Dell Endpoint Security Suite Enterprise for Mac

Technical Advisories v2.0

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.

Endpoint Security Suite Enterprise for Mac Technical Advisories

2018 - 08

Rev. A01

Contents

1

Endpoint Security Suite Enterprise for Mac Technical Advisories

Endpoint Security Suite Enterprise for Mac offers advanced threat prevention at the operating system and memory layers and encryption, all centrally-managed from the Dell Server. 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.

- Endpoint Security Suite Enterprise - client software that provides Advanced Threat Prevention and Encryption
- Policy Proxy - used to distribute policies
- Security Server - used for client encryption software activations
- Dell Security Management Server/Security Management Server Virtual - provides centralized security policy administration, integrates with existing enterprise directories and creates audit logs and reports

  These Dell components interoperate seamlessly to provide a secure mobile environment without detracting from the user experience.

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.

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

Technical Advisories and Documentation

These Technical Advisories provide information about new client features and changes in each major release, any issues resolved from a prior release, and any Technical Advisories in the current release.

Should you need additional assistance administering this product, contact Dell ProSupport.

New Features and Functionality v2.0

- The Preference Panel lists the disk status for missing security tokens from the user when FileVault cannot be initiated. For more information on granting a security token to the user, follow procedures for Apple in: https://www.dell.com/support/article/us/en/04/sln309192/mobile-users-unable-to-activate-dell-encryption-enterprise-for-mac-on-macos-high-sierra?lang=en.
- macOS High Sierra 10.13.5 -10.13.6 are now supported
- Advanced Threat Prevention provisioning into geographical data centers for the Government Cloud is now supported.

Resolved Technical Advisories v2.0

Advanced Threat Prevention v2.0

- No resolved technical advisories exist.

Encryption Client v10.0

- No resolved technical advisories exist.

Technical Advisories v2.0

Advanced Threat Prevention v2.0

No technical advisories exist.

Encryption Client v10.0

- Apple has changed the management of Secure Tokens within macOS 10.13.0 and later. This may result in activation failures with "mobile users" or non-administrative users on macOS devices. This is not necessarily inherent to Dell Encryption, though may become more noticeable. These errors can cause repeat activation prompts, cause the primary volume to be noted as "Excluded" within the Dell Encryption Enterprise preferences panel, or even to have a direct failure when attempting to enable FileVault. To work around this, activate Dell Encryption Enterprise for Mac with an administrative account. For more information, please see: https://www.dell.com/support/article/us/en/04/sln309192/mobile-users-unable-to-activate-dell-encryption-enterprise-for-mac-on-macos-high-sierra?lang=en.
- Encryption fails on non-boot volumes on an iMac Pro with the selection of all fixed volumes and policy set to filevault encryption. [DDPMS-1807]
- In rare occurrences, to successfully eject a drive from the External Media tab in the preferences panel, the user must right-click and select **Eject** on the drive and then select **Eject** again after the drive is removed from the desktop. To work around this issue, the user can use Finder to eject the drive. [DDPMS-1846]

New Features and Functionality v1.5

- Encryption Client creates a hidden user to allow enforcement of policy with less user interaction on APFS FV2 volumes.
- Endpoint Security Suite Enterprise for Mac now supports IPv6.
- Encryption Client supports macOS High Sierra 10.13.4.
- Advanced Threat Prevention 1481 is supported with High Sierra 10.13.4.

Resolved Technical Advisories v1.5

Advanced Threat Prevention v1.5

- No resolved technical advisories exist.

Encryption Client v8.18

- APFS FileVault 2 is able to add users with v10.13.2 and above. [DDPMS-1659]
- The recovery tool allows customers to decrypt APFS volumes on macOS High Sierra 10.13.2. [DDPMS-1689]
- When a user enters the recovery key through the Disk Utility with FileVault recovery of *iMac Pro, it mounts the drive. [DDPMS-1709, DDPMS-1722]

Technical Advisories v1.5

Advanced Threat Prevention v1.5

Technical Advisories

No technical advisories.

