtAgent service. [CYL-435]

Encryption Client v8.11

- 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]
- In some cases, an encryption sweep pauses and the Local Management Console continues to display "Compliance in progress...." To restart encryption, copy WSProbe from the installation media, and run it: at the command line, enter `wsprobe`. [DDPC-4499]
- The user receives an access denied error when attempting to access removable media, although policy is set to allow full access to unShielded media. [DDPC-4523]
- After upgrade to Windows 10 Fall Update using WSProbe -E on a computer with Hardware Crypto Accelerator, during re-encryption with WSProbe -R, the Local Management Console freezes and a message displays regarding HCA key backup and provisioning. [DDPC-4645]
- The WSScan Unencrypted Files in Violation option to list Unencrypted Files option does not indicate that the files in violation should be encrypted. Using a previous version of WSScan will properly show these files. [DDPC-4790]

- Amended 2/2017 - Due to hibernation changes introduced in the Windows 10 Anniversary Update, computers will no longer be able to resume from hibernation when the Secure Windows Hibernation File policy is enforced. If you rely on secure hibernation, Dell recommends that you not upgrade to Anniversary Update at this time. This issue will be fixed in a future release. [DDPSUS-1346]

Advanced Authentication v8.11

- 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 v1.1.1

- A new Advanced Threat Protection Agent Auto Update feature is available and can be enabled from **Services Management** in the left pane of the Remote Management Console. Enabling Agent Auto Update allows clients to automatically download and apply updates from the Advanced Threat Protection server. Updates are released monthly.
- Advanced Threat Protection has Enhanced Script Controls for Powershell to mitigate against Powershell attack vectors. This feature is available for the Advanced Threat Protection client with build 1391, available in early October. To enable this feature on the client, either enable auto update or go to the FTP site to get the update to deploy.
- Advanced Threat Protection has Enhanced Script Controls to protect against malicious Microsoft Office macros. This feature is available for the Advanced Threat Protection client with build 1391, available in early October. To enable this feature on the client, either enable auto update or go to the FTP site to get the update to deploy.
- Advanced Threat Protection has enhanced “Memory Action: Exploitation” to protect against malicious payloads created using the Metasploit toolkit. This feature is available for the Advanced Threat Protection client with build 1391, available in early October. To enable this feature on the client, either enable auto update or go to the FTP site to get the update to deploy.
- The Encryption client now supports Microsoft Windows 10 Anniversary Update (Redstone release).
- Customers upgrading to Windows 10 from an earlier version of Windows OS are no longer required to decrypt and re-encrypt data at OS update.
- The Encryption client now supports Audit Mode. Audit Mode allows administrators to deploy the Encryption client as part of the corporate image, rather than using a third-party SCCM or similar solutions to deploy the Encryption client. To suppress activation until deployment is complete, install the Encryption client and perform the necessary restart when the configuration computer is in Audit Mode.
- A new policy allows the administrator to hide Encryption overlay icons in File Explorer for managed users.
- The Encryption client and BitLocker Manager are now supported with TPM 2.0.

Resolved Technical Advisories v1.1.1

Advanced Threat Protection v1.1.1

- If Endpoint Security Suite Enterprise is uninstalled and then reinstalled on the same computer, committing a policy change at the Dell Data Protection Server is no longer necessary for the endpoint to receive policies. [DDPC-1616, CSF-1305]

Encryption Client v8.10.1

- A timeout message logged during a failed activation has been modified to clarify the timeout period in milliseconds. [DDPC-2625]
- On computers running Windows 10 Education Edition, log files are now stored in \ProgramData\Dell\Dell Data Protection\Encryption as expected, rather than in \ProgramData\Application Data\Dell\Dell\Data Protection\Encryption\. [DDPC-2651]
- An issue that caused the computer to very rarely become unresponsive when renaming a file has been resolved. [DDPC-3086]
- An issue that caused a prompt to reboot in some cases with SDE encryption enabled is resolved. [DDPC-3525]
- If the activation prompt times out for a second or subsequent user on a computer with an activated user, the prompt now displays again. [DDPC-3705]
- UEFI computers with Secure Boot enabled now boot as expected after Microsoft Security Bulletin MS16-100 is applied. [DDPC-4032]
- Added 12/2016 - Hardening against credential update failures within the Encryption client is now enabled by default. [DDPC-936]

Preboot Authentication v8.10.1

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

Technical Advisories v1.1.1

Advanced Threat Protection v1.1.1

- No Technical Advisories exist.

Encryption Client v8.10.1

- The recovery file that is downloaded from the Dell Data Protection Server does not execute with the provided recovery image, and the following message displays: "The subsystem needed to support the image type is not present." [DDPC-2409]
- When migrating from one edition of Windows to a different edition during a Windows 10 upgrade, the Encryption client is not migrated. The same issue occurs if either the option to keep only personal files or to keep nothing is selected during a Windows 10 upgrade. To resolve this issue, reinstall the Encryption client after upgrade. [DDPC-4191]
- When WSProbe -z is run to prepare for the Windows 10 Anniversary Update on a computer with Dell Data Protection-encrypted data, an error may display that says an encryption sweep could not be stopped. To work around this issue, restart the computer and then re-run WSProbe -z. [DDPC-4254]
- Direct upgrade from v8.5.1 and earlier on 32-bit operating systems is not supported. To work around this issue, uninstall the previous version then install the latest version. [DDPC-4268]
- Aventail Access Manager is not supported with the Encryption client on Windows 10 computers. [DDPC-4335]

New Features and Functionality v1.1

- Amended 6/2017 - Dell Data Protection | Endpoint Security Suite Enterprise is now supported on the following server operating systems:
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
- Dell Data Protection | Server Encryption is now supported. Server Encryption provides remote management of servers, including the following:
  - Software encryption
  - Port control
  - Removable storage encryption
  - Support for maintenance scheduling, which allows control over enforcement of policies that require reboot
- Endpoint Security Suite Enterprise now includes an automatic client update feature. This feature automatically delivers the latest advanced threat prevention updates to clients, with the latest threat detection algorithms tested and approved by Dell, without requiring a new Endpoint Security Suite Enterprise release. This feature is disabled by default. To enable the automatic update feature, contact Dell ProSupport at 877-459-7304 Ext. 4310039.
- 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 Endpoint Security Suite Enterprise client version to support Hardware Crypto Accelerator functionality is v1.0.1. Support for v1.0.1 will continue through April 8, 2020.

