Dell Security Management Server Virtual

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.**

Dell Security Management Server Virtual

2018 - 08

Rev. A01

Contents

1

Dell Security Management Server Virtual Technical Advisories

Dell Security Management Server Virtual is an all-in-one management solution that includes a management console, integrated database, and key management system. The Dell Server runs in a virtual environment and is targeted for the small or mid-sized enterprise with an existing VMware environment. Essentially, there is no difference between the features of Security Management Server and Security Management Server Virtual except that Security Management Server Virtual supports a maximum of 3,500 devices and has an internal database. Additionally, Security Management Server Virtual comes with a number of preset default policies and has an installation wizard that makes initial deployment much easier for small to mid-sized IT organizations.

Contact Dell ProSupport

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

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

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

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

New Features and Functionality v10.0

- Advanced Threat Prevention provisioning into geographical data centers for the Government Cloud is now supported.
- Additional maintenance tasks have been introduced to reduce the overall disk space used.

Resolved Technical Advisories v10.0

- BitLocker recovery keys are now sorted by date. [DDPS-6496]
- Advanced Threat Events are not properly populated within the Dell Compliance Reporter. [DDPS-6695]
- Advanced Threat Prevention email alert configuration is properly maintained on. [DDPS-6710]
- An issue resulting with an error message of "A data access error occurred" when accessing the Key Revocation tab from the external user management page with text in the search box has been resolved. [DDPS-6716]
- Emails now properly send at the scheduled time within the Dell Compliance Reporter. [DDPS-6770]
- Intermittent domain communication no longer results in users being removed from the Dell Security Management Server. [DDPS-6914]
- Resolved an issue with updates not correctly retaining the username for connections to audit event data. [DDPS-7036]
- Basic authentication is now functioning again within the Dell Security Management Server Virtual. [DDPS-7244]

Technical Advisories v10.0

- During the upgrade of the Security Management Server Virtual from v9.11 to v10.0 in connected mode, the installation window may become unresponsive, to continue the upgrade, the user must press Enter on the console. [DDPS-7166]
- Dell Security Management Server Virtual leverages typical linux repositories for pulling updates, due to known issues these may not always properly respond on IPv6, trying again later should result in a success in the update attempt. [DDPS-7351]

- Audit Events with pins per object counts close to 500 cause the management console to become unresponsive for some time. To work around this issue, modify the search scope to reduce the count below 500 consolidated events. [DDPS-7430]
- When a user navigates to the management console to make custom changes under Reporting > Audit Events , the changes are not saved if the user navigates away from the page. Navigating away and returning back to the Audit events page resets the values on the page. To work around this issue, create a managed report and save it. [DDPS-7445]
- The email audit event under Data Guardian's Advanced Details for open events shows the recipient email instead of sender email in From . [DDPCE-9846]

New Features and Functionality v9.11

- Starting with Dell Security Management Server Virtual 9.11.0, software updates will be pulled from a Dell-hosted Debian repository. Development OVA builds are configured to pull from the development Debian repository. Production OVA builds are configured to pull from the production Debian repository
- Operating system has been upgraded to Ubuntu 16.04.3 Long Term Support.
- Python interpreter used to drive the Administration Console has been upgraded to 3.5.2.
- PostgreSQL database system has been upgraded to 9.5.
- Virtualized Environments requirements have changed to the following minimum requirements:
  - Vmware hardware compatibility profile: Workstation 10.x
  - 2 CPU Cores
  - 8GB RAM
- Rebranding of Security Management Server Virtual with the following changes are now complete:

Product Name

DDP|E VE 9.10.0	*DSMSV 9.11.0*
Dell Data Protection | Virtual Edition Dell DDP Virtual Appliance	Dell Security Management Server Virtual
VE	V
dellddp (Used as the Debian package name)	dsmsv

Host Name

DDP|E VE 9.10.0	*DSMSV 9.11.0*
dellddp	dds

User Names

User names have been changed to shield the DSMSV code from future re-branding impacts.

DDP|E VE 9.10.0	*DSMSV 9.11.0*
ddpconsole	dellconsole
ddpuser	delluser
ddpsupport	dellsupport

- The following user interface changes have been made
  - Standardized color palette across all forms
    - Green - Selected form field of button.
    - Dark red - Form field which failed validation. Appears light red if the field is selected
  - Form header changes

    - All screens display product branding as the main title text. (i.e. top line)
    - All screens display a subtitle to denote the configuration category being modified.
    - Host name and IP address information have been relocated to the System Dashboard screen.
  - Form validation changes
    - Validation failure messages relocated under the associated field, similar to what the Management Console web interface does.
    - "OK" button disabled if any form field fails validation.
  - Introduced System Dashboard
    - Replaces the Server Status screen from VE < 9.10.0.
    - Includes server status and system information.
    - Includes 'Version History' widget that displays versioned database schema changes. Data comes from the 'information' table and is sorted by time, with newest version on top.
  - UI elements are now localized. Not just the EULA text.
  - Current time zone setting will be selected automatically when the form is displayed
  - Administrator Console has been added as a sub-menu under View Logs

Resolved Technical Advisories v9.11

- Added 08/2018- Dashboard notification of immediate threats now read "Advanced Threat Prevention". [DDPS-4995]
- Dell Security Management Server Virtual 9.11 is built with Workstation 10.x hardware compatibility. [DDPS-5085]
- Customer is now able to upgrade with a default non-standard JKS password when trying to do a server recovery. [DDPS-5854]
- Adding devices to an existing endpoint group no longer requires a policy change for the destination endpoint group [DDPS-6002]
- Endpoints screen now displays serial number based off the bios serial number WMI value. [DDPS-6161]
- ATP Widget is now displayed by default for Administrators who log in to the WebUI before ATP is provisioned . [DDPS-6268]
- An issue resulting when a user would decline the End User License Agreement while set to English, the language screen would not appear after a reboot to the machine has been resolved. [DDPS-6365]
- The Dell Virtual Server has applied the latest OS patches to protect against Meltdown and Spectre vulnerabilities. Further patching to the processor microcode, hypervisor, and host OS may also be required by following the manufacturers steps of these components. [DDPS-6253]

Technical Advisories v9.11

- Currently, there is no option to disable the IPv4 protocol on the Security Management Server Virtual. [DDPS-6447].
- Currently, the log files are being managed with the auto logrotate schedule, but the controls from the Security Management Server Virtual menu may not function in the ways the user might expect them to behave. [DDPS-6483]
- Currently, users are unable to receive policy updates when the encryption client is activated and IPV6 protocol is selected in the Security Management Server Virtual. The current workaround is to install a front-end proxy to receive policy updates with IPV6 selected. IPV4 and IPV6 cannot be used at the same time. [DDPS-6500]
- When a user double clicks the login button on the Dell Data Guardian Web Portal, the download page will open instead of the upload page. To work around this issue, open a new tab and navigate back to the primary web portal URL. [DDPS-6792]

New Features and Functionality v9.10

- The option to remove user sweeps from protected status calculation on the server has been added.

  To enable, the administrator must modify the InventoryObjects.config file which is located in < C:\Program Files\Dell\Enterprise Edition \Core Server\> by default.

  the section to change is :

  ```
  <object name="DeviceInventoryQueueProcessor" singleton="false"
  type="Credant.Inventory.Processor.DeviceInventoryQueueProcessor, Credant.Inventory.Processor" >

  <property name="EvaluateLastLoggedInUserForProtection" value="true"/>

  </object>
  ```

Changing the "true" value to "false" (this is not case sensitive) will require a restart of the core server service. Once the service has restarted the user sweep values are not calculated into the protected status for the device.

- Data Guardian has added the policies for protected office documents :
  - **Block Print Screen**: disables the user's ability to take screen captures via the Windows Print Screen capability while a Protected Office Document is open
  - **Protected Office Document Process Protection**: A comma separated list of EXE's that will be blocked from running while a Protected Office Document is open
- Web Portal Policies and their tool tips are localized.

Resolved Technical Advisories v9.10

- The "Enable Digital Signature Check" box in the WebUI now blocks the user from adding any text. [DDPS-5857]
- An issue that resulted in an error message during installation of Security Management Server with TLS 1.0 and TLS 1.1 disabled on the target SQL has been resolved. [DDPS-5982]
- Resolved an issue with the Dell Security Management Server Virtual would stop responding to requests to the server. [DDPS-6155,DDPS-6199]
- Resolved an issue where the Dell Security Management Server Virtual's WebUI would fail based to display policy data. [DDPS-6164]

Resolved Customer Issues

- The database console does not accept invalid characters such as " ' " or " / ", etc. [DDPS-6102]

Technical Advisories v9.10

- Security Management Server Virtual may crash when pulling a high volume of keys in a short time-span. [DDPS-6193]

New Features and Functionality v9.9

- Uncommitted changes are now displayed in badge icon in the top left of the Remote Management Console.
- Widgets are now available in the Dell Server. In the top right of the Dashboard, the following options can be added or removed with the Widgets menu:
  - Notifications
  - Protections Status
  - Threat
  - Protection History
  - Inventory History
  - Summary Statistics
- The encryption technology in use now displays in the Protection Status tab of the Endpoint Details and Actions page.
- The Dell Server now supports IPV6.
- A Policy column has been added to **Manage Reports > Log Analyzer** which displays administrator actions related to Policy.
- License Management now uses the following definitions for license usage:
  - **Overage** - Over license count maximum. Activation of new endpoints will fail. Re-activation of clients will fail. Existing clients will function normally.
  - **Warning** - License count nearing limit. Activation of new endpoints will persist until 105% of maximum. Consider purchasing additional licenses.
  - **OK** - No action needed. Activation of new endpoints will persist until 105% of maximum. [DDPS-2115]
- 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 Dell Server now supports TLS 1.2.

