Dell Encryption Enterprise for Mac

Technical Advisories v10.0

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.

Encryption Enterprise for Mac Technical Advisories

2018 - 08

Rev. A01

Contents

1

Encryption Enterprise for Mac Technical Advisories

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

- Encryption Enterprise - client encryption software that encrypts all data and enforces access control
- 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.

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

Contact Dell ProSupport

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

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

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.

For the most up-to-date list of supported Mac operating systems, see the following Knowledge Base article: http://www.dell.com/support/Article/us/en/19/SLN296718/EN

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

Encryption Enterprise for Mac New Features and Functionality v10.0

- 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

Encryption Enterprise for Mac Resolved Technical Advisories v10.0

Encryption Client v10.0

- No resolved technical advisories exist.

Encryption Enterprise for Mac Technical Advisories v10.0

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]

Encryption Enterprise for Mac New Features and Functionality v8.18

- Encryption Client creates a hidden user to allow enforcement of policy with less user interaction on APFS FV2 volumes.
- Encryption Client supports macOS High Sierra 10.13.4.

Encryption Enterprise for Mac Resolved Technical Advisories v8.18

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]

Encryption Enterprise for Mac Technical Advisories v8.18

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]

Encryption Enterprise for Mac New Features and Functionality v8.17.2

- macOS High Sierra 10.13.3 are now supported.

Encryption Enterprise for Mac Resolved Technical Advisories v8.17.2

Encryption Client v8.17.2

Resolved Customer Issues

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

Encryption Enterprise for Mac Technical Advisories v8.17.2

Encryption Client v8.17.2

No Technical Advisories exist.

Encryption Enterprise for Mac New Features and Functionality v8.17

- macOS High Sierra 10.13.3 is now supported.
- 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.

Encryption Enterprise for Mac Resolved Technical Advisories v8.17

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]

Encryption Enterprise for Mac Technical Advisories v8.17

Encryption Client v8.17

No Technical Advisories exist.

Encryption Enterprise for Mac New Features and Functionality v8.16.2

- macOS High Sierra 10.13.2 is now supported.

Encryption Enterprise for Mac Technical Advisories v8.16.2

Encryption Client v8.16.2

- Decrypt recovery is not supported with macOS High Sierra 10.13.2 and higher on Mac Encryption v8.16.2 and higher. [DDPMS-1689]
- An unmounted, encrypted APFS volume may impair Encryption client performance.

Encryption Enterprise for Mac New Features and Functionality v8.16

- 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.

Encryption Enterprise for Mac Technical Advisories v8.16

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]

Encryption Enterprise for Mac New Features and Functionality v8.15

- macOS Sierra 10.12.6 is now supported.
- Enterprise Edition is rebranded to Encryption Enterprise (Dell-Encryption-Enterprise.dmg).
- 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.

Encryption Enterprise for Mac Resolved Technical Advisories v8.15

Encryption Client v8.15

Resolved Customer Issues

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

Encryption Enterprise for Mac Technical Advisories v8.15

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]

Enterprise Edition for Mac New Features and Functionality v8.13.2

- Added 06/2017 - EMS is now supported with macOS Sierra 10.12.5.

Enterprise Edition for Mac Resolved Technical Advisories v8.13.2

Resolved Customer Issues

- 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]

Enterprise Edition for Mac New Features and Functionality v8.13.1

- Added 05/2017: Apple released macOS Sierra 10.12.5 on 05/15/17. Through testing, Dell discovered that Apple made changes to the disk utility that are problematic with this product. A fix was put in place to support macOS Sierra 10.12.5 when using Dell-Data-Protection-Mac-**8.13.1.65** (Dell-Data-Protection-Mac-8.13.0.64 should **not** be used). At this time Mac EMS v8.13.1, which is included in Dell-Data-Protection-Mac-8.13.1.65, is **not** supported with macOS Sierra 10.12.5. Organizations using Mac EMS should not upgrade to macOS Sierra 10.12.5.