Resolved Technical Advisories v1.1

Advanced Threat Protection v1.1

- After upgrade to Windows 10 and restart, the Enrollments and Password Manager tiles display as expected in the DDP Console. [DDPC-2322]
- An issue that caused a Windows 10 computer running the Encryption client to become unresponsive after restart is resolved. [DDPC-2336]
- After upgrade from a previous Endpoint Security Suite version the popup message, "The system information has been copied to the clipboard" from the **DDP Console system tray icon** > **About** > **Copy Info**, now closes when the user presses the **Enter** key to select **OK**. [DDPC-2394]
- An issue that cauased the DDP Console to become unresponsive due to an unhandled exception is resolved. [DDPC-3480]

Encryption Client v8.9.3

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

Advanced Authentication v8.10

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

Preboot Authentication v8.10

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

Technical Advisories v1.1

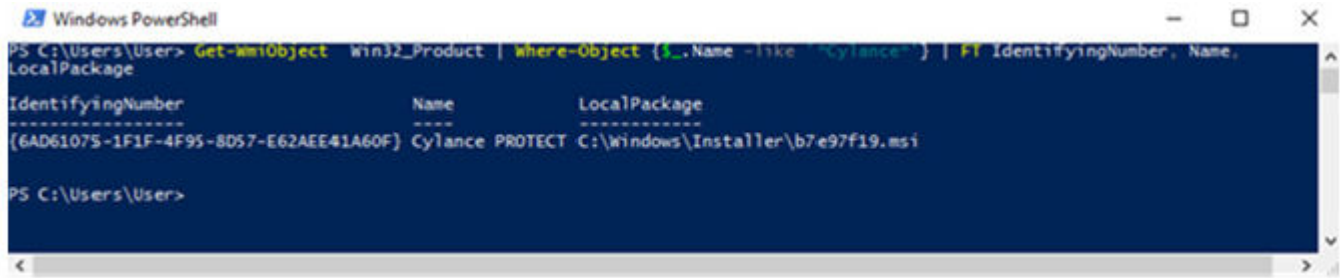
Advanced Threat Protection v1.1

- Policies display in the DDP Console Policies page only if they are enabled in the Remote Management Console. [DDPC-3545]
- Added 09/2016 - If the child installer is run a second time after installation is complete, Advanced Threat Protection is uninstalled. To work around this issue, run the master installer to repair an installation. [DDPC-4155]
- When upgrading to v1.1, the previous version must be uninstalled. Before upgrade, follow these instructions:

1 Ensure that the installation files for the currently installed client are stored in a safe location where they can be accessed after the upgrade.

2 Obtain the product code.

Enter the following Windows PowerShell command:



3 Run the v1.1 installer to upgrade the client.

For installation instructions, see the *Endpoint Security Suite Enterprise Advanced Installation Guide* or *Endpoint Security Suite Enterprise Basic Installation Guide*.

4 After upgrade, open a command prompt in the same location as the installation files that you stored in an accessible location in step 1, and enter the following command:

```
msiexec.exe /X {6AD61075-1F1F-4F95-8D57-E62AEE41A60F} /norestart
```

[CYL-249]

Encryption Client v8.9.3

- Standard practice is that the master installer version is the same version number as the Encryption client installer. However, in this release, the master installer is v8.10 and the Encryption installer is v8.9.3. Versions will be aligned in the future, to avoid confusion. In the event that you need support, ProSupport will need your **Encryption client** version number.
- To upgrade with HCA-encrypted data, issue a policy of Hardware Crypto Accelerator (HCA) = Off. After data is unencrypted, issue a policy of Policy-Based Encryption = On. Then run the v8.10/v8.9.3 installation. [DDPC-2608]
- Added 09/2016 - In the rare case that a user with smart card authentication becomes deactivated, smart card authentication succeeds for the first logon after restart for each user but fails on subsequent smart card logon attempts until at least one user restarts the computer. [DDPC-2721]
- After a computer crash or forced shutdown, encrypted files occasionally become unavailable. To work around this issue, run WSDeactivate then reactivate the Encryption client. [DDPC-3228]

SED Client v8.10

- Added 09/2016 - When PBA is activated on a Windows 7 computer without Microsoft Security Advisory 3033929 installed, the computer becomes unstable when resuming from sleep (S3). To work around this issue, install Microsoft Security Advisory 3033929 before installing the SED Client. If the SED Client is already installed, deactivate PBA and uninstall. After installing the Microsoft

Security Advisory, reinstall the SED Client. For more information, see https://technet.microsoft.com/en-us/library/security/3033929. [DDPC-4237]

Preboot Authentication v8.10

- Occasionally, the access code prompt displays rather than the Preboot Authentication login screen on computers with a wired network connection. [DDPC-3188]
- Added 09/2016 - When PBA is activated on a Windows 7 computer without Microsoft Security Advisory 3033929 installed, the computer becomes unstable when resuming from sleep (S3). To work around this issue, install Microsoft Security Advisory 3033929 before installing the SED Client. If the SED Client is already installed, deactivate PBA and uninstall. After installing the Microsoft Security Advisory, reinstall the SED Client. For more information, see https://technet.microsoft.com/en-us/library/security/3033929. [DDPC-4237]

Resolved Technical Advisories v1.0.1

All Clients

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

Advanced Threat Protection v1.0.1

- No Resolved Technical Advisories exist.