Encryption Client v8.18

- Currently, after encrypting drives using FileVault Encryption and then selecting second option of "Accept New System Configuration" from the listed recovery options, the recovery fails. The workaround is to mount all drives first through Disk Utility or Recovery tool and then select "Accept New System Configuration ". Recovery fails if "Accept New System Configuration " is done without a mount. [DDPMS-1743]

New Features and Functionality v1.4.1

- Dell Encryption Enterprise supports macOS High Sierra 10.13.3.

Resolved Technical Advisories v1.4.1

Advanced Threat Prevention v1.4.1

- No resolved technical advisories.

Encryption Client v8.17.2

Resolved Customer Issues

- Dell Encryption Enterprise for Mac is supported on iMac Pro computer. [DDPMS-1709]

Technical Advisories v1.4.1

Advanced Threat Prevention v1.4

Technical Advisories

No Technical Advisories exist.

Encryption Client v8.17.2

No Technical Advisories exist.

New Features and Functionality v1.4

- Encryption client is compatible as a 64-bit application
- Inventory information sent to Dell Server is now encrypted.
- EMS Explorer indicates encrypted files with lock icon.
- Advanced Threat Prevention 1451 is supported with High Sierra 10.13.3.
- Advanced Threat Prevention 1451 has been integrated in Endpoint Security Suite Enterprise v1.4

Resolved Technical Advisories v1.4

Advanced Threat Prevention v1.4

- An issue where the Endpoint Security Suite Enterprise was not consuming the plist properly for command line install has been resolved. [DDPU-23]

Encryption Client v8.17

Resolved Customer Issues

- An issue where a dialog stated a System Extension was blocked while installing Dell Encryption on macOS High Sierra with SIP enabled has been resolved. [DDPMS-1490]
- An issue resulting when converting a managed drive that had been encrypted using FileVault to APFS and causing the drive to go to an unmanaged state has now been resolved. [DDPMS-1622]

Technical Advisories v1.4

Advanced Threat Prevention v1.4

No Technical Advisories exist.

Encryption Client v8.17

No Technical Advisories exist.

New Features and Functionality v1.3

- macOS High Sierra 10.13.1 is now supported.
- With macOS High Sierra, only FileVault encryption is supported, which Encryption Enterprise for Mac will manage. After an upgrade to v8.16 and then to High Sierra with the *Dell Volume Encryption* policy set to **On** and *Encrypt Using FileVault for Mac* set to **Off**, a policy conflict message displays on the Encryption client. The administrator must set both policies to **On**.
- Dell Encryption is only supported on macOS Sierra and earlier versions.
- System Integrity Protection (SIP) was hardened in macOS High Sierra (10.13.x) to require users to approve new third-party kernel extensions. For information on allowing kernel extensions on macOS High Sierra, see KB article SLN307814.

- Updated to Certified Agent Installer 1451.
- Dell Server policies support Global Exclusions for all threat types.

Technical Advisories v1.3

Advanced Threat Prevention v1.3

No technical advisories exist.

Encryption Client v8.16

- With Encryption External Media, if a user erases a drive and formats it to HFS+ or a variant of FAT, the user may not be prompted to provision and the Preference pane displays an error message. To work around this issue, the user can remove and then reinsert the media. [DDPMS-1121]
- On the Policies tab, after you enable Encryption External Media and FileVault 2 on a system drive and then add PBA users, the Ctrl + Option + Command does not display options. To work around this issue, close the Preferences pane and reopen the Policies tab. [DDPMS-1394]
- If an IPv6 address is used in either the installer pane or the .plist file, a symbolic or domain name address must be used to communicate with the Dell Server rather than a numeric address. [DDPMS-1405]
- With macOS High Sierra and Encryption External Media, some required resources for Dell Encryption must be allowed or a dialog regularly opens to remind the user. To work around this issue, the user must navigate to **System Preferences > Security and Privacy** and click **Allow** for the extension by Benjamin Fleischer (# 3T5GSNBU6W) or any other extension specified by their administrator. [DDPMS-1436, DDPMS-1500]
- If encryption is enabled and then disabled with the System Volume Only policy and FileVault 2, policy is not updated on the Encryption client. To work around this issue, reboot the computer if prompted. [DDPMS-1464]
- With High Sierra, HFS+, or FileVault 2, after logging in and activating a domain user through PBA, the Policies tab may omit some user information. Since this is not a local user ID, the user information is not available. [DDPMS-1477]

New Features and Functionality v1.2

- External Media Edition is rebranded to Encryption External Media (Access Encrypted Files.dmg).
- Enterprise Server is rebranded to Dell Security Management Server.
- Virtual Edition is rebranded to Dell Security Management Server Virtual.