Enterprise Edition for Mac New Features and Functionality v8.13

- New Server policies replace the need to manage some 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*.

Enterprise Edition for Mac Resolved Technical Advisories v8.13

Resolved Customer Issues

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

Enterprise Edition for Mac Technical Advisories 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]

Enterprise Edition for Mac New Features and Functionality v8.11.2

- macOS Sierra v10.12.3 and v10.12.4 are now supported.
- Administrators can modify the FV2PBAUsers key in the .plist file and then notify users to enable their FileVault account.

Enterprise Edition for Mac Resolved Technical Advisories v8.11.2

- Amended 4/2017 - Device Server has been renamed to Security Server in the .plist. [DDPMS-1226]
- Amended 4/2017 - An error no longer displays when accessing Mac-provisioned removable media that was previously accessed on a Windows computer. [DDPMS-1296]
- Amended 4/2017 - An issue is resolved that caused the computer to become unresponsive during encryption or decryption of some Fusion drives. [DDPMS-1302]

Enterprise Edition for Mac New Features and Functionality v8.11.1

- macOS Sierra v10.12.2 is now supported.
- If an enterprise wants to migrate from Dell Volume Encryption to FileVault Encryption and also upgrade the OS, the *Enterprise Edition for Mac Administrator Guide* provides steps for the migration process.

Enterprise Edition for Mac Resolved Technical Advisories v8.11.1

- 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]
- Amended 4/2017 - An issue is resolved that resulted in a rare activation failure on a computer with a Fusion drive. [DDPMS-1306]

Enterprise Edition for Mac New Features and Functionality v8.11

- macOS Sierra v10.12.0 and v10.12.1 are now supported.

Enterprise Edition for Mac New Features and Functionality v8.10

- Mac OS X El Capitan v10.11.5 and v10.11.6 are now supported.
- In the Remote Management Console, Mac policies have been reorganized to enhance usability:
  - The *Mac Encryption* technology group has two policy groups: *Dell Volume Encryption* and *Mac Global Settings*. The *Removable Media Encryption* technology group has *Mac Media Encryption*.
  - Master policies use On/Off instead of True/False. The *Encryption Enabled* master policy is renamed to *Dell Volume Encryption*.
  - Non-master policies that previously had True/False options are now a check box to select or clear.
  - Policies are divided into Basic and Advanced.
  - For the 8.10 release, in the Mac **Dell Data Protection > Policies** tab, the previous policy names and technology groups display, but the *Mac Shield Help* identifies the corresponding names.

Enterprise Edition for Mac Resolved Technical Advisories v8.10

- In the .plist, the HFS+ opt-in is disabled by default. If set to True, EMS will provision policy to HFS+ media. [DDPMS-142]
- With the Copy whitelist rule, the administrator can now exclude media from EMS based on media size and file system type (HFS+, ExFAT, or FAT). [DDPMS-1157, DDPMS-1158]

Enterprise Edition for Mac Resolved Technical Advisories v8.7.2

- Files with multi-byte accented characters are now compatible across Mac and Windows platforms with External Media Shield. [DDPMS-964]
- Recovery using the recovery keychain now proceeds as expected when the recovery file is stored on a volume with spaces in its name. [DDPMS-966]
- The recovery application now allows access to a fallback recovery keychain generated before the final UUID of an encrypted HFS+ volume is determined. [DDPMS-969]

Enterprise Edition for Mac New Features and Functionality v8.7.1

- Added 03/2016 - Mac OS X El Capitan v10.11.4 is now supported.