Encryption Client v8.9.1

- A Dell Data Protection-encrypted Windows 10 computer can now be upgraded to the Windows 10 Fall Update, after a few prerequisites are met. The prerequisites must be met, due to a change Microsoft has made to the Windows update process beginning with Windows 10. For more information, see Upgrade to the Windows 10 Anniversary Update. [DDPC-928, DDPC-1146, DDPC-1443]
- SDE key material download failures now result in a meaningful log entry, "Failed to validate key material bundle against the device." Erroneous validation failure warnings no longer display. [DDPC-960, DDPC-961]
- Corrected a misspelling of szRegValueLoginTimeout in the registry override variable and log message. [DDPC-966]
- The computer now boots as expected after Intel Rapid Storage Technology drivers are installed. [DDPC-1246]
- The HideOverlayIcons registry setting that is used to hide the encryption icons for all managed users on a computer after the original installation now works as expected. The HideOverlayIconsOverlay registry setting now effectively hides Dell Data Protection Encryption overlay icons when File Explorer is refreshed or reopened. [DDPC-1267, DDPC-1327]
- External Media Shield Explorer now launches properly after more than one incorrect password entry when accessing media that has been provisioned on a Mac. [DDPC-1273]
- A few WSProbe options have been deprecated to improve security. The WSProbe utility no longer supports the following options: -u (enable or disable Application Data Encryption), -x (exclude application from Application Data Encryption), and -i (revert an excluded application back to included in Application Data Encryption). [DDPC-1279]
- All characters of the 32-character Endpoint Code now fully display in the External Media Shield manual authentication dialog. [DDPC-1295]
- Excess logging of file-create operations no longer occurs. [DDPC-1339]
- An issue that caused excessive memory consumption has been resolved.[DDPC-1468]
- On a Windows computer, External Media Shield now successfully opens files and folders named with accented characters that are stored on external media and provisioned using a Mac computer. [DDPC-1517]
- When encryption models are changed (SDE to HCA) after an encryption sweep has completed, the computer no longer experiences a temporary blue screen. Previously, this occurred while key types were swapped, and allowing the computer to reboot typically restored functionality. [DDPC-1536]
- External Media Shield no longer displays Access Denied errors when the Windows Media Encryption and Windows Port Control policies are set to Off and Disabled. [DDPC-1572]

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

Advanced Authentication v8.9.1

- 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]

SED Client v8.9.1

- A non-administrator user can now run an application through User Account Control on a Windows 8, 8.1, or 10 computer with Security Tools installed. [CSF-1313, DDPC-1578]
- Volumes with Unicode strings in their serial numbers are now correctly reported in inventory. [DDPC-1899]
- Added 07/2016 - The following Dell computer models are supported with UEFI:

Dell Computer Models - UEFI Support

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

Preboot Authentication v8.9.1

- A non-administrator user can now run an application through User Account Control on a Windows 8, 8.1, or 10 computer with Security Tools installed. [CSF-1313, DDPC-1578]
- The issue that led to shutdown at PBA login on a computer running ActivClient v7.0.2 is resolved. [DDPC-1898]
- Volumes with Unicode strings in their serial numbers are now correctly reported in inventory. [DDPC-1899]

BitLocker Manager v8.9.1

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

Technical Advisories v1.0.1

Advanced Threat Protection v1.0.1

- Advanced Threat Protection cannot be upgraded in place from v1.0 to v1.0.1. To work around this issue, uninstall Advanced Threat Protection v1.0 and install Advanced Threat Protection v1.0.1:

1 Run the following command line to uninstall Advanced Threat Protection:

```
msiexec.exe /X {6AD61075-1F1F-4F95-8D57-E62AEE41A60F} /norestart
```

If uninstallation does not succeed, follow these steps:

a Enter the following powershell command to get the product code for the currently installed version:

```
Get-WmiObject win32_product | Where-object {$_.Name -like "*Cyl*"} | FT
IdentifyingNumber, Name, Version
```

The product code displays.

b From an administrative command prompt, run the following command:

```
Msiexec.exe /x <productcodehere> /norestart
```

2 Extract the Endpoint Security Suite Enterprise installer:

```
DDPSuite.exe /z"\"EXTRACT_INSTALLERS=C:\Extracted\""
```

3 Run the following at a command prompt:

```
AdvancedThreatProtection_x64.msi /qn REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1 /l*v "C:
\ProgramData\Dell\Dell Data Protection\Installer Logs\ATP.log" APPFOLDER="C:\Program Files
\Dell\Dell Data Protection\Advanced Threat Protection"
```

[DDPKM-871]

New Features and Functionality v1.0

Endpoint Security Suite Enterprise includes the following components:

- Advanced Threat Prevention provides real-time threat detection by analyzing potential file executions for malware in both the operating system and memory layers, to prevent the delivery of malicious payloads. Control of execution at the endpoint allows for accurate and effective detection of malicious threats - even those that have never been seen before. Advanced Threat Prevention uses machine learning techniques that allow detection of new malware, viruses, bots and unknown future variants, where signatures and sandboxes fail. Memory protection strengthens basic operating system protection features by providing an additional layer to detect and deny certain behaviors that are commonly used by exploits.
- The Dell Data Protection | Encryption client provides data-centric, policy-based protection of data on any device or external media, allowing enterprises to manage encryption policies for multiple endpoints and operating systems from the DDP Server. With the optional DDP | Hardware Crypto Accelerator, the Dell Data Protection | Encryption client offloads encryption processing to hardware for enhanced performance over software encryption and supports the highest level of FIPS 140-2 protection commercially available for system disks.
- Advanced Authentication fully integrates authentication options, including fingerprint, smart card, and contactless smart card readers, with Dell ControlVault for secure hardware credential processing. For added security, the Dell FIPS 140-2 compliant TPM is available on select Dell Latitude laptops and select Dell Precision mobile workstations.
- The SED client provides centralized, secure management of local and remote self-encrypting drives across an organization and seamlessly integrates with the other Endpoint Security Suite Enterprise components. All policy, authentication, management tasks, and storage and retrieval of encryption keys are available from the DDP Server, reducing the work of keeping critical data safe, and reducing the risk that systems are unprotected in the event of loss or attempts at unauthorized access.
- BitLocker Manager seamlessly integrates with the other Endpoint Security Suite Enterprise components through the DDP Server to provide flexible policy enforcement and TPM management, reducing the strain on an organization's IT resources. Reporting and auditing processes are simplified, with comprehensive protection and FIPS compliance. Extensive reporting and auditing capabilities and secure recovery key escrow help auditors easily determine compliance.