Resolved Technical Advisories v9.9

- The IP Exclusions for the Web Protection field in the Remote Management Console now only accepts valid formats. [DDPS-2206]
- If browser cookies are not enabled, the message "Cookies must be enabled on your browser to use this application" now displays at logon to the Remote Management Console. [DDPS-2661]
- A notification for a successful bulletin pull will now appear for the first successful bulletin pull after a bulletin pull failure. [DDPS-4811]
- Precedence changes for Endpoint Groups and User Groups are now displayed in the Log Analyzer. [DDPS-5024]
- AdminHelp and Compliance Reporter Help have been updated with Administrator Roles changes. The System role is marked as being able to "Manage Data Guardian external user key requests". [DDPS-5392, DDPS-5562, DDPS-5563]
- Duplicate Data Guardian key revocation requests involving the same file and user are displayed correctly in the Remote Management Console Key Revocation table. [DDPS-5570]
- The Device ID on the Enterprise-level Threat Events tab is now hyperlinked to its Endpoint Detail page in the Remote Management Console. [DDPS-5571]
- Logs now display the group name of a removed Admin-Defined User Group in Log Analyzer in the Remote Management Console. Logs are now generated when an Admin-Defined Endpoint Group is modified. [DDPS-5564, DDPS-5565]
- When running Log Details in Compliance Reporter, logs now show Username details as expected. [DDPS-5584]
- Logs are now generated as expected when an Approve or Deny file access request is issued. [DDPS-5589]
- The Dell Server now overwrites the values for "Set Proxy Settings" in the restore process. [DDPS-5635, DDPS-1547]
- Endpoints can now be exported as expected in Excel or CSV format. [DDPS-5825, DDPS-5826]

Resolved Customer Issues

- An issue that resulted in the Advanced Threats tab failing to load is resolved. [DDPS-5025]
- Compliance Reporter now shows the hostname of endpoints activated with Opt-in parameters. [DDPS-5527]
- Encryption External Media reports now show user information. [DDPS-5576]
- Japanese translations for city and state are now display correctly in the setup wizard. [DDPS-5595]
- Recovery keys now download as expected for a hostname containing Unicode. [DDPS-5614]
- The appropriate number of licenses are now consumed when Endpoint Security Suite Enterprise is installed with Client Firewall and Web Protection features. [DDPS-5673]
- Files exported as CSV from the Advanced Threat Events tab now display the correct time stamp. [DDPS-5732]
- When using an unauthenticated SMTP connection, the Server Configuration Tool no longer requires a username or password. [DDPS-5785]
- The Security Management Server Virtual now displays password requirements when creating the database password. The password parameters are as follows: Password must be at least 8 characters and must have at least 1 digit, 1 lowercase letter, one uppercase letter, 1 special character in ! @ # $ % & _ -. [DDPS-5808]
- An issue has been resolved that resulted in an internal error when accented characters were entered in the commit field. [DDPS-5805]

Technical Advisories v9.9

- Added 02/2018- Upgrades to Dell Security Management Server Virtual to 9.9.2 are now blocked for server versions prior to Dell Data Protection | Encryption Enterprise Server version 9.4.1 . Anything from 9.4.1 can upgrade to the latest generally available version. [DDPS-6254]
- When setting a Firewall Rule and defining an executable within that rule, the MD5 checksum value does not validate the syntax. Ensure that the MD5 entry is properly set before finalizing the addition of an executable. [DDPS-5858]

New Features and Functionality v9.8

- Security Management Server Virtual now supports the Data Guardian web client. Based on policy, internal and external users can view and edit protected Office documents and .xen files, with Print Control, Block Copy, and Embargo features, without installing the full Data Guardian client on their computers. The administrator runs a quick installation to set up a virtual machine that hosts the web client and communicates with the Dell Server.
- An administrator can revoke Data Guardian keys for individual files shared with an external user, on either the External User Management page or the Audit Events page, and can now blacklist an external user from the Audit Events page.

- Policy allows Data Guardian Windows and Mobile to apply an onscreen watermark to protected Office documents and PDFs. The watermark identifies the user and is displayed when the document is printed or shared.
- Advanced Threat Prevention and Data Guardian endpoints now show to have Protected status on the Endpoints page when their agents report their plugins' status as Functional. Plugin Status is displayed on the Providers tab of the Endpoint Details & Actions page.
- Advanced Threat Prevention audit events can now be exported to a SIEM/syslog server and to a local file from **Management** > **Services Management** in both connected and disconnected mode.
- Advanced Threat Event notification emails now include hyperlinks to additional detail about each category of event (Critical, High, Medium, Low, and Total).
- A new Web Protection policy allows administrators to block more than 100 specific categories of information.
- Administrators can now bulk upload and import a CSV list of Users to add to Admin-Defined User Groups. User Group priority can now be modified using drag-and-drop functionality.
- The License Management page now displays On the Box Licenses Collected, with the relevant Service Tags.
- Pre-Boot Authentication policies now display in the Authentication Technology Group on the Security Policies tab. A new policy allows the administrator to enable or disable users' ability to select **Remember Me** on the PBA login screen.
- As of v9.8, the ESXi vSphere thick client can no longer be used for deployment.
- The Remote Wipe command to remove a Dropbox for Business user has been deprecated. Administrators may use the Dropbox for Business function to remove users.
- Hardware Crypto Accelerator and Mobile Edition are no longer supported. Their policies have been deprecated.
- Virtual Edition is rebranded to Security Management Server Virtual.

Resolved Technical Advisories v9.8

- An error now displays when an invalid domain address is entered for DNS blocking in Threat Prevention Client Firewall settings. [DDPS-3201]
- Connection types are now validated; the executables table now displays the value entered for Signature and the correct column name for Fingerprint; and a network name is now required for specifying network protocol, when adding a Threat Prevention Client Firewall custom rule. EtherType and custom EtherType values (for non-IP network protocol) and transport protocol values display after a Firewall rule is saved. Duplicate rules must now be saved with unique rule names. [DDPS-3429, DDPS-3678, DDPS-3679, DDPS-3725, DDPS-3726, DDPS-3727, DDPS-5196]
- The administrator role change confirmation prompt now shows the correct user name after a user's administrative roles are modified, and the prompt now displays for changes made from the User Details Admin tab. [DDPS-4097, DDPS-4099]
- An external user no longer must reactivate Data Guardian after being removed from the Full Access List. [DDPS-5021]
- Log Analyzer logs are now generated when notification email addresses are added or edited in Notification Management. [DDPS-5063]
- Audit event exports to the SIEM/syslog server are now resent if a transmission error occurs during the initial export attempt. [DDPS-5132]
- Active Directory contacts' Data Guardian registration now succeeds, and the prompt for a domain password no longer displays during registration. [DDPS-5160, DDPS-5164, DDPS-5168]
- Formatting requirements for the following Advanced Threat Prevention policies are now included in Dell Server tooltips and AdminHelp: Memory Actions - Exclude executable files, Script Control - Approve Scripts in Folders (and Subfolders), and Protection Settings - Exclude Specific Folders (includes subfolders). AdminHelp now correctly indicates that the Help Desk and Security Administrator roles can download recovery key bundles. [DDPS-5184, DDPS-5287]
- Hyperlinks in Advanced Threat Prevention notifications now function properly when one or more endpoints are activated against a Dell Server with the host property set to the front-end Server host. [DDPS-5188]
- The "Certificate" type is now populated in the Type of Notification column of the All Notification Report in Compliance Reporter. [DDPS-5217]
- Audit events can be exported to a SIEM/syslog server with TLS/SSL over TCP, with the following configuration changes:

  To use TLS/SSL, the syslog server must be configured to listen for TLS/SSL messages. The root certificate used for the syslog server configuration must be added to the Dell Server Java keystore.

  The following example shows necessary configurations for a Splunk server with default certificates. Configurations are specific to individual environments. Property values vary when using non-default certificates.

  a Configure the Splunk server to use the Splunk Server certificate and root certificate to listen on TCP for TLS/SSL messages:

  $SPLUNK_HOME\etc\system\local\inputs.conf

  ```
  [tcp-ssl:<port number>]
  ```

```
disabled = 0

[SSL]

serverCert = $SPLUNK_HOME\etc\auth\server.pem

sslPassword = <password>

requireClientCert = false
```

$SPLUNK_HOME\etc\system\local\server.conf

```
[sslConfig]

sslRootCAPath = $SPLUNK_HOME\etc\auth\cacert.pem

sslPassword = <password>
```

b Restart the Splunk server.