Enterprise Edition for Mac Resolved Technical Advisories v8.7.1

- The restart prompt now consistently displays on the client computer after Dell Encryption is enabled. [DDPMS-736]
- Improvements have been made to reported status in the System Preferences panel. [DDPMS-760, DDPMS-766, DDPMS-783, DDPMS-788, DDPMS-797, DDPMS-800, DDPMS-804, DDPMS-823, DDPMS-825]
- Unmanaged FileVault2 volumes are now indicated as Not Protected on the DDP Server, as expected, since their recovery keys are not available. Status of unmanaged FileVault2 volumes previously shown as Protected will change to Not Protected. [DDPMS-787, DDPMS-808, DDPMS-816, DDPMS-822]
- If a user declines DDP|E management of a FileVault-encrypted non-boot fixed volume on a computer with more than one non-boot fixed volume, the user is now prompted to accept management of each of the remaining system volumes. [DDPMS-789]
- Non-boot volumes are now FileVault-encrypted even though the boot volume has no recovery partition. If the boot volume is Core Storage, it will also be encrypted. [DDPMS-790]
- On a computer with multiple volumes including an external volume, FileVault encryption now proceeds as expected and status is accurately displayed on the System Volumes tab.[DDPMS-791]
- After FileVault encryption of multiple volumes, the DDP Server now displays the correct number of protected volumes. [DDPMS-792]
- The DDP Server now displays encryption sweep time stamps for endpoints with more than one Core Storage volume on the boot disk when both FileVault encryption and System Volume Only encryption are enabled. [DDPMS-806]
- When policy is changed to enable FileVault encryption, FileVault encryption now begins without requiring restart on managed endpoints that are running Mac OS X El Capitan 10.11.x. [DDPMS-812]
- After policy is changed to enable FileVault encryption, the necessary restart now occurs according to Restart Delay policies regardless whether a user is logged in. [DDPMS-817]
- When the Volumes Targeted for Encryption policy is changed from All Fixed Volumes to System Volume Only, the DDP Server now displays endpoints as Protected during decryption. [DDPMS-818]
- An issue has been resolved that occurred when Disk Utility made changes to a Dell-encrypted volume, in some circumstances rendering it unusable. Generally, this issue occurred with volumes on which a FAT partition resided between HFS+ or Core Storage partitions. [DDPMS-858]
- Added 02/2016 - The issue that led to continuous prompts for administrator credentials with FileVault encryption on Mac OS X Yosemite 10.10.5 is resolved. [DDPMS-897]
- Added 02/2016 - When pre-installation scripts cannot run, for example, when the installer is run directly from the .dmg file and permissions on /tmp are incorrect, a message now explains this. Previously, an installation log entry incorrectly indicated that the operating system is not supported, and the user received no indication that the scripts could not run. [DDPMS-899]
- Added 02/2016 - An issue that led to activation failure with a log entry, "Unknown canWrap failure," is resolved. [DDPMS-900]

Mac OS X El Capitan 10.11.0 In-Place Upgrade

On a computer running Dell Encryption, decryption must be performed prior to upgrade to Mac OS X El Capitan 10.11.0. When upgrading a computer with FV2 encryption, decryption before upgrade is not necessary.

Enterprise Edition for Mac New Features and Functionality v8.7

- Amended 01/2016 - Mac OS X El Capitan v10.11.0, v10.11.1, v10.11.2, and v10.11.3 are now supported.

Enterprise Edition for Mac Resolved Technical Advisories v8.7

- The endpoint hostname can now include Unicode characters. [DDPMS-669]
- Added 05/2018- The restart dialog displays following FileVault decryption of more than one volume. [DDPMS-707]

Enterprise Edition for Mac 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.

Enterprise Edition for Mac New Features and Functionality v8.6.1

- Amended 10/2015 - Mac OS X Yosemite v10.10.4 and 10.10.5 are now supported.

Enterprise Edition for Mac Resolved Technical Advisories v8.6.1

- Occasionally, the Security Server/Device Server can take longer than the default timeout period, resulting in activation timeout errors. A new plist entry has been added to provide greater flexibility in these cases, as follows:

  <key>ClientActivationTimeout</key>

  <integer>120</integer>[Range: 5 to 300, inclusive. The default value is 30. The time in seconds to give the Security Server/Device Server time to respond to an activation attempt before giving up. This plist value is valid for clients running v8.6.0.6627 or later.]