Technical Advisories v1.0

Advanced Threat Protection v1.0

- To avoid very long installation times due to Windows updates running on Windows 7, ensure that all updates are installed before beginning installation. If Windows KB2913763 is not yet installed, install it then reboot before installing Endpoint Security Suite Enterprise. For more information, see https://support.microsoft.com/en-us/kb/2913763. [CSF-847, DDPC-1619]
- After upgrade to Windows 10 with Advanced Threat Protection installed, the Advanced Threat Protection Service is not available. To work around this issue, either uninstall and reinstall Advanced Threat Protection or manually add the service with the appropriate command, listed below.

  If Advanced Threat Protection was installed with the Endpoint Security Suite master installer, use this command:

  sc create CylanceSvc binpath="C:\Program Files\Dell\Dell Data Protection\Advanced Threat protection\CylanceSvc.exe" start=auto displayname="Cylance PROTECT"

  If Advanced Threat Protection was installed with the child installer, use this command:

  sc create CylanceSvc binpath="C:\Program Files\Cylance\Desktop" start=auto displayname="Cylance PROTECT"

  [CSF-998, DDPC-3833]
- Before installation on a computer running Windows 7 and Microsoft .Net Framework 4.6, if all Windows updates have not been applied, the computer becomes unresponsive after installation. To work around this issue, ensure that all Windows updates are applied before beginning installation. [CSF-1158]
- Endpoint Security Suite Enterprise is not supported with PC Cleaner Pro. [CSF-1211]
- After a Quarantined file is Waived at the EE/VE Server and the Advanced Threat Protection client moves the file from Quarantined to Waived, the client does not send an event to the Server to indicate the file has been Waived. [CSF-1322]

Encryption Client v8.9

- Added 04/2016 - A computer running Windows 7 hibernates although the client is unable to encrypt the hibernation data and the Prevent Unsecured Hibernation policy is enabled. [DDPC-1220]
- The organization and naming of some policies differ in the local console and EE or VE Server Remote Management Console. [DDPC-1253]
- Added 8/2017 - When the user inserts EMS-encrypted media and clicks **Access Encrypted Files** on a Windows 10 computer without the Encryption client installed, the options **Install EMS Service** and **Run EMS Explorer** are not available. [DDPC-1449]
- On HCA-encrypted computers running the Windows 10 Fall Update, HCA decryption does not start after the HCA encryption policy is changed to Off. [DDPC-1452]
- On some USB drives, External Media Shield leaves some files unencrypted and renamed with "CEF????<original filename>ERR." This occurs only occasionally, with USB drives or drivers that repeatedly disconnect and reconnect the drives. To work around this issue, rename the files with their original filenames, then remove and reconnect the drive. If the EMS Scan External Media policy is On, the resulting encryption sweep will process the files. [DDPC-1532]
- If the HCA algorithm is changed after encryption, HCA encryption does not start. [DDPC-1533]

Advanced Authentication v8.9

- On UEFI computers running the Windows 10 Fall Update and AVG Antivirus, Advanced Authentication installation with the child installer is interrupted and never completes. [CSF-1192]
- The fingerprint reader on the Latitude 7510 running Windows 10 loses functionality after upgrade to Windows 10 Fall Update. To work around this issue, perform two restarts and the fingerprint reader will function again. [CSF-1210]
- Occasionally on computers running the Windows 10 Fall Update, fingerprints may need to be re-enrolled. [CSF-1225]

Preboot Authentication v8.9

- After recovering PBA access through recovery questions, the password change page displays a message that, if no action is taken, the user will be automatically logged in to the Windows session, although no automatic login occurs. [CSF-1083]
- Added 4/2017 - Login or recovery fails when a German keyboard is used to enter special characters into the password or recovery answer fields. [DDPC-5531]

Previous Technical Advisories

This section includes previous Technical Advisories for the Dell Data Protection | Encryption client, SED client, Advanced Authentication, and BitLocker Manager for releases of Enterprise Edition v7.0/7.0.1 - v8.7.1. Depending on the Endpoint Security Suite Enterprise deployment and operating systems of client computers, some issues are not applicable.

Technical Advisories v8.7.1

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

Technical Advisories v8.7

Encryption Client

- 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]
- 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]

Technical Advisories v8.6.1

No Technical Advisories were introduced in v8.6.1.

Technical Advisories v8.6

Encryption Client

- Added 09/2015 - In order to add new features, functionality, and the newest operating systems, Enterprise Edition for Windows will support Windows XP through Shield version 8.5.
- Added 08/2015 - If Microsoft TPM Base Services is improperly installed, the following functionality is affected: HCA provisioning, fingerprint enrollment in the DDP Console/Security Console, and BitLocker Manager operation. For more information and to work around this issue, refer to this KB article: http://www.dell.com/support/article/us/en/19/SLN296706. [CSF-454]
- If HCA policy is disabled or the HCA encryption algorithm is changed during encryption, the computer may experience a blue screen after reboot or at PBA logon. [DDPMTR-282]
- 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]
- Due to Microsoft's change in the way Windows handles stopping a critical service, stopping a DDP service such as CMGShield service, EMS service, or the Dell Data Protection | Encryption process in Task Manager will result in the computer experiencing a blue screen. [DDPMTR-945]
- In Windows 10, when using EMS Explorer to open a 5GB file on encrypted removable media an error displays, "The... file is too large for notepad," and the file does not open. [DDPMTR-990]
- When opening a file on encrypted removable media through EMS Explorer on a non-Shielded computer, if the removable media is removed without being ejected, the file remains in the computer's Ems Explorer Temporary Files folder in clear text after the file is closed. Properly ejecting the removable media properly removes these clear-text files. [DDPMTR-1157]
- After recovery of a computer running Windows 10 with HCA policy enabled, if HCA policy is then disabled the computer experiences a blue screen rather than decrypting as expected. [DDPMTR-1303]
- **Advanced Authentication**