After the restart, **splunkd.log** will have entries similar to the following:

```
07-10-2017 16:27:02.646 -0500 INFO TcpInputConfig - IPv4 port 5540 is reserved for raw input (SSL)

07-10-2017 16:27:02.646 -0500 INFO TcpInputConfig - IPv4 port 5540 will negotiate new-s2s protocol

07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig - IPv4 port 5540 is reserved for raw input (SSL)

07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig - IPv4 port 5540 will negotiate new-s2s protocol

07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig - IPv4 port 9997 is reserved for splunk 2 splunk

07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig - IPv4 port 9997 will negotiate new-s2s protocol

07-10-2017 16:27:02.653 -0500 INFO TcpInputProc - Creating raw Acceptor for IPv4 port 5540 with SSL

07-10-2017 16:27:02.653 -0500 INFO TcpInputProc - Creating raw Acceptor for IPv4 port 5541 with Non-SSL

07-10-2017 16:27:02.654 -0500 INFO TcpInputProc - Creating fwd data Acceptor for IPv4 port 9997 with Non-SSL
```

c Configure the Dell Server to communicate with the Splunk server and export audit events.

Use the keytool command to add the Splunk server's root certificate (cacert.pem) to the Dell Server operating system Java keystore. The certificate is added to the operating system Java keystore and not to the Dell Server application Java keystore.

```
keytool -keystore <keystore_location> -alias <alias-name> -importcert -file
<certificate_file>
```

For Security Management Server - Add the Splunk server's root certificate (cacert.pem) to the Java keystore, which in Windows is usually located in this path: C:\Program Files\Dell\Java Runtime\jre1.8\lib\security\cacerts

For Security Management Server Virtual - Add the Splunk server's root certificate (cacert.pem) to /etc/ssl/certs/java/cacerts and restart the Dell Server.

d Modify the Dell Server database to change the SSL value from **false** to **true**.

In the database, navigate to the information table, SIEM-specific support configuration.

Change the "SSL":"false" value to "SSL":"true" - for example:

```
{"eventsExport":{"exportToLocalFile":{"enabled":"false","fileLocation":"./logs/siem/audit-
export.log"},"exportToSyslog":
```

```
{"enabled":"true","protocol":"TCP","SSL":"true","host":"yourDellServer.yourdomain.com","po
rt":"5540"}}}
```

[DDPS-5234]

Resolved Customer Issues

- Custom ipWhitelist values are now retained in **/opt/dell/server/security-server/conf/webdefault.xml** after upgrade. [DDPS-5075]
- Attempts to re-register a Data Guardian user that is already registered now fail with a messages that the user is already registered and confirmed. [DDPS-5133]
- An issue related with Microsoft platform validation profile changes that prevented BitLocker Manager from beginning to encrypt on Windows 10 is now resolved. [DDPS-5243]
- The Device Lease Period can now be reduced to a minimum of 14 days. [DDPS-5281]
- An issue that resulted in an access violation error in module 'GKConsole.exe' is now resolved. [DDPS-5300]
- A page selector and drop-down list now allows the administrator to navigate between pages of Endpoint Groups and select the number of groups to display per page. [DDPS-5349]
- Policy commit comments that begin with special characters are now logged in Commit History. [DDPS-5353]
- Duplicate entries no longer display in the BitLocker Manager Detail report in Compliance Reporter after upgrade. [DDPS-5432]
- An issue is resolved with Threat Protection (TP) licenses for Web Protection and Firewall, and they now match consumed licenses for Advanced Threat Prevention (ATP) with Web Protection and Firewall. [DDPS-5491]

Technical Advisories v9.8

- Added 01/2018-Advanced Threat Event results are automatically limited to the first 10000 results. This will resolve issues where Advanced Threat Events were not properly displaying when selecting the tab within the Dell Security Management Server
- To block all PowerShell scripts with Advanced Threat Prevention, both the PowerShell and PowerShell Console policies must be set to **Block**. When both policies are set to Block, no scripts can be run, either through the PowerShell console or the Cmd console. PowerShell one-liners are blocked. 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. 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]
- The Encryption recovery file that is downloaded from the Dell Server is wrapped inside an executable file. To extract it, run the following command:

  ```
  <recovery file>.exe -extract
  ```

  [DDPS-5054]
- The Office Protected Files Cover Page Corporate Logo policy cannot be committed when running the Remote Management Console in Firefox. To work around this issue, use Internet Explorer or Google Chrome. [DDPS-5538]
- Added 08/2018-The Dell Policy Proxy service may incorrectly send two requests to the back end server for SKID3 requests. This can safely be ignored. [DDPS-5585]

New Features and Functionality v9.7

- VE now supports Advanced Threat Prevention with optional Client Firewall and Web Protection features. Client Firewall and Web Protection policies are reorganized to simplify management of these features. Prior to client upgrade to the new features, refer to Default Policy Changes.
- VE now supports Disconnected Mode, for air-gapped environments.
- Added 7/2017 - VE is now supported with VMware ESXi 6.5.
- VE is now supported with Hyper-V.
- Active Directory groups and domains can now be specified when adding or modifying Endpoint Groups. VE collects Active Directory information from endpoints and makes this data available for Endpoint Group specification.
- Endpoint Group Precedence can now be modified using drag-and-drop functionality. This functionality applies to Admin-Defined, Rule-Defined, and Active Directory but not System-Defined Endpoint Groups. Precedence of System-Defined Endpoint Groups for new installations and upgrades is as follows: Highest precedence is given to Non-Persistent VDI followed by Persistent VDI Endpoint Group. Lowest precedence is given to Default followed by Opt-in Endpoint Group.

- Added 7/2017 - Administrators can now bulk upload and import a CSV list of Endpoints to add to Admin-Defined Endpoint Groups.
- Advanced Threat Prevention and Dell Data Guardian events can now be exported to a syslog server or to a local file through a streamlined Events Management screen.
- New Advanced Threat Prevention policies allow Application Control folder exclusions and automatic deletion of quarantined files after a configurable length of time.
- Log Analyzer results can now be exported to Excel or CSV file.
- New Enterprise Edition for Mac policies replace the need to manage some settings through .plist entries.
- Secure Lifecycle is rebranded to Dell Data Guardian.

Resolved Technical Advisories v9.7

- On the Client Firewall Custom Rule Specify Network page in the Remote Management Console, the Fully qualified domain name field now validates and rejects invalid formats. Also, the Transport protocol drop-down list item **ICMP** and the displayed Message type are now consistent. [DDPS-2820, DDPS-2826, DDPS-2885]
- Transport Protocol values are now populated in the drop-down list in Client Firewall Custom Rules. [DDPS-3819].
- AdminHelp can now be moved to avoid obscuring important fields in the Remote Management Console. [DDPS-4258]
- A few Data Guardian External User Management items that were previously untranslated in the Remote Management Console are now translated. [DDPS-4404]
- The following Enterprise Port Control policies now display with Class: Storage, their parent policy: Subclass Storage: External Drive Control, Subclass Storage: Optical Drive Control, and Subclass Storage: Floppy Drive Control. [DDPS-4682]
- Added 08/2018- Administrators can log in to endpoints with the Logon Authentication Policy for Administrator policy set to **None** and **None**. [DDPS-4739]
- Filtering in the Remote Management Console Advanced Threats Protection tab is now functioning as expected. [DDPS-4772]
- The Error Validating Policy dialog that displays when an updated policy value fails validation now includes the related policy name. [DDPS-4812]
- The Data Guardian policy, Enable Callback Beacon, is now disabled by default. [DDPS-4985]
- Advanced Threat Event Dashboard Notifications are now properly categorized by Type. [DDPS-4994]
- VE updates now succeed as expected. [DDPS-5130]
- Localizations of Remote Management Console and the VE terminal are improved.

Resolved Customer Issues

- Recovery of an EMS-encrypted device now proceeds as expected on a computer and Dell Server other than the original encrypting computer and Server originally managing the device encryption, when the Servers belong to the same federation. To configure federation, follow these steps:

  a On one of the Servers to be federated, edit <root>/opt/dell/server/security-server/conf/federatedservers.properties:

  server.code - Replace "ENC(<Server code>)" with "CLR(<new code; string of characters you select>)". This will be a shared code among the federated Servers.

  Server.uris - List the Servers to be federated, separated with commas. Example: https://server1:8443,https://server2:8443

  b Save federatedservers.properties.

  c Copy federatedservers.properties and save it off the Security Server.

  NOTE: The file must be saved off the Security Server before restart.

  d Restart the Security Server.