Resolved Technical Advisories v1.2

Advanced Threat Prevention v1.2

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

Resolved Customer Issues

- Non-encrypted NTFS media can now successfully mount with Encryption External Media. [DDPSUS-1781]

Technical Advisories v1.2

Advanced Threat Prevention v1.2

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

- When the EMS Trust for Unsupported File Systems policy is set to Ignore, policy is not enforced on removable media. This is working as designed. To block unsupported file systems as unencrypted media, set the value of the EMS Trust for Unsupported File Systems policy to Provisioning Rejected. [DDPMS-1415]

New Features and Functionality v1.1

- Amended 6/2017 - macOS Sierra 10.12.4 and 10.12.5 are now supported.
- Policy signing is now available and can be enabled through the .plist DisablePolicySigningCheck key or with the Terminal utility, DellCSFConfigTool.
- New Server policies replace the need to manage some Encryption client settings through .plist entries.

  When upgrading to Dell Enterprise Server or VE v9.7, ensure that the following policies' values are correctly set. Policy settings override .plist file settings when policies are updated on the client.

  - FileVault 2 PBA User List (FV2PBAUsers in .plist)
  - FileVault 2 Policy Conflict Behavior (FV2PolicyConflict in .plist)
  - Firmware Password Mode (FirmwarePasswordMode in .plist)
  - No Auth User List (NoAuthenticateUsers in .plist)
  - Restrict Access To Unencrypted Media (AccessUnencryptedMediaRestriction in .plist)
  - Restricted user list for access to unencrypted media (AccessUnencryptedMediaRestrictionUsers in .plist)
  - EMS Trust for Unsupported File Systems(EMSTreatsUnsupportedFileSystemAs in .plist)
  - Delay Authentication (DelayAuthentication in .plist)
  - Max Password Delay (MaxPasswordDelay in .plist)

  For information about policies, see *AdminHelp*.
- Migration from Dell Volume Encryption to FileVault Encryption with an OS upgrade is now supported. For instructions, see the *Endpoint Security Suite Enterprise for Mac Administrator Guide*.

Resolved Technical Advisories v1.1

Advanced Threat Prevention v1.1

Resolved Customer Issues

- An issue is resolved that resulted in the client computer status, "Management disabled by policy." [DDPU-29]

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 v8.13.2

Following is a cumulative list of technical advisories that are resolved in Encryption client releases v8.11.1, v8.11.2, and v8.13, v8.13.1, and v8.13.2.

- Device Server has been renamed to Security Server in the .plist. [DDPMS-1226]
- For network users of Enterprise Edition for Mac v8.11.x with Mac OS El Capitain 10.11.6 and higher, EMS now displays and USB media can be mounted if the user chooses not to encrypt the drive when prompted. [DDPMS-1259, DDPMS-1260, DDPMS-1262]
- An error no longer displays when accessing Mac-provisioned removable media that was previously accessed on a Windows computer. [DDPMS-1296]
- An issue is resolved that caused the computer to become unresponsive during encryption or decryption of some Fusion drives. [DDPMS-1302]
- An issue is resolved that resulted in a rare activation failure on a computer with a Fusion drive. [DDPMS-1306]
- Added 6/2017 - EMS now launches as expected on macOS Sierra 10.12.5. Previously, Dell discovered through testing that Apple made changes to the disk utility in macOS Sierra 10.12.5 that were problematic when running EMS. This issue is resolved. [DDPMS-1410, DDPMS-1412, DDPSUS-1733, DDPSUS-1734]
- Added 6/2017 - Removable media now successfully mount with EMS. Previously, removable media did not mount after installation of macOS Sierra 10.12.5, Apple Security Update 2017-002 El Capitan, or Apple Security Update 2017-002 Yosemite. For more information about these updates, see https://support.apple.com/en-us/HT207797. [DDPMS-1414, DDPSUS-1752, DDPSUS-1755]