  When a user begins credential enrollment but quits without saving before enrollment is complete, the credentials are enrolled rather than discarded. To work around this issue, if policy allows the user to modify their own credentials, the user can open the DDP Console, select the **Enrollments** tile, select and delete the credentials. Otherwise, an administrator must remove them. [CSF-146]
- Password Manager does not support the Windows 10 web browser, Microsoft Edge. [CSF-281]
- When running on Windows 10, the DDP Console About window displays incorrect BIOS information and an incorrect serial number for the computer's motherboard. [CSF-291, CSF-301]
- When a contactless smart card is moved across the card reader, a popup notification prompts the user to enroll the smart card. If the card is moved multiple times in a short length of time, multiple popup notifications may simultaneously display. [CSF-293]
- Amended 08/2015 - When using the child installer, no reboot automatically occurs, but a restart is necessary. The user must manually restart the computer or, to force a restart after installation, add /forcerestart to the installation command. [CSF-336]
- On Windows 10, if the Validity Fingerprint Sensor driver is out-of-date, when PBA is activated, the computer experiences a blue screen. To work around this issue, ensure that PBA is not enabled by policy, then follow these steps:

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

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

   [CSF-349]

- 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]
- When running Windows 10 on a computer with smart card authentication through PBA activated, after resuming from hybrid sleep, single sign-on fails. [DDPLP-308]
- To protect communications against the OpenSSL CVE-2014-3566 vulnerability, Dell Enterprise Server v8.5.1 and DDP Enterprise Server - Virtual Edition v9.0 and later are set to communicate using TLS, by default. However, Dell Data Protection | Encryption SED and HCA v8.6 clients communicate with Enterprise Server using SSL. This means that when running Enterprise Server v8.5.1 and later, Dell Data Protection | Encryption SED or HCA v8.6 clients with Preboot Authentication activated will fail to communicate with Enterprise Server. To work around this issue, refer to knowledge base article SLN296006 at http://www.dell.com/support/article/us/en/19/SLN296006. This workaround must be implemented as soon as possible, in order to prevent PBA client communication issues with Enterprise Server v8.5.1 or Virtual Edition v9.0 and later. [DDPUP-733, DDPMTR-1331]
- On Dell Latitude E7250, E7350, E7450, and Venue Pro 11 (Model 7139), recovery fails with Dell Opal SED Recovery Utility one-time unlock of the drive. To work around this issue, use the recovery key to unlock a drive on one of these models. [DDPUP-763]

Enterprise Edition for SED

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

BitLocker Manager

- Amended 08/2015 - When using the child installer, the installer will effect a reboot only if necessary. To force a restart after installation, add /forcerestart to the installation command. [CSF-246]
- Added 08/2015 - If Microsoft TPM Base Services is improperly installed, the following functionality is affected: HCA provisioning, fingerprint enrollment in the DDP Console/Security Console, and BitLocker Manager operation. For more information and to work around this issue, refer to this KB article: http://www.dell.com/support/article/us/en/19/SLN296706. [CSF-454]

Technical Advisories v8.5.1

No Technical Advisories were introduced in v8.5.1.

Technical Advisories v8.5

Encryption Client

- Pausing encryption is not reflected in the local console if the menu option "Process Encryption Only When Screen is Locked" is enabled. [DDPC-620]
- The computer does not single sign-on after resuming from Sleep-to-Hibernate. After the user enters their credentials at the Preboot Authentication (PBA) screen, the computer stops at the Windows logon screen and the user must manually log on to the computer. Dell Data Protection | Security Tools and the Dell Data Protection | Encryption client do not support Sleep-to-Hibernate and single sign-on. Disable Sleep-to-Hibernate when using Preboot Authentication if your organization intends to use single sign-on. [MMW-841]

Advanced Authentication

- Password Manager does not support Google Chrome v35 and later, due to a change in the way Chrome handles extensions. [MMW-619, MMW-754]
- Password Manager does not support importing credentials from Internet Explorer 10 and 11 (because the interface is not published by Microsoft). [MMW-770]

- On computers running ActivClient 7, single sign-on may not function properly. Also, multiple smart card icons may display in the Windows credential provider screen. [MMW-837]
- When Preboot Authentication is activated on a computer with more than one user and with only fingerprint authentication enabled, if two or more users enroll with the same fingerprint, at authentication for second and subsequent users an error message may display, "The fingerprint is not verified." However, the first user is able to authenticate successfully. [MMW-848]
- Eikon external fingerprint readers do not function properly on Windows 8.1 without the latest drivers. To work around this issue, when using an external fingerprint reader, download and install the latest drivers required for your specific reader. [MMW-880]

Preboot Authentication

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

SED Client

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

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

Technical Advisories v8.4.1

Encryption Client

- 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

- Fingerprint enrollment does not prevent the user from using fingerprints from different fingers when enrolling a single finger. [MMW-212, MMW-724]

Preboot Authentication

- Single Sign-on intermittently fails on computers with self-encrypting drives on which Preboot Authentication is activated. [DDPLP-144]
- When replacing a provisioned self-encrypting drive (with the Preboot Authentication environment active) with a *new* self-encrypting drive and provisioning the Preboot Authentication environment, after the new SED is provisioned, the old SED can no longer be recovered. [DDPLP-150, MMW-581]
- On the Dell Latitude Rugged Extreme, the user is able to detach the tablet from the dock. However, the dock is needed to log in through the PBA. Detach the tablet only after the PBA authentication step is complete. [DDPLP-162, DDPLP-163]
- UPN name is not supported by PBA. The correct usage would be to login with a non-UPN user name, domain\username, or enter the username independently and select the domain from the drop-down menu. [DDPLP-167, DDPC-80, MMW-591]
- After successfully authenticating to the Preboot Authentication environment, the computer will not complete Single Sign-on. Instead, the computer halts at the Windows Logon screen for another user. Microsoft Windows 8.1 defaults to the Logon screen for the previously authenticated user. To complete logon, return to the User Tiles screen by selecting the back arrow in the top right of the screen and then selecting the correct user tile for the user authenticated in the PBA. SSO data captured by the PBA may still be present and once the user tile is selected, Windows authentication may be completed automatically. [MMW-564]

Technical Advisories v8.3.2

Encryption Client

- Local options to manage the secondary drive are unavailable in the Dell Data Protection | Encryption console until after a policy change on that drive is applied and the computer is re-booted. [29046]
- PCIe SSDs are not supported on Precision T-series computers.