  [DDPMS-716]
- The issue of encryption not beginning while logged in as an AD_Domain user that is missing a mobile account locally is resolved. [DDPMS-717]
- Previously, encryption would never begin when enabling Dell full disk encryption on multiple partitions or volumes. This issue is resolved, and was only seen on OS X Yosemite. [DDPMS-734]
- All volumes are now properly encrypted when using FV2 and changing encryption from System Volume Only to All Volumes. [DDPMS-746]
- EMS now ignores all partitions that share physical media with the boot volume. [DDPMS-729]

Enterprise Edition for Mac Resolved Technical Advisories v8.6

- After the Encrypt Using FileVault for Mac policy is changed from True to False, the user is now prompted to allow decryption to begin, as expected. [DDPMS-621]
- When Mac OS Extended Media is connected to the computer and the EMS Encrypt External Media policy is set to False, the user is no longer notified that the media format is unsupported. [DDPMS-626]
- FileVault encryption is now performed on a CoreStorage boot volume without a restart. [DDPMS-631, DDPMS-633]
- FileVault encryption status now displays in Dell Data Protection Preferences, as expected. [DDPMS-632]
- A non-administrator user can now successfully mount and provision a USB volume. [DDPMS-662]

Enterprise Edition for Mac Technical Advisories v8.6

No technical advisories exist.

Enterprise Edition for Mac New Features and Functionality v8.5.0.6506

- Amended 06/2015 - Mac OS X Yosemite v10.10.2 and 10.10.3 are now supported.
- Enterprise Edition for Mac now supports FileVault encryption of unencrypted non-boot volumes as well as management of FileVault-encrypted non-boot volumes.
- Recovery keys can now be easily refreshed by obtaining the recovery bundle from the Dell Enterprise Server and dragging it onto the Dell Data Protection Preferences Pane.
- For ease in decryption and recovery of data that is FileVault-encrypted by policy, protection with institutional recovery keys can now be converted to protection with both institutional and personal recovery keys on computers running Mac OS X Mavericks 10.9.5 and later.

Enterprise Edition for Mac Resolved Technical Advisories v8.5.0.6506

- User interaction is no longer required during decryption of FileVault-encrypted data based on policy setting. [DDPMS-460]
- After a computer name is changed, only the latest hostname displays as an endpoint in the Dell Remote Management Console, and user activations and recovery options now proceed as expected on the computer. [DDPMS-476]
- On drives with a total number of sectors that is not divisible by eight, Enterprise Edition for Mac now functions as expected without requiring an extra reboot. [DDPMS-494]
- Several improvements have been made regarding status of a volume and its encryption/decryption in the Dell Data Protection Preferences Pane.

Enterprise Edition for Mac Resolved Technical Advisories v8.4.1.6310

- After Dell Recovery Utility is used to recover a Dell-encrypted disk, occasional activation failures no longer occur. Previously, activation failed on some computers due to a disk ownership issue based on the Mac OS setting, "Ignore ownership on this volume." Dell Recovery Utility now resolves this setting and disk ownership. [DDPMS-478]
- External media Shielded with Enterprise Edition for Mac 8.4.0.6247 is now compatible with Yosemite after use on a Windows computer running Enterprise Edition for Windows 8.4.1. [DDPMS-485]
- The encryption process no longer stops when it encounters large drives with nonstandard layouts. [DDPMS-494]

Enterprise Edition for Mac New Features and Functionality v8.4.0.6247

- Amended 11/2014 - Mac OS X Yosemite v10.10.0 and v10.10.1 are now supported without a preference file override.
- External Media Edition now provides the option to scan and encrypt files and folders on removable storage media each time the media is connected to the client computer. Also, a more detailed encryption status is available at the client computer.