Resolved Customer Issues

- EMS recovery now proceeds as expected on the original encrypting computer when the EMS Automatic Authentication policy is disabled. [DDPMS-1331]

Technical Advisories v1.1

Advanced Threat Prevention v1.1

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

- Encryption does not begin after the client activates and receives Server policy. To work around this issue, click **Restart** or restart the computer. [DDPMS-1332]
- A restart is required for each drive on the computer when the Server policy, Volumes Targeted for Encryption, is changed from System Volume Only to All Fixed Volumes after the system drive is encrypted. [DDPMS-1384]
- With FileVault encryption, a policy update may result in an error, Invalid Element of Type. [DDPMS-1395]

New Features and Functionality v1.0

Endpoint Security Suite Enterprise for Mac 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.

  Advanced Threat Prevention is supported with Mac OS X Mavericks 10.9.5, Mac OS X Yosemite 10.10.5, and Mac OS X El Capitan 10.11.6.
- The 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 Dell Server.

Resolved Technical Advisories v1.0

Advanced Threat Prevention v1.0

Added 4/2017 - Resolved Technical Advisories v2.0.1421

The following issues are resolved in v1.0.1421, 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 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 v1.0.1411, 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.

- macOS Sierra Support
- Memory Protection enhancements
- 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 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 not 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 4/2017 - Resolved Technical Advisories v1.2.1401

The following issues are resolved in v1.0.1401, 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.

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.

Technical Advisories v1.0

Advanced Threat Prevention v1.0

- The Advanced Threat Prevention client installer does not prevent installation or inform the user of a conflict when other vendors' antivirus, antimalware, and antispyware applications are installed. However, Advanced Threat Prevention is not supported with other antivirus, antimalware, and antispyware applications. Uninstall other vendors' antivirus, antimalware, and antispyware applications before installing the Advanced Threat Prevention client to prevent installation failures. [DDPMS-1295]

Previous Technical Advisories

This section includes previous Technical Advisories for the Encryption client v7.7 - v8.11. Depending on the Endpoint Security Suite Enterprise deployment and operating systems of client computers, some issues are not applicable.

Technical Advisories v8.7

- Dell Encryption is not supported with System Integrity Protection (SIP), which Apple has introduced in Mac OS X El Capitan v10.11.0. To use Dell Encryption, SIP must be disabled. For instructions on how to disable SIP, see http://www.dell.com/support/Article/us/en/19/SLN299063.

Technical Advisories v8.6

No technical advisories exist.

Technical Advisories v8.4.0.6247

- Recovery of a FileVault-encrypted volume on Mac OS X Mavericks and later requires that Apple's procedure is followed to create and deploy recovery keys before FileVault is enabled on client computers. For more information, see http://support.apple.com/kb/HT5077?viewlocale=en_US&locale=en_US. [DDPMS-249]
- With FileVault encryption through the Encryption client on Mac OS X Yosemite 10.10 with an internal Apple SSD, the Security & Privacy - FileVault Tab may not display optimization progress although the Encryption client System Volumes Tab does display progress. To verify that optimization is in progress, enter the following command:

  diskutil cs list

Technical Advisories v8.1.3

- Amended 03/2014 - Since clients that encrypt using proprietary FDE will not function with hibernation enabled, Dell Data Protection turns off hibernation prior to encrypting the system drive. Starting with the Encryption client for Mac v8.1.1, the original hibernation setting is restored when the drive is decrypted, but the initial setting was not persisted in versions prior to v8.1.1. If this setting was turned off by a client prior to v8.1.1, Dell Data Protection cannot restore the setting when it decrypts the drive. [DDPMS-83, 14942]

Technical Advisories v8.1

- It has been observed on some Mac computers that setting the Workstation Scan Priority policy to Normal increases boot time. To work around this issue change the Workstation Scan Priority policy to Highest. [4585203]

Technical Advisories v8.0

- There are no Technical Advisories to report.