Technical Advisories v8.3

All Clients

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

Encryption Client

- Windows logon fails with some new CAC smart cards, which use multiple certificates with the same name. One certificate is the authentication certificate and the other is a signing certificate. The algorithm used to select the certificate uses the newest certificate. If the newest certificate is the signing certificate, Windows logon will fail. To work around this issue, create an Active Directory entry for the principle name for the signing certificate. [27857]
- During a command line uninstall, the installer will not download the encryption keys for the computer unless Silent mode is specified using the parameter CMGSILENTMODE=1. To work around this issue, specify CMGSILENTMODE=1 in the command. [27979]
- All registry keys and installation files are not removed after uninstallation. [28219]
- After uninstallation, logon with cached credentials occasionally fails when the computer is not connected to the network. During uninstallation, the cached credentials are decrypted. If this decryption fails for any reason, the user will not be able to login while disconnected from the network. To work around this issue, reconnect to the network and log on to cache the credentials. [28277]
- The encryption icon that indicates that a drive is encrypted does not display when a drive has been encrypted using HCA. [28400]
- During an attended (non-silent) upgrade from v8.1, the installer does not prompt the user to confirm that the upgrade is desired before continuing the installation. [28574]
- Preboot Authentication uses a "Basic" disk partition and cannot be converted to "Dynamic" partition (for RAID arrays). Attempts to convert the partition will result in the PBA not being created or the PBA not starting. [28587]
- After partial decryption recovery on a computer with an HCA card, the local Dell Data Protection | Encryption console may display duplicate information about local disks. To work around this issue, reboot the computer. After the restart, disk information displays properly. [28656]
- After installation of the Dell Data Protection | Encryption client, the Microsoft Usbccid Smartcard Reader is intermittently reported as being in a problem state in Device Manager. However, smart cards and fingerprints seem to function normally. Dell ControlVault relies on the Microsoft Usbccid drivers. A premier case has been opened with Microsoft regarding this issue. [28697]
- Decryption on computers with HCA cards removes Preboot Authentication, which must be reinstalled. At the next logon, both an Encryption Administrator Password prompt and a Security Tools shutdown message display. When the computer is shut down, PBA activation begins. However, provisioning will be completed only after a subsequent reboot and entry of the Encryption Administrator Password. [28722]
- Infrequently, after HCA policy is set, the Preboot Authentication screen does not display until the computer is restarted a second time. [28762]
- During Preboot Authentication activation, if the computer is not connected to the network with access to the Enterprise Server, the Dell Data Protection | Encryption client does not enforce required shutdown and Preboot Authentication activation is not completed. If the Dell Data Protection | Encryption client cannot access the Enterprise Server to back up encryption keys and other critical data, PBA activation is not completed and the required shutdown does not occur. To work around this issue, ensure that the computer has access to the Enterprise Server during the installation of the Dell Data Protection | Encryption client and policy deployment to back up encryption keys and other critical data, complete PBA activation, and enforce required shutdown. [28787/DDPC-37]
- 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]

- 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 the Dell Data Protection | Encryption client installed
  - HCA with Dell Data Protection | Security Tools and the Dell Data Protection | Encryption client 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 the Dell Data Protection | Encryption client installer remains on the computer. [28885]
- During an SDE encryption sweep, although the disk is only partially encrypted based on the progress of the sweep, the Security Console Encryption screen shows the disk as Protected. [28888]
- After a user is suspended in the Remote Management Console, the Shield ID is blank rather than indicating that the Shield is unmanaged. On the client computer, the Dell Data Protection | Encryption local console does not open properly. [28893]
- Fingerprints and smart cards stop working after the Port Control System policy to disable USB ports is applied. Broadcom USH hardware is a USB-attached device. When the policy to disable USB ports is applied, it prevents data transmission to and from the Broadcom USH hardware, which prevents users from logging on with fingerprints or smart cards. The problem can be resolved by applying a combination of policies that restrict access to USB external media by setting Windows Portable Device and External Storage Device class policy to Read Only. This policy combination allows the Broadcom USH hardware to function properly but prevents data from being transferred from the computer to external media such as USB flash drives and smart phones. [28895]

Advanced Authentication

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

1. In the Google Chrome Settings page, select **Make Google Chrome my default browser**.
2. Select **Show advanced settings** > **Content settings** > **Disable individual plug-ins** and then select **Always allowed** for the Dell Data Protection | Security Tools Plug-in. Close the Plug-ins page.

3 In the Google Chrome Settings page, select **Extensions** and check the Enable box next to the Dell Data Protection | Security Tools Extension.