Enterprise Edition for Mac Resolved Technical Advisories v8.4.0.6247

- External Media Edition stability is improved. [DDPMS-245, DDPMS-344]
- When FileVault encryption is enabled with a network account for which credentials are not locally cached, a message now informs the user that the account cannot use FileVault encryption without locally cached credentials. [DDPMS-312, DDPMS-331]

Enterprise Edition for Mac 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 Enterprise Edition on Mac OS X Yosemite 10.10 with an internal Apple SSD, the Security & Privacy - FileVault Tab may not display optimization progress although the Enterprise Edition System Volumes Tab does display progress. To verify that optimization is in progress, enter the following command:

  diskutil cs list

Enterprise Edition for Mac New Features and Functionality v8.1.3.6126

- Mac OS X Mavericks v10.9.5 is now supported without a preference file override.

Enterprise Edition for Mac New Features and Functionality v8.1.3.5902

- Mac OS X Mavericks v10.9.3 is now supported without a preference file override. An updated installation preference file (.plist) is included in the client package.
- Windows 8.1 Update 1 is now supported for accessing encrypted external media.

Enterprise Edition for Mac Resolved Technical Advisories v8.1.3.5902

- When a folder containing symbolic links is copied to a drive provisioned with External Media Shield (EMS), the copy operation is now successful. [DDPMS-122]
- The recovery extension now loads only when the Recovery utility runs a Mount or Accept new configuration operation on a volume encrypted with Dell full disk encryption. The recovery extension is no longer loaded for a FileVault encrypted volume. [DDPMS-150]
- The Enterprise Edition for Mac installer now supports the use of port 80 with Dell Policy Proxy. [DDPMS-212]
- When an external drive that is provisioned with EMS is used on a computer that does not have EMS installed, the Access EMS Get Info window now correctly displays the EMS build number. [DDPMS-228]
- EMS Explorer now allows multiple file operations to be simultaneously performed on a provisioned drive. [DDPMS-229]
- When booting from an OS X 10.9.2 recovery partition that uses FileVault 2 Recovery, updates to recovery scripts have corrected the recovery process. [DDPMS-236, DDPMS-249]
- Encrypted files stored on an external drive now open in EMS Explorer without errors, regardless of file size. [DDPMS-239]
- When EMS is enabled and an external drive is connected to the computer immediately after start up, EMS now correctly prompts the user to provision the drive rather than returning a file system error or changing external media files to read-only. [DDPMS-245]

Enterprise Edition for Mac New Features and Functionality v8.1.3.5821

Apple has announced that there is a security flaw in iOS and OS X 10.9.x. In iOS 6, iOS 7, and OS X 10.9, the security flaw could in some cases allow hackers to intercept communication sent using SSL/TSL security protocols. The flaw was patched by Apple in the OS X 10.9.2 update, released 02/25/2014, and iOS 6.1.6 and 7.0.6 updates, released 02/21/14.

For the Reuters report that explains the issue, see http://www.reuters.com/article/2014/02/22/us-apple-encryption-idUSBREA1L10220140222.

This flaw could potentially affect Enterprise Edition and Cloud Edition customers depending on how they have configured their OS X clients. In particular, activation of DDP iOS and Mac OS X clients running 10.9 over a DMZ (non-VPN) connection to DDP or CMG Servers could expose the authentication credentials of the activating user. Activations done over VPN and non-domain activations will not expose authentication credentials during activation. Dell recommends that customers with OS X or iOS clients take the following precautions:

1 Notify all DDP|EE OS X 10.9 users to immediately apply the 10.9.2 update.

2 Notify all iOS 6.x and 7.x users to update to the 6.1.6 and 7.0.6 versions immediately by selecting "Settings... General... Software Update" on their iOS device(s).

3 Enforce password change for any users that activated over non-VPN connection with a DDP OS X client between the release of 10.9 (10/22/13) and the date when the 10.9.2 update is applied to the computer.