Technical Advisories v7.7

- Recovering a multi-volume system encrypted by FDE for Mac, requires that all encrypted volumes be recovered at the same time. [26056]
- When running v7.7 and Mac OS X Lion 10.7.5, ejecting EMS-provisioned external media without safely ejecting it causes kernel panic and possible loss of data. EMS-provisioned external media must be safely ejected to allow the EMS processes to complete. [26026]
- Hard drives with 4k block size (standard block size is 512 bytes) are not supported on Mac OS X Snow Leopard or earlier, due to a defect in the OS partition resize command. This defect has been fixed in Mac OS X Lion and later. [24726]
- Using Mac OS X Lion (32- or 64-bit/Standard or Admin User) and performing a copy operation of a large number of files (about 2000 in our tests) via Finder using EMS Service causes Finder to crash. [23752]
- On Mac hardware released prior to 2011, decrypting a drive that was encrypted by FDE for Mac will clear the firmware password, even if it was previously set by the user. [23673]
- Removable media inserted before authentication does not prompt for password. [22924]
- A Windows Blue Screen error may occur if you boot to a Windows Boot Camp partition while the client is decrypting a Mac partition. To work around this issue, wait until the decryption process is complete before booting to Windows. [21132]
- After a decryption sweep completes, if a computer restart is not performed or if the restart prompt is ignored prior to attempting to re-encrypt, the Encryption tab in the System Preferences Pane continues to display *Preparing volume for encryption* (even after multiple restarts). To correct the problem, issue a decryption policy, allow the sweep to complete, and restart the computer. After the computer restarts, re-initiate encryption. Note that the user is prompted to restart the computer after the decryption sweep. If the user delays the restart multiple times, a mandatory restart is performed, as specified in their policy settings. [21185]
- The Hostname field in the Compliance Reporter Device Detail report lists the encrypted Mac computer's *Unique ID* value instead of its hostname. [21134]
- At times, the Policy view in Dell Data Protection Preferences may become unresponsive when the client is configured to communicate with multiple Policy Proxies. To work around this issue, configure the client to communicate with only one Policy Proxy, as specified in the installer plist file, and leave the client policy entry for Policy Proxy hosts blank, as specified in the Dell Remote Management Console. [20624]
- The Dell Recovery Utility displays all visible volumes attached to the system when the *All* button is clicked. Volumes excluded from management will incorrectly show up as two volumes, one nested in the other, rather than a single volume. [15802]
- On rare occasions, the Dell Recovery Utility may become unresponsive when applying the *Accept New Configuration* recovery option. If this occurs, restart the Mac and re-attempt the recovery operation. [15947]
- On rare occasions, the *Accept New Configuration* recovery process may not complete after restart and the Mac may become unresponsive. If the login screen is not displayed after several minutes, restart the Mac. The client will automatically retry the recovery operation. [15947]
- Recovery operations can only be applied to one encrypted volume at a time. If a disk targeted for recovery contains multiple encrypted volumes, repeat the Dell Recovery Utility steps for each volume. [15325]
- The client uninstaller displays an incorrect error dialog if the user presses the Cancel button when prompted for their password. [15597]
- The Dell Data Protection System Preferences pane may show incorrect encryption status for another encrypted system volume attached to the computer. This occurs only if the other system volume was encrypted using a different computer. [15611]

2

Workarounds

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

- Modifying the system RAM configuration will invalidate the security protection profile of an encrypted volume. This will prevent the computer from booting on the following restart. To validate the new configuration and restore the bootability of the encrypted system volume, apply the *Accept new system configuration* operation in the Dell Recovery Utility. See the Online Help for instructions. [15665]
- When using Boot Camp on an encrypted Mac computer, and the computer is booted to Windows, the Mac OS X system volume is displayed as a separate drive letter in Windows Explorer. Since this volume is encrypted, Windows displays a dialog indicating it cannot open this volume.