4 Exit Google Chrome and re-launch.

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

[28528, 28678, 28719]

- In Password Manager, the Select Logon Data window does not show the user name of the first enrolled user. [28531]
- When using Password Manager with Firefox, double-clicking the pre-train icon does not open the Add Logon dialog. [28693]
- The Password Manager shortcut (CTRL+WIN+H) cannot be used on tablets, because the WIN button is not present. [28706]
- Password Manager prompts for credentials only when accessed for the first time after the user logs on and not again until the next log on or computer restart. This is working as designed. [28714]
- The Password Manager version number may differ across web browsers. [28808]
- In the Security Console, the Backup and Restore feature is described as providing data backup and restore functions but is specifically related to backup and restore of Password Manager data. [28856]
- When dual-factor authentication is enabled and the computer resumes from sleep, the computer intermittently stops responding and the screen is black. To recover from this situation press and hold the power button until the computer shuts down, then reboot the computer. [28900]

SED Client

- Windows logon fails with some new CAC smart cards, which use multiple certificates with the same name. One certificate is the authentication certificate and the other is a signing certificate. The algorithm used to select the certificate uses the newest certificate. If the newest certificate is the signing certificate, Windows logon will fail. To work around this issue, create an Active Directory entry for the principle name for the signing certificate. [27857]
- Preboot Authentication fails if a self-encrypting drive is configured as drive 1. To work around this issue, configure a self-encrypting drive as the boot drive (drive 0) for Preboot Authentication to function properly. [28266]
- Single Sign On does not function properly when cached credentials in UPN format are used. [28660]
- When Security Tools Authentication components are uninstalled, the user is not warned that Preboot Authentication is provisioned. Uninstalling Security Tools Authentication will impact only the user's ability to update credentials in the PBA but will not prevent the user from authenticating with existing user accounts. The proper uninstallation sequence is as follows:

  Deactivate the PBA

  Uninstall Security Framework (this also uninstalls the SED client)

  Uninstall Security Tools Authentication

  [28791]
- Attempting to upgrade from 8.0.0 or 8.0.1 to the latest release fails and an error message is displayed saying that the computer has not been modified. This issue occurs because the installer cannot deactivate the PBA and, therefore, uninstallation of the earlier version is blocked. To work around this issue, deactivate the PBA and reboot the computer before attempting to upgrade to the new version. [28817]
- The Dell Optiplex XE2 computer intermittently does not display the Windows logon or credential provider screen after waking from sleep. To work around this issue, upgrade to the latest applicable BIOS version, which is A05 as of 03/2014. In the BIOS screen, locate the option for Deep Sleep and disable it. [28862]
- Hybrid Sleep is not supported on Windows 8.1 with SED drives on the Precision M6800/M4800 platform. [28897]
- Secure Boot is a Unified Extensible Firmware Interface (UEFI) protocol that Windows 8 and 8.1 users can enable in the computer's BIOS to ensure that the computer boots using trusted firmware signed by the computer manufacturer. The feature is not supported when the following conditions are met:

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

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

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

  Instructions:

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

[28790]

Technical Advisories v8.2.1

Encryption Client

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

Advanced Authentication

- 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]
- 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]

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 Advanced Authentication installation, because smart card reader drivers are updated during installation. To work around the issue, unmount the smart card from the reader prior to installing Advanced Authentication. [27856]
- When using Microsoft Windows 8.1, Single Sign-On with Password Manager does not work with some email providers. [28259]
- 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.

Technical Advisories v8.1

Encryption Client

- 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]

SED Client

- 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 the SED client do not support Hybrid Sleep states and SSO when Preboot Authentication (PBA) is Active. Disable Hybrid Sleep when using Preboot Authentication if your organization intends to use SSO. [27496, 25785]
- When using a Precision M6800, Single Sign-On will fail if a USB device is currently plugged into the computer. [27595]
- With Windows 8, after a computer automatically moves from the sleep to hibernate state, when the computer resumes, Single Sign-On is not functioning properly. [27888]

Advanced Authentication

- The fingerprint reader on Latitude 10, Latitude 5530, and Latitude 5430 for OS logon does not work with Advanced Authentication.

BitLocker Manager

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

Technical Advisories v8.0

Encryption Client

- EMS cannot be used side-by-side with most third-party USB device encryption solutions, whether hardware or software. To use EMS, either add your third-party USB device to your whitelist, or remove the third-party encryption software.
- When the local console is left open and the computer sleeps, a message displays that "no fixed storage is found." Closing and re-opening the local console corrects the issue. If the local console cannot contact its internal server because the computer is sleeping, it correctly displays this message.
- Advanced Authentication cannot be installed when Dell Data Protection | Access is present on the computer. Follow the steps in the *Dell Data Protection | Endpoint Security Suite Administrator Guide* to uninstall DDP|A. [27073]
- When uninstalling the Dell Data Protection | Encryption client, 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]

SED Client

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

Advanced Authentication

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

Technical Advisories v7.7

Encryption Client

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

Technical Advisories v7.2.3

Encryption Client

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

BitLocker Manager

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

Technical Advisories v7.2.1

Encryption Client

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

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

Technical Advisories v7.2

Encryption Client

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

  Registry

  Profiles

  COM+ DB

  WFP.dll cache

  WMI DB

  IIS Metabase

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

Technical Advisories v7.0/7.0.1

Encryption Client

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

2

Workarounds

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

- To host EMS, external media must have 55 MB available, plus open space on the storage that is equal to the largest file to be encrypted. To work around the issue, free up space on the storage or use media with more storage capacity. [DDPC-243]
- Performing an upgrade during an encryption sweep may prevent the Shield Service from restarting normally after the installation finishes. A system restart corrects this issue. To work around the issue, we recommend upgrading when no encryption sweep is running. [14344]
- Encrypted data must be backed up while its owner is logged in. If encrypted files are backed up to an unencrypted location, the result is an unencrypted backup. To work around this issue, back up encrypted data while its owner is logged in. [3139, 11389, 12479]
- When Dell Data Protection | Encryption is installed, Guest accounts work properly, and Guest user account data is deleted at logoff, but Guest user account folder structures (located in the Windows user hives, normally Documents and Settings) may not be deleted at logoff. Because the data is deleted, the folder structures take up very little disk space. If this happens, you can work around the issue by having an administrator delete the excess folders periodically. [8900]
- If a user adds or removes smart card reader hardware without rebooting the Windows smart card, Dell Data Protection | Encryption may not properly recognize authentication. If this happens, the Dell Data Protection | Encryption prompts for alternate authentication. To work around this issue, reboot the Windows device. [9135]
- When one user attempts to access data encrypted for another user on a multi-user Windows device, the Windows software involved, including the operating system itself, may or may not handle this error condition gracefully. If this happens: 1) Review the *User Encrypted Folders* policy involved to see whether the folder should be moved to the *Common Encrypted Folders* policy. 2) See whether an upgrade for your third-party software is available.