4 Enforce password change for any users that authenticated with DDP | Cloud Edition iOS prior to patching their iOS devices, or Cloud Edition for Mac between the release of 10.9 and the date when the 10.9.2 update is applied to the computer.

5 Ensure that all OS X 10.9 devices have been activated and show as "Protected" in Compliance Reporter. Any OS X clients missing or not showing as Protected in Compliance Reporter should be considered unmanaged and should be investigated by IT Administrators to ensure that the endpoint has not been activated and encrypted with keys stored on an impersonated server.

Enterprise Edition for Mac Resolved Technical Advisories v8.1.3.5821

- Recovery of Fusion Drive and FileVault volumes is improved. [DDPMS-95, DDPMS-102, DDPMS-130]
- Improvements have been made to installation and upgrade procedures as well as to support of property list file overrides of allowed OSs. [DDPMS-125, DDPMS-144, DDPMS-151]
- Non-boot disk partitions can now be encrypted with Dell FDE encryption. [DDPMS-137]
- The Shield now maintains stability when a property list file is missing or renamed. [DDPMS-145]
- Installation and functioning on computers running OS X 10.9 or 10.9.1 is now prevented by the Enterprise Edition for Mac installer. [DDPMS-223, DDPMS-230]
- Enterprise Edition for Mac Shields with computer names containing the apostrophe character now properly activate. [DDPS-350]

Enterprise Edition for Mac New Features and Functionality v8.1.3

- Amended 03/2014 - Mac OS X Mavericks 10.9 is not supported.
- Fusion Drive support has been added.
- The new Client Tools feature offers the administrator the capability to remotely activate and examine a client. A client can be activated directly through a shell or through a script, using either Administrator credentials or temporary activation as the user without leaving evidence of the activation.
- Hibernation mode is restored upon decryption when using proprietary FDE.
- Mac OS X Mountain Lion v10.8.5 is now supported without a preference file override. An updated installation preference file (.plist) is included in the client package.

Enterprise Edition for Mac Resolved Technical Advisories v8.1.3

- Previously, client computers were not showing as Protected in the Remote Management Console after initial activation and encryption. To work around this issue, it was necessary to commit a minor policy change (such as Workstation Scan Priority), to reset the Protected flag. Once the flag was reset, the policy could be set back to its original value and recommitted. This issue has been resolved. [4586067]
- Enterprise Edition for Mac now handles the standby mode on newer computers, such as MacBook Air 6,2, on which default standby mode is set to 1 to prevent draining the battery while encrypted. [DDPMS-84; 9158-4587769]

- Added 03/2014 - Mac OS Safe Mode, as documented at http://support.apple.com/kb/HT1455, is now supported and issues that previously caused boot failure are now resolved. [DDPMS-60, 15664]

Enterprise Edition for Mac 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 Enterprise Edition 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]

Enterprise Edition for Mac New Features and Functionality v8.1

- Mac OS X Mountain Lion v10.8.4 is now supported without a preference file override. An updated installation preference file (.plist) is included in the client package.

Enterprise Edition for Mac 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]

Enterprise Edition for Mac New Features and Functionality v8.0

- Windows 8 Enterprise, Pro, and Windows 8 (Consumer) is now supported for accessing encrypted external media.
- exFAT format on flash drives is now supported for accessing external media encrypted by External Media Edition. exFAT (Extended File Allocation Table) is a Microsoft file system optimized for flash drives.
- The Dell Device Server default port number is now 8443. However, port number 8081 will still allow activations.

Enterprise Edition for Mac Resolved Technical Advisories v8.0

- Previously, when using FileVault encryption, the fields *Device Encryption Updating*, *Sweep Completed*, and **Protected** were not properly updating in the Remote Management Console. This issue has been resolved. [26799]

Enterprise Edition for Mac Technical Advisories v8.0

- There are no Technical Advisories to report.

Enterprise Edition for Mac 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.