  After restart, "CLR(<new code; string of characters you select>)" is changed to "ENC(<new shared code>)" and the new shared Server code is applied to the Security Server.

  e Copy the federatedservers.properties file to the **/security-server/conf** folder of each Server to be federated.

  f Restart each Security Server after copying federatedservers.properties to its /conf folder.

  [DDPS-2889]

- The Compliance Reporter Advanced Threat Protection Details report now runs as expected. [DDPS-4327]
- An issue is resolved that resulted in an intermittent Internal Error in the Remote Management Console. [DDPS-4446]
- An issue is resolved in the French Remote Management Console that resulted in an internal error when accessing the Dashboard. [DDPS-4675]
- A single alias can now be used for more than one domain, allowing filtering for users across the different domains. [DDPS-4683]
- The Spanish translation of the policy override success message is corrected. [DDPS-4718]
- Time stamps on data points now include the current year rather than a future year, in all time zones. [DDPS-4771]
- The Pending Value field now displays the correct value in the Compliance Reporter Pending Policy Detail Report. [DDPS-4840]
- SED data time stamps are now preserved when recovery data is archived. [DDPS-4877]
- A Cloud Profile Update poll no longer results in uncommitted policies. [DDPS-4878]
- An issue is resolved that resulted in an Internal Error when **Reporting** > **Audit Events** is selected in the Remote Management Console. [DDPS-4882]
- The Compliance Reporter Advanced Threat Protection Details report now runs as expected when a Type filter is applied. [DDPS-4926]
- The Policy Proxy Polling Interval value is now correct in the Compliance Reporter Effective Policy Report. [DDPS-4927]

Technical Advisories v9.7

- 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]
- The Client Firewall and Web Protection features of Endpoint Security Suite Enterprise v1.4 require VE v9.7 or later. Before upgrading clients to use these features, VE 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 Default Policy Changes for the policy's new default value. Do not begin client upgrade before the new policy is enforced on the client. [DDPS-5112]
- Added 7/2017 - VE does not support .local domains. [DDPS-5334]

New Features and Functionality v9.6

- VE is now supported with VMware Workstation 12.5.
- VE now supports Advanced Threat Prevention and Encryption on persistent and non-persistent VMware and Citrix VDI clients.
- Secure Lifecycle audit events logs can now be exported to SIEM.
- New Server Encryption policies allow the administrator to configure the maximum number of attempts and retry interval for connection to the Dell Server.
- Remote PBA management of local user accounts is now available.
- New policies and functionality support the Disconnected Mode beta release.

Resolved Technical Advisories v9.6

- The tool tip for the Audit Control policy, Client Retention Storage, now indicates that maximum storage is measured in megabytes. [DDPS-3682]
- The installer error message that occurs when a hostname includes an underscore, which is not allowed, is now more specific. [DDPS-3902]
- A data access error no longer occurs in the Remote Management Console when the default language of a SQL profile is not English. [DDPS-4349]
- A non-domain endpoint is no longer reported as unprotected in the Remote Management Console if the user has logged in more recently than other users on an endpoint and that user has a pending or incomplete encryption sweep. [DDPS-4470]
- The Secure Lifecycle agent is now correctly named on the Remote Management Console Endpoint Details & Actions tab. [DDPS-4512]
- VE v9.6 and later includes a security update addressing a Linux privilege escalation vulnerability (CVE-2016-5195). Customers and field teams should take the latest VE update and all VE updates or sustaining releases as a best practice. [DDPS-4528]
- Added 4/2017 - SSL/TLS protocols for Compliance Reporter are now configurable in the eserver.ssl.protocols property in the /opt/dell/server/reporter/conf/eserver.properties file and are preserved during backup/restore operations. [DDPS-4546]
- An external Secure Lifecycle user can no longer access protected documents after their domain is removed from the Full Access list (previously, whitelist), regardless whether the user is individually granted Full Access/whitelisted. [DDPS-4602]
- Added 08/2018-Registration is now successful when an external user registers to use Data Guardian with Proxy Mode installed. [DDPS-4603]

- Password complexity rules are now enforced when a Secure Lifecycle external user resets the password. [DDPS-4604]
- Filtering with the Removed field in the Compliance Reporter BitLocker Manager Detail-TMP Aware report now returns correct results. [DDPS-4608]
- Forensic key retrieval now proceeds as expected when one or more key_id instances is invalid. [DDPS-4689]

Resolved Customer Issues

- An issue is resolved that resulted in a Core Server process crash after running continuously for several weeks. [DDPS-4471]
- An issue is resolved that resulted in uncommitted policies that were not initiated by the administrator. [DDPS-4761]

Technical Advisories v9.6

- When running Compliance Reporter with Google Chrome, the date selection calendar does not display in the Value column when the **Created *** field is selected in Filter Fields area of the Report Layout. [DDPS-4691]
- Added 4/2017 - Threat Protection Status categories differ between Remote Management Console Dashboard Notifications and Email Notification Summaries. Dashboard Notification categories are Critical, Major, Minor, and Warning. Corresponding email notification categories are Critical, High, Medium, and Low. [DDPS-4802]

New Features and Functionality v9.5

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

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

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

  - Files remain encrypted for unauthorized users, for example, when files are attached in email, moved in a web browser or File Explorer, or stored on removable media.
  - A callback beacon can be inserted into every protected Office file, when the beacon server is installed as part of the Proxy Mode installation.
- As of v9.4.1.11,DDP Enterprise Server - VE supports Advanced Threat Prevention on Mac computers. 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.
- Restoring from backup to DDP Enterprise Server - VE v9.5 is supported with v9.4.1.11 and later.
- As of v9.5, Cloud Edition is no longer supported.

Resolved Technical Advisories v9.5

- After restoring from backup, customized Compliance Reporter reports views and settings are now available as expected. [DDPS-3832, DDPS-4199]
- Searching for endpoints in the Remote Management Console using the Shield Recovery ID now returns expected results. [DDPS-4017]
- An issue is resolved that resulted in Summary Statistics in the Remote Management Console Dashboard occasionally not updating as expected. [DDPS-4082]

- A second or subsequent notification that is added in Notification Management in the Remote Management Console no longer retains the Type and Priority values of the previously added notification. [DDPS-4178]
- The Compatibility Service now starts as expected after restoring from backup to the same VE build from which the backup was taken. Previously, in rare cases the Compatibility Service did not start. [DDPS-4209]
- After the user browses for the Service Account Run As user name, the credentials now populate in the Service Runtime Account Information dialog in the installer. [DDPS-4234]
- The Advanced Threat Prevention category is now populated in Log Analyzer in the Remote Management Console. [DDPS-4241]
- An issue that resulted in failure of Advanced Threat Prevention Agent Auto Update enrollment is resolved. [DDPS-4244]
- The Add User and Add Group options are removed from Domain Detail for Members of Non-Domain Users in the Remote Management Console. These options are not applicable for non-domain users. [DDPS-4255]

Resolved Customer Issues

- The Specification field in the Remote Management Console Add Endpoint Group page is now validated for length and displays an error if more than 4,000 characters are entered. [DDPS-2953, DDPS-4260]
- The TPM Enabled field in the Compliance Reporter BitLocker Manager Detail report is now accurate. [DDPS-3394]

Technical Advisories v9.5

- Amended 7/2017 - The Remote Management Console **Login** button may be disabled in Google Chrome or Internet Explorer on Server 2012. To work around this issue, clear the browser cache and then attempt login or use Mozilla Firefox 41.x or later. [DDPS-4558]
- Advanced Threat Prevention policies are not properly validated if their values are not enclosed in double quotes (") and contain wildcards or special characters, including commas (,), brackets ([ ]), and tildes (~). To force validation, enclose strings in double quotes ("). Do not use wildcards and special characters, which are not allowed. [DDPS-4589]
- Added 2/2017 - Policy validation beginning in v9.5 may result in an "Error Validating Policy " message in the Remote Management Console when attempting to view policy when the value of the policy is incorrectly formatted. To work around this issue, correct the formatting of affected policy values. To identify the affected policies, follow these steps:

  a Open <Core Server install directory> **PolicyService.config**.

  Enterprise Server - Program Files\Dell\Enterprise Edition\Core Server

  VE - /opt/dell/server/core-server

  b Change the StrictValidation property value from **true** to **false**: `<property name="StrictValidation" value="false"/>`

  c Restart the services.

  d In the Remote Management Console, navigate to view policy at the level where the Error Validating Policy previously occurred, and note the policy name identified in the error.

  e Correct the policy value formatting, and click **Save**.

  f In the left pane, click **Management** > **Commit**, enter the policy change description, and click **Commit Policies**.

  g If desired, change the StrictValidation property value from **false** back to **true**, to re-enable policy validation.

  [DDPS-4779]

New Features and Functionality v9.4.1.11

- DDP Enterprise Server - VE now supports Advanced Threat Prevention on Mac computers. 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.