3

Software and Hardware Compatibility

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

Upgrade to the Windows 10 Creators Update

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

Upgrade to Endpoint Security Suite Enterprise v1.4

IMPORTANT:

If you are upgrading Endpoint Security Suite Enterprise clients to Endpoint Security Suite Enterprise v1.4 and installing the new Client Firewall and Web Protection features, you must upgrade to Enterprise Server or VE v9.7 or later, then set the policy value of Memory Actions - Exclude Executable Files to the New Default Value shown below and push it to pre-v1.4 clients. Do not begin client upgrade before the new policy is enforced on the client.

For more information about setting policies, see *AdminHelp*, available in the Dell Server Remote Management Console.

After upgrade to Dell Server v9.7, enter the following exclusions as the policy value for Memory Action: Exclude executable files. Push the new policy to Endpoint Security Suite Enterprise clients before upgrade to Endpoint Security Suite Enterprise v1.4.

\Windows\System32\CmgShieldService.exe

\Windows\System32\EMSService.exe

\Program Files\Dell\Dell Data Protection\Threat Protection\DellAVAgent.exe

\Program Files\McAfee\Agent\cmdagent.exe

\Program Files\McAfee\Agent\FrmInst.exe

\Program Files\McAfee\Agent\macmnsvc.exe

\Program Files\McAfee\Agent\macompatsvc.exe

\Program Files\McAfee\Agent\maconfig.exe

\Program Files\McAfee\Agent\masvc.exe

\Program Files\McAfee\Agent\x86\FrmInst.exe

\Program Files\McAfee\Agent\x86\macompatsvc.exe

\Program Files\McAfee\Agent\x86\marepomirror.exe

\Program Files\McAfee\Agent\x86\McScanCheck.exe

\Program Files\McAfee\Agent\x86\McScript_InUse.exe

\Program Files\McAfee\Agent\x86\mctray_back.exe

\Program Files\McAfee\Agent\x86\Mue.exe

\Program Files\McAfee\Agent\x86\policyupgrade.exe

\Program Files\McAfee\Agent\x86\UpdaterUI.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\ESConfigTool.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\MFEConsole.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\mfeesp.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\mfeProvisionModeUtility.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\PwdUninstall.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\RepairCache\CCUninst.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\RepairCache\McAfee_Common_x64.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\RepairCache\McAfee_Common_x64.msi

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\RepairCache\McAfee_Common_x86.msi

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\RepairCache\setupCC.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\aacinfo.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\cacheinfo.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\fwinfo.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfecanary.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfefire.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfehidin.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfemms.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfevtps.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mmsinfo.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\vtpinfo.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\aacinfo.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\cacheinfo.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\fwinfo.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfecanary.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfefire.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfehidin.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfemms.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfevtps.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mmsinfo.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\vtpinfo.exe

\Program Files\McAfee\Endpoint Security\Firewall\FWInstCheck.exe

\Program Files\McAfee\Endpoint Security\Firewall\FwWindowsFirewallHandler.exe

\Program Files\McAfee\Endpoint Security\Firewall\mfefw.exe

\Program Files\McAfee\Endpoint Security\Firewall\RepairCache\McAfee_Firewall_x64.msi

\Program Files\McAfee\Endpoint Security\Firewall\RepairCache\McAfee_Firewall_x86.msi

\Program Files\McAfee\Endpoint Security\Firewall\RepairCache\setupFW.exe

\Program Files\McAfee\Endpoint Security\Web Control\McChHost.exe

\Program Files\McAfee\Endpoint Security\Web Control\mfewc.exe

\Program Files\McAfee\Endpoint Security\Web Control\mfewch.exe

\Program Files\McAfee\Endpoint Security\Web Control\mfewcui.exe

\Program Files\McAfee\Endpoint Security\Web Control\RepairCache\McAfee_Web_Control_x86.msi

\Program Files\McAfee\Endpoint Security\Web Control\RepairCache\setupWC.exe

\Program Files\McAfee\marepomirror.exe

\Program Files\McAfee\McScanCheck.exe

\Program Files\McAfee\McScript_InUse.exe

\Program Files\McAfee\mctray_back.exe

\Program Files\McAfee\Mue.exe

\Program Files\McAfee\policyupgrade.exe

\Program Files\McAfee\UpdaterUI.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\MaComServer.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\MFEConsole.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\mfeProvisionModeUtility.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\RepairCache\CCUninst.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\aacinfo.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\cacheinfo.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\fwinfo.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfecanary.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfefire.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfehidin.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfemms.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfevtps.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mmsinfo.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\vtpinfo.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\aacinfo.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\cacheinfo.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\fwinfo.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfecanary.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfefire.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfehidin.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfemms.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfevtps.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mmsinfo.exe

\Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\vtpinfo.exe

\Program Files (x86)\McAfee\Endpoint Security\Web Control\McChHost.exe

\Program Files (x86)\McAfee\Endpoint Security\Web Control\mfewc.exe

\Program Files (x86)\McAfee\Endpoint Security\Web Control\mfewch.exe

\Program Files (x86)\McAfee\Endpoint Security\Web Control\mfewcui.exe

\Program Files (x86)\McAfee\Endpoint Security\Web Control\RepairCache\McAfee_Web_Control_x64.msi

\Program Files (x86)\McAfee\Endpoint Security\Web Control\RepairCache\setupWC.exe

\Program Files (x86)\McAfee\Endpoint Security\Web Control\x64\mfewch.exe

\Windows\System32\mfevtps.exe

\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\LogDebugSetter.exe

\Program Files\McAfee\Endpoint Security\MfeUpgradeTool.exe

Aventail Access Manager

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

Windows Devices

- Whole-disk compression is not supported with the Encryption client.

Synaptics TouchPad

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

PartitionMagic

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

ePocrates Rx Pro

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

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

Hacks and Utilities

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