New Features and Functionality v9.4.1

- A new Advanced Threat Prevention 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 Prevention server. Updates are released monthly.
- New Advanced Threat Prevention policies allow the administrator to configure automatic handling upon detection of a malicious payload and extended Script Control settings for Active Scripts, PowerShell, and Office macros.
- The Advanced Threat Events Report can now be exported as an Excel or .csv file from the Advanced Threat Events tab in the Remote Management Console.
- A new policy allows the administrator to hide encryption icons in File Explorer for managed users.

Resolved Technical Advisories v9.4.1

- Dell will continue to support current versions of Virtual Edition on third-party software platforms as long as it is technically and commercially reasonable for Dell to do so, when there is no external dependency. Due to external dependency, VMware ESXi 5.1, VMware Workstation 9, and VMware Workstation 10 are no longer supported as of the v9.4.1 release. For more information, see http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/product-lifecycle-matrix.pdf.
- An error now alerts the administrator that special characters are not allowed in ddpuser, ddpconsole, or ddpsupport passwords. Special characters in these passwords may cause authentication issues with VE services. [DDPS-3357]
- The Inventory Received field on the Endpoint Detail page of the Remote Management Console is now populated upon activation of an endpoint. [DDPS-3982]
- Notification emails are now sent as expected when All Notification Types are selected when configuring Notification Management in the Remote Management Console. [DDPS-4003, DDPS-4038]
- The SED Authentication Method Policy Compliance Reporter report is now present after a VE update from the update server. [DDPS-4014]
- An issue that resulted in an internal error when clicking Device Recovery Keys on an Endpoint Detail page in the Remote Management Console is resolved. [DDPS-4222]

New Features and Functionality v9.4

- The Remote Management Console now features enhanced configurable Dashboard and Email Notifications, to update administrators about threat events, certificate expirations, license availability, configuration changes, product updates, and knowledge base articles.
- Advanced Threat Prevention customers can now take advantage of these capabilities, available in the Remote Management Console:
- Certificates can now be imported and added to the Safe list.
- Security Information Event Management (SIEM) software can be integrated to capture Advanced Threat events.
- Enhanced data about threats and devices on which they are identified is now available.
- The File Folder Encryption policy category in the Remote Management Console has been renamed to Policy-Based Encryption.
- The Alerts Management menu item in the Remote Management Console has been renamed to Notification Management.
- Proxy Mode installations are no longer supported on 32-bit operating systems.

Resolved Technical Advisories v9.4

- The policy values in the BitLocker Manager Policy report are now correctly populated, and managed devices no longer display on duplicate rows. [DDPS-2810, DDPS-3427]
- DDP Enterprise Server - VE now supports multiple entitlements associated with a single service tag. [DDPS-2949]
- Added 7/2017 - The Administrator Roles topic in AdminHelp no longer indicates that the System Administrator can commit policies, recover data, and recover endpoints, and the Security Administrator can delegate administrator rights, although these administrators do not have these permissions, and now correctly indicates that Account administrators can delegate administrator rights. [DDPS-3004, DDPS-3005, DDPS-3006]
- The valid key format is now downloaded from Virtual Edition in Enterprise Edition for Mac recovery files, and an issue that resulted in the Server delivering blank FileVault recovery keys is resolved. [DDPS-3139, DDPS-3873]
- A forensic key bundle download using the Administrative Download Utility (CMGAd) and the Administrative Unlock Utility (CMGAu) now succeed. [DDPS-3244]
- Domains with names that include spaces or special characters can now be added in the Remote Management Console. [DDPS-3329]

- Domain Alias Names are now resolved as expected in the Remote Management Console, and login with an invalid Domain Alias no longer succeeds. [DDPS-3330, DDPSUS-767]
- The Compliance Reporter Advanced Threat Prevention Events report now includes the Type field, which displays the threat type. [DDPS-3331]
- Dropbox for Business remote wipe function is available in the Remote Management Console. [DDPS-3333]
- Administrators can now update Domain Settings in the Remote Management Console after their user credentials are changed in Active Directory and when the Active Directory server or service is unavailable. A "Failed to Retrieve Domain" or "'code':10180" message no longer displays. [DDPS-3336, DDPS-3337, DDPS-3338]
- Entering any combination of upper- and lower-case characters in Compliance Reporter settings now returns expected results. [DDPS-3369]
- VE 9.3.0.40 and later includes a security update addressing a Linux kernel vulnerability (CVE-2015-1805). Customers and field teams should take the latest VE update and all VE updates or sustaining releases as a best practice. [DDPS-3383]
- An issue that led to Remote Management Console timeouts when searching for endpoints is resolved. [DDPS-3400]
- Administrators with UPNs exceeding 32 characters can now effectively send SED commands to devices. [DDPS-3432]
- An issue that led to an internal error in the Remote Management Console is resolved. [DDPS-3454]
- Logging is improved for the error that results when a user with duplicate UPNs in the Dell Data Protection database attempts to log in to the Remote Management Console. [DDPS-3578]
- Logging is improved for the error that results when searching for a user whose group name includes a special character. [DDPS-3587]
- The Common Encrypted Folders policy is now correctly applied to %ENV:USERPROFILE%\Downloads. [DDPS-3752]
- Endpoints that were previously removed can now be consistently added back into inventory and receive new policies as expected. [DDPS-3772]
- The Remote Management Console Domain Details & Actions page is no longer illegible if the domain service account that is used to add the domain includes a quotation mark (") in its password. [DDPS-3813]
- An issue that led to high Compatibility Server CPU load at restart when forensics are enabled in the Security Server is resolved. [DDPS-3833]
- An error that caused occasional Core Server service crashes when multiple inventories are run is now properly handled. [DDPS-3877]

Technical Advisories v9.4

- After Dell Enterprise Server and DDP Enterprise Server - Virtual Edition installation, the Remote Management Console displays "1 Uncommitted Override," indicating a pending policy commit. The policy represents an internal setting. To work around this issue, commit policies after installation. In the left pane, click **Management** > **Commit**, enter the description, "Initial commit," and click **Commit Policies**. [DDPS-3163]
- An error occurs during forensic key bundle download from VE.[DDPS-3244]
- In order for Dell Data Protection SED and HCA v8.5.1 and earlier clients to communicate with Dell Enterprise Server and Virtual Edition v9.4, the following settings must be configured on the Server:

1 On the Security Server, access <root>/opt/dell/server/security-server/conf/spring-jetty.xml, and comment out the excludeProtocols property:

```
<!--

<property name="excludeProtocols" value="SSL,SSLv2,SSLv3" />

-->
```

2 In the <root>/opt/dell/java runtime/jre1.8/lib/security/java.security file, remove "SSLv3, " from the line below:

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 768
```

[DDPS-3371]

- Universal security groups are not supported due to the way they are created within Active Directory. [DDPS-3765]
- Email/SMTP settings are not retained after upgrade and restore from backup. To work around this issue, after upgrade and restore are complete, reconfigure SMTP settings in the VE Terminal:

1 From the Advanced Configuration menu, select **Email Notifications**.

2 In the Set up Email Notifications screen, to enable email alerts, press the Spacebar to enter an **X** in the Enable Email Alerts field.

3 Enter the SMTP Server fully qualified domain name.

4 Enter the SMTP Port.

5 In the From User field, enter the email account ID that will send email notifications.

6 In the Enter User field, enter an email account ID for access to change configured email notifications.

7 In the Password field, enter a password for access to change configured email notifications.

8 In the Mail IDs fields for VE Status, Password Updates, and Updates Availability, enter lists of recipients for each notification type. Follow these conventions when listing recipients: Email address format is recipient@dell.com. Recipients are separated with commas or semicolons.

9 In the Service alert reminder field, to enable reminders, press the Spacebar to enter an X in the field then set the reminder interval in minutes.

10 A Service alert reminder is triggered when the reminder interval has passed after a notification is sent about a system health issue and the host or service remains in the same state.

11 In the Summary Report field, to enable reports of notifications, select the desired interval (Daily, Weekly, or Monthly) and then press the Spacebar to enter an X in the field.

12 Select OK.

13 Restart the services.

[DDPS-4037]

New Features and Functionality v9.2

- DDP Enterprise Server - VE now supports Advanced Threat Prevention. 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 Remote Management Console has a new look and feel, with a responsive HTML 5 design that can be viewed on virtually any screen size. It no longer requires installation and is now accessed at this URL:

  https://server.domain.com:8443/webui/
- The Remote Management Console now offers the following new features and capabilities:
  - Email alert notifications can be set for Threat Protection and Advanced Threat Prevention events.
  - When data is recovered on a computer with more than one self-encrypting drive, each drive can be individually selected for recovery.
- Amended 07/2016 - The Console Web Service component is no longer used as of v9.2, with the removal of the Silverlight Console.

Resolved Technical Advisories v9.2

- The SMTP Server field in the VE Terminal Set up Email Notifications screen is now validated and no longer allows a comma, which is an invalid character. [DDPMTR-1562/DDPS-1900]
- Further research into entitlement issues yielded testing improvements, resulting in the resolution of some open and unresolved issues. [DDPMTR-1768, DDPS-1571, DDPS-1716/DDPSUS-235]
- A few items on Remote Management Console screens that were previously untranslated are now translated. [DDPS-846, DDPS-1519, DDPS-1525, DDPS-1722, DDPS-1928]
- The Compliance Reporter Effective Policy Report now displays Gatekeeper connections and the correct value type for the Policy Proxy Polling Interval policy. [DDPS-1233]
- When a non-domain computer is joined to the domain, duplicate endpoint entries no longer display in the Remote Management Console, and the endpoint properly receives policies. [DDPS-1304]
- The Compliance Reporter Administrator List Report now includes the Group Name field. [DDPS-1720]
- In the Remote Management Console, when Client Firewall rules are added or edited, the executable Signed by field is now validated. [DDPS-1794/DDPSTE-445]
- When retrieving the BitLocker Manager recovery password in the Remote Management Console for more than one volume, the first recovery password is now cleared before second and subsequent BitLocker volumes are selected. [DDPS-1808]

- Permissions that are inherited from a group are now removed from Remote Management Console administrators when the group is removed. [DDPS-1853]
- The Compliance Reporter Local Policy Report now includes device-based policy changes made at the Endpoint Group and Endpoint levels. [DDPS-1859]
- After upgrade from v8.2.x, Compliance Reporter reports for Server Encryption and Threat Protection are now retained. [DDPS-1861]
- The new name of a renamed computer now replaces the previous name rather than displaying as a second endpoint in the Remote Management Console when keys are escrowed before the new computer name is processed in inventory. [DDPS-1895]
- An error message now displays when invalid input is entered into the VE Terminal UI Hostname field. [DDPS-1896]
- The Cloud Storage policy, OneDrive Message, is no longer applicable and is now removed from the Remote Management Console. [DDPS-1917]
- Previously untranslated text on the VE Terminal UI Certificate Configuration and Server Status screens is now translated. [DDPS-1939]
- The default Cloud Encryption Help File delivered to endpoints through the Help File Contents policy now renders properly on endpoints. [DDPS-2071]
- The Mac recovery bundle now includes the hostname and extension in the Save dialog that displays on the endpoint. [DDPS-2090]
- An Unknown Exception no longer occurs during upgrade after users have been manually removed from Active Directory. [DDPS-2330]
- Inventory polls for managed clients have been reduced from twelve to two hours to more accurately reflect status changes. [DDPS-2371]
- After a certificate request is successfully created in the VE Terminal, returning to the Create Certificate Request screen no longer returns the user to the shell prompt. [DDPS-2405]
- The Server Encryption identity certificate is now preserved when restoring from a pre-v9.1 backup. [DDPS-2431]
- When an endpoint is moved from one Endpoint Group to another non-default Endpoint Group, Endpoint Group policies are now consistently applied based on Precedence settings. [DDPS-2881]
- A default SDE Encryption Rules policy which caused problems with Windows updates has been resolved. The issue resulted from encryption of \System32 executable files. The default policy has been changed for EE and VE Servers v9.2 and later. [DDPS-2952, DDPC-1207]
- VE v9.2.0.216 and later includes a security update addressing a Linux GNU C Library (glibc) vulnerability (CVE-2015-7547). Customers and field teams should take the latest VE update and all VE updates or sustaining releases as a best practice. [DDPS-3328]

Technical Advisories v9.2

- A Compliance Reporter report layout can be deleted without an error message although subordinate reports are attached to it. [DDPS-1094]
- The IP Exclusions for Web Protection field in the Remote Management Console accepts invalid formats. [DDPS-2206]
- The description of a custom Client Firewall rule in the Remote Management Console does not include local or remote network type. [DDPS-2278]
- If browser cookies are not enabled, the message "An internal error occurred" displays at logon to the Remote Management Console rather than a message prompting the user to enable cookies. [DDPS-2661]
- Compliance Reporter customizations are lost when updating from a pre-v9.2 version of VE. [DDPS-2667, DDPS-2811]
- The Compliance Reporter Mobile Device Policy report is not populated. [DDPS-2675]
- In Compliance Reporter Report View Scheduling, the tooltip for the Email Recipients field says that email addresses can be separated by commas or placed on separate lines. Email addresses cannot be placed on separate lines but should be separated by commas. [DDPS-2678]
- When restoring a v8.5 VE backup to a v9.2 VE with a customized hostname, Compliance Reporter will not start. [DDPS-2759]
- During services restart, navigating to the Enterprise Population pages in the Remote Management Console results in an Access Denied message rather than a return to the login page. [DDPS-2815]
- After the Advanced Threat Prevention service is provisioned, Advanced Threat Events do not begin to display until the administrator logs off then logs back on to the Remote Management Console. [DDPS-2816]
- The Remote Management Console Endpoint Security Policies tab shows values for the BitLocker Recovery Information to Store in AD DS policy as *Recovery Passwords and Keys Packages* and *Recovery Passwords Only*. In Endpoint Effective Policies, the values for the same policy are *Passwords and Keys* and *Passwords Only*. [DDPS-2821]
- The Client Firewall custom rule allows the administrator to enter subnet addresses although subnets cannot be created for local or remote networks. [DDPS-2838]
- A few tooltips and areas of a few pages are not localized in the Remote Management Console. [DDPS-2842, DDPS-2844, DDPS-2989, DDPS-2994, DDPS-2996, DDPS-2997, DDPS-2999]
- "Override Count" is truncated on the Endpoint Security Policies tab in the Spanish, Italian, French, Portuguese, and Brazilian Portuguese Remote Management Console. [DDPS-2843]

- The Remote Management Console User Detail tab displays the Effective Policies icon for mobile devices although effective policies do not apply to mobile devices. [DDPS-2880]
- There is a delay between completion of the VE poll based on the configured Server Polling Interval and display of Threat Protection events in the Remote Management Console. [DDPS-2896]
- The refresh button is not functioning on the Alerts Management page in the Remote Management Console. [DDPS-2923]
- Resetting the database password in the VE Terminal with a password that contains a pound or number sign character (#) causes database-dependent services to fail. [DDPS-2924]
- The Add Domain page in the Remote Management Console has no vertical scrollbar, so on small screens or screens with low resolution, the Add Domain button is not visible. [DDPS-2945]
- Entering an invalid LDAP password when adding a domain in the Remote Management Console results in a prompt to check the logs rather than a message that the password is invalid. [DDPS-2954]
- The Remote Management Console does not function if TLS v1.0 is disabled. [DDPS-2955]
- The Network Settings default button in the VE Terminal differs between initial setup and subsequent visits to the Network Settings page. During setup, the Cancel button is default. After setup, the OK button is default. [DDPS-3002]
- If an invalid hostname is entered during Advanced Threat Prevention Service setup, a timeout occurs. To work around this issue, click OK in the Timeout dialog to return to the Services Management page. Verify the hostname, and begin Advanced Threat Prevention Service setup again. [DDPS-3019]
- Email alerts of Advanced Threat Prevention events are not being sent. [DDPS-3031]
- When upgrading a VE Server to v9.2, after it was previously upgraded to v8.2.3 and the database password was set to non-default before upgrade to v8.2.3, the Server Encryption root certificate is not properly stored in the database and Server Encryption clients will not activate against VE. To work around this issue, before upgrade to v9.2, follow these steps to reset the database password:

1. In the VE Terminal Advanced Configuration Menu, select **Database Password**.
2. Enter a new database password, and select **OK**.

   If upgrade to v9.2 has already been performed, to work around this issue, follow these steps:
3. In the VE Terminal Advanced Configuration Menu, select **Database Password**.
4. Enter a new database password, and select **OK**.
5. At the login prompt, log in as the ddpsupport user.
6. Run the following script to generate a new Server Encryption certificate and store it in the keystore and database:

   ```
   sudo /opt/dell/vascripts/gen_ssos_cert.py
   ```

   [DDPS-3047]

New Features and Functionality v9.1.5

- Cloud storage provider profiles are now automatically updated daily on DDP Enterprise Server - VE. Updates are delivered to Dell Data Protection | Cloud Edition clients when policies are committed.

Resolved Technical Advisories v9.1.5

- The setting field of the Threat Protection policy, Exclude Processes, no longer accepts invalid values in the Remote Management Console. [DDPMTR-1346]

Technical Advisories v9.1.5

- The command line interface that is used to force VE to poll for cloud storage provider profile updates outside the daily polling and update cycle is not yet functional. [DDPS-1916]
- Added 02/2016 - After migration to v9.1.5, the Domain Users group in the Remote Management Console does not display all users in the group. [DDPS-1937]
- Added 02/2016 - The Remote Management Console displays unprotected status for EMS-encrypted USB drives. [DDPS-2835]

New Features and Functionality v9.1

- Forensic Administrator rights for a User Group can now be delegated by the Superadmin or Security Administrator to a member of the User Group.
- Dell Enterprise Server - Virtual Edition v9.1 includes the new Server Encryption policies to support Beta activity. If you are interested in participating in the Beta, please contact your Dell account team for more information.
- Deferred Client Activation is now supported, allowing an enterprise to extend centrally managed encryption policies to users' devices in a BYOD environment.
- New policies allow administrators to suppress or filter Endpoint Security Suite popup notifications on client computers. This update is supported with Endpoint Security Suite v1.1.1 and later clients.
- Support for user feedback to Dell is now available through policy for most Dell Data Protection clients.

Resolved Technical Advisories v9.1

- When Client Firewall rules are added or edited in the Remote Management Console, Custom EtherType now accepts only four characters, and values entered into the Domain name field are now validated. [DDPMTR-528, DDPMTR-732]
- In the Remote Management Console, when Core Networking rules are added or edited, the Connection types field is now locked as expected and cannot be edited. [DDPMTR-562]
- In the Remote Management Console, an endpoint that has been previously removed can now be recovered. [DDPMTR-640]
- The format of the email notification that Virtual Hard Drive capacity exceeds 90 percent is now consistent with other VE notification emails. [DDPMTR-685]
- Authorization of the link between the Server and Dropbox now succeeds when Cloud Edition is deployed. [DDPMTR-748]
- When Cloud Edition is deployed and an external user activates against the Server, on the User Details page in the Remote Management Console, the User Type no longer incorrectly displays as "AD." [DDPMTR-762]
- In the Remote Management Console, when an attempt is made to import an invalid or duplicate license, the previous generic error message has been replaced with a message that more clearly describes the error. [DDPMTR-764]
- The Secure Windows Credentials policy is now correctly grouped with Fixed Storage Policies rather than with General Settings policies. The SDE Encryption Enabled policy must be set to True in order for the Secure Windows Credentials to be applied. [DDPMTR-786, DDPSTE-638]
- In the Compliance Reporter Mobile Device report, time stamps for commands sent to mobile devices are now correct. [DDPMTR-839]
- In the Remote Management Console, Log Analyzer - Admin Actions now displays accurate data for endpoint policy changes, and System Logs now displays login entries for users from sub-domains. [DDPMTR-911, DDPMTR-991]
- The Threat Protection Security policy now disables all Threat Protection policies and features. [DDPMTR-1011]
- The Host Name field is now selected for inclusion by default and Host Names displayed in the Report Result are now correct in the Compliance Reporter Threat Protection Details report. [DDPMTR-1014]
- Active Directory reconciliation no longer fails when one of multiple domains is offline or inaccessible on the network. [DDPMTR-1153]
- When an executable is edited in Default/Custom Firewall rules, an "Invalid Signer" error no longer displays in the Remote Management Console. [DDPMTR-1156]
- VE v9.1 includes a security update addressing an OpenSSL vulnerability (OpenSSL CVE-2015-4000). Customers and field teams should take v9.1 and all VE updates or sustaining releases as a best practice. [DDPMTR-1507]
- Performance is improved for client activations based on streamlined access of Active Directory. [DDPMTR-1538]
- The Threat Protection Security policy now disables all Threat Protection policies and features. The three policies, Malware Protection, Client Firewall, and Web Protection, no longer have to be individually set to False. [DDPSTE-451]

Technical Advisories v9.1

- Portions of a few Compliance Reporter, Remote Management Console, and VE Terminal screens are not translated. [DDPMTR-1471, DDPMTR-1472, DDPMTR-1473, DDPMTR-1477, DDPMTR-1479]
- With Cloud Edition, if an external user has previously registered and then is added to the blacklist, the user is not prevented from registering again. [DDPMTR-1599]
- With Deferred Client Activation, on the first attempt to remove an endpoint, an error displays and the endpoint is not removed. To work around this issue, perform the action again. The endpoint is removed as expected. [DDPMTR-1711]
- An error displays and the search fails when searching System logs in Log Analyzer for the first time. To work around this issue, perform the search again. [DDPMTR-1714]

- Amended 09/2015 - The BitLocker External Media report displays two Protection Status columns with different values in Compliance Reporter. [DDPS-1719]
- When an Identity Certificate to be used with Server Encryption is imported and the process fails, no active root certificate is present and Server Encryption activations cannot proceed. To work around this issue, import a valid certificate and ensure that the import succeeds without error. After successful import, activations proceed as expected. [DDPMTR-1726]
- Very rarely, Server Status does not display following a VE update. To work around this issue, reboot VE. [DDPMTR-1733]
- Amended 02/2016 - Pressing Esc navigates to a higher level menu than expected in a few VE Terminal screens. If no time zone is selected in the VE Terminal Time Zone screen, pressing Esc does not navigate to the next higher level menu. [DDPS-1849, DDPS-1862, DDPS-1920]

New Features and Functionality v9.0

- VE now supports Endpoint Security Suite with an extensive set of new policies and Compliance Reporter reporting options. Endpoint Security Suite includes the following:
- Malware Protection
- Client Firewall
- Web Protection
- DDP|E Encryption
- SED Management
- Advanced Authentication
- BitLocker Manager
- Capability is added to update self-signed certificates through the VE Terminal user interface.

Resolved Technical Advisories v9.0

- When a proxy server is used, proxy server settings and firewall credentials can now be configured through the VE Terminal UI for communication with the Update Server. [DDPS-803]
- The System Snapshot Log file contents no longer includes unnecessary files. [DDPS-1139]
- If VE disk utilization exceeds 90 percent, notification emails are now sent every hour rather than several times an hour. [DDPS-1177]
- VE communication with the Update Server is now properly logged without duplication. [DDPS-1215]
- Regular checks for VE updates and results of these checks are now logged to the syslog file as expected. [DDPS-1217]
- VE now sends an email notification if a check for VE update fails. [DDPS-1285]
- Translated text in a few localized VE Remote Management Console screens is corrected. [DDPS-1327]
- The time zone setting is now preserved after restoring VE from backup. [DDPS-1329]
- A Restore operation is now prevented if all VE services are not Running before the Restore operation is initiated. All services must be Running before a backup is restored, or they will not automatically start after the backup is restored. [DDPS-1348]
- Occasional activation failures that previously occurred during automated database clean-up no longer occur. [DDPS-1423]
- VE v9.0 includes a security update addressing an OpenSSL vulnerability (OpenSSL CVE-2014-3566). Customers and field teams should take v9.0 and all VE updates or sustaining releases, as a best practice. [DDPS-1437, DDPS-1438, DDPS-1440]
- During an update, the VE Terminal Update Installation Status window now scrolls properly to display complete progress of the update. [DDPS-1459]
- VE v9.0 includes a security update addressing a Linux GNU C Library (glibc) vulnerability (CVE-2015-0235). Customers and field teams should take v9.0 and all VE updates or sustaining releases, as a best practice. [DDPSTE-363]

Technical Advisories v9.0

- Added 02/2016 - Virtual Edition is not sending email notifications as expected. [DDPS-1705]
- To protect communications against the OpenSSL CVE-2014-3566 vulnerability, DDP|E Virtual Edition v9.0 is set to communicate using TLS, by default. However, DDP|E SED and HCA v8.5 and earlier clients communicate with VE using SSL. This means that when running VE Server 9.0, DDP|E SED or HCA v8.5 and earlier clients with Preboot Authentication activated will fail to communicate with the VE Server. To work around this issue, search "SLN295960" at www.dell.com/support, to find the knowledge base article associated with this issue. This workaround must be implemented as soon as possible, in order to prevent PBA client communication issues with the VE Server v9.0. [DDPSTE-169]
- When running the EAS Configuration Tool to set up Exchange ActiveSync management while the Exchange ActiveSync web application is configured to run in IIS Classic mode, policy communication errors occur and the following message displays: "Failed to add the

OTASync module declaration." To work around this issue, if possible, use IIS Integrated mode. As an alternative, the web.config and EASMailboxManager.exe.config files can be modified to correct the issue. For more information about modifying these configuration files, search "SLN295997" at www.dell.com/support, to find the knowledge base article associated with this issue. [DDPSTE-307]

- In the Remote Management Console, when duplicate entries of a Mobile Edition endpoint exist, selecting the Resolve User option returns an error and does not resolve the duplicate entries. [DDPSTE-371]
- In the Remote Management Console, when Client Firewall rules are added or edited, the IP address and Network type fields are not validated; column headers can be moved and resized to the extent that headings become illegible; multiple rows can be selected, preventing them from being edited; the Cancel button is unresponsive in the Add and Edit dialogs; and an executable that is added does not display until the rule is closed then reopened. [DDPSTE-414, DDPSTE-415, DDPSTE-421, DDPSTE-426, DDPSTE-430, DDPSTE-431, DDPSTE-437, DDPSTE-443]
- In the Remote Management Console, when Client Firewall rules are added, the Add dialog occasionally freezes when incorrectly formatted values are entered. To work around this issue, click the close button in the upper right corner of the dialog then click the Add button under Specify Networks to reopen the dialog. [DDPSTE-432]
- When Virtual Edition is updated, the Remote Management Console must also be updated. For instructions, see the *Virtual Edition Quick Start Guide and Installation Guide*.

New Features and Functionality v8.5

- DDP Enterprise Server - Virtual Edition (VE) now supports automated migration from DDP Personal Edition to Enterprise Edition with the DDP Managed Migration Utility.
- VE now supports Secure LDAP (LDAPS).
- VE v8.5 has been validated with VMware ESX/ESXi 5.5.

Resolved Technical Advisories v8.5

- The user can no longer download a duplicate update but is, instead, now prompted to install the previously downloaded update. [DDPS-504]
- Various improvements have been made to the VE Terminal user interface. [DDPS-622, DDPS-624, DDPS-881]
- Logs are now properly rotated based on the log rotation interval configured in the VE Terminal. [DDPS-653]
- VE user password complexity requirements are now correctly enforced. [DDPS-654]
- Changes to time zones are now correctly set, regardless the length of time zone names. [DDPS-656]
- A few previously unlocalized portions of VE Terminal and Remote Management Console screens and AdminHelp topics are now localized. [DDPS-757, DDPS-758, DDPS-760, DDPS-761, DDPS-762, DDPS-763, DDPS-764, DDPS-766, DDPS-832, DDPS-943, DDPS-972]
- When the VE hostname is changed in the VE Terminal, the syslog and the Dropbox for Business landing page now correctly display the updated VE hostname. [DDPS-797, DDPS-801]
- In AdminHelp, default values now correctly reflect the defaults implemented in VE for these Mac Encryption policies: EMS Access Code Attempts Allowed and EMS Cooldown Time Increment. [DDPS-804, DDPS-805]
- Custom reports in Compliance Reporter are now preserved in VE backups. [DDPS-838]
- The Cloud Edition download page on the Japanese VE now correctly displays Japanese characters. [DDPS-845]
- After a backup is restored to a VE when remote database access is enabled, access is now enabled, and the VE Terminal Enable Database Remote Access field is properly selected. [DDPS-854]
- When restoring a backup on a VE with a hostname that has been changed since the backup, backup proceeds normally, and an email notification that VE is unable to resolve the host is no longer sent to the root user. [DDPS-855]
- When VE email notification settings are changed, VE Servers now correctly restart and Cloud Edition account registrations are successful. [DDPS-865]
- Self-encrypting drives (SEDs) now successfully activate against VE. Previously, in a few cases, SEDs did not activate as expected. [DDPS-867]
- File names are no longer duplicated in backups extracted on Windows computers. [DDPS-884]
- The Support Tools option in the VE Terminal, Generate System Snapshot Log, now correctly includes rollover logs and system-level logs. [DDPS-890, DDPS-909]
- When VE disk utilization exceeds 90 percent, an email is now sent to notify the administrator that the oldest VE backups will be removed. [DDPS-894]
- The Cloud Edition download page on VE now correctly displays the OS versions supported with Cloud Edition. [DDPS-908]
- The VE Terminal Available Update screen now displays the version of the update. [DDPS-952]

- Notification of a reboot now displays after an update is installed. [DDPS-955]
- In the Portuguese Remote Management Console, the tool tip for the Inactivity Period for Device Lock policy now displays the correct value range. [DDPS-965]
- If the Update Server experiences a timeout during update download, after the second VE startup, VE now automatically reattempts the download. [DDPS-982]
- Key material now downloads normally after reactivation of non-domain users who were previously deactivated. [DDPS-1136]
- When VE starts for the first time, the Update Server Hostname dialog no longer displays. The dialog has been removed, because the Check for Update function fails if the hostname is changed at initial startup. [DDPS-1271]
- VE has been updated to eliminate the potential for exploitation through the Shellshock Vulnerability, described in Ubuntu Security Notices USN-2362-1 (http://www.ubuntu.com/usn/usn-2362-1/) and USN-2364-1 (http://www.ubuntu.com/usn/usn-2364-1/). As a matter of best practice, customers (and field teams) should always take VE updates or sustaining releases. [DDPS-1368]

Technical Advisories v8.5

- In Compliance Reporter, results of generated report views and plugin data are not retained after VE is updated. [DDPS-1155, DDPS-1156]

New Features and Functionality v8.4

- DDP Enterprise Server - Virtual Edition now supports new Cloud Edition policies that offer expanded protection and management options. When Cloud Edition is used with Dropbox for Business, the following features are now available:
  - The Dropbox for Business administrator can now remote wipe a Dropbox for Business account.
  - New policies offer multi-account support, providing the capability to distinguish between Dropbox for Business and Dropbox personal accounts.
- Dell Compliance Reporter offers new reporting options:
  - A new Cloud Users report displays enrollment and remote wipe information about Dropbox for Business users.
  - New filtering options are available with the Cloud Edition Encrypted Files/Actions report to provide greater customization of event and key management detail.
  - The Device Detail report now includes a field to indicate devices that have self-encrypting drives installed.

Resolved Technical Advisories v8.4

- Dell Policy Proxy now activates normally when an iOS web clip URL is specified before activation. [DDPS-162]
- AdminHelp is now updated to reflect accurate default values and ranges of the following policies: Cloud Storage Server Polling Interval, Self-Encrypting Drives Initial Access Code, User Group precedence default value, and Mobile-EAS Number of Failed Passcode Attempts Before Device Wipe and Inactivity Period for Device Lock. [DDPS-462, DDPS-545, DDPS-559, DDPS-636, DDPS-641]
- A few previously unlocalized screens of the Remote Management Console installer are now localized. [DDPS-477]
- It is no longer necessary to install a previous VE version before restoring from a backup created with a pre-v8.2.0.44 VE. [DDPS-503]
- Compliance Reporter Help is now updated to reflect the functions currently available in the Compliance Reporter Admin Functions pane. [DDPS-512, DDPS-513]
- Hidden endpoints no longer display as Visible on the Remote Management Console Endpoint Search page. [DDPS-554]
- The SFTP Config user can no longer configure or change the VE users, ddpuser, ddpconsole, and ddpsupport. [DDPS-598]
- All users now receive their correct policy on Shielded computers that have multiple users. [DDPS-603]
- Dell Manager v7.1 now successfully activates against VE. [DDPS-614]
- Remote Management Console login no longer fails when the user's display name in Active Directory is blank. [DDPS-615]
- In the VE Terminal, the <Esc> key now correctly cancels the operation and displays the next higher menu from these menu options: Reboot Appliance, Shutdown Appliance, Start Application, Stop Application, and Last successful update applied. [DDPS-619]
- Remote database access is now available immediately after it is enabled. A VE restart is no longer required. [DDPS-652]
- The email sent by VE to notify the administrator that a password has been changed for the ddpuser, ddpconsole, or ddpsupport account now correctly displays the name of the recipient. [DDPS-667]
- When remote database access is enabled, a backup of VE is no longer initiated. The backup impacted no other VE process but may have affected performance in installations with large databases. [DDPS-679]

- VE v8.4 is a security update addressing an OpenSSL vulnerability (OpenSSL CVE-2014-0224). Customers and field teams should take v8.4, and all VE updates or sustaining releases, as a best practice. [DDPS-822]

Technical Advisories v8.4

- With Internet Explorer, if VE is configured with localhost self-signed certificates, authenticating Dropbox with Cloud Edition fails. To work around this issue, use Google Chrome or Mozilla Firefox as the default browser if using self-signed certificates. If Internet Explorer is set as the default browser when the user activates against VE, the user must change the default browser to Google Chrome or Mozilla Firefox then activate against VE again. [DDPS-765]

New Features and Functionality v8.2.3

- DDP Enterprise Server - Virtual Edition now supports VMWare Workstation 10.

Resolved Technical Advisories v8.2.3

- When the task to enable remote database access is canceled with no changes, the selection is now cleared in the Enable Database Remote Access field. [DDPS-160]
- The health monitoring notification email format is now consistent with other VE notification emails. [DDPS-412]
- VE Admin Help now correctly states that an interval of 1 to 1440 minutes will be accepted by the Server for the Cloud Storage > Server Polling Interval policy. [DDPS-462]
- VE Admin Help now correctly states that an unlimited number of attempts can be set for the Global Settings > Non-Cached User Login Attempts policy. [DDPS-465]
- In the VE Remote Management Console installer Set Host Data dialog, if a valid hostname is not entered in the Host field, installation now proceeds and the user is prompted to enter the hostname when installation is complete. [DDPS-471]
- When a large VE backup is restored, a progress indicator now displays. [DDPS-489]
- Script text no longer overwrites the VE Terminal menu during these procedures: setting or adjusting Logrotate; enabling SSH access; and configuring automatic backup or email server settings. [DDPS-501, DDPS-505, DDPS-506, DDPS-507]
- Pressing <Esc> or selecting Cancel from a VE Terminal menu now displays the next higher menu instead of the Main Menu. [DDPS-508]
- In the Dell Policy Proxy installer Ready to Install dialog, the Back button now correctly returns the user to the Certificate Authority dialog rather than the Front End Configuration dialog. [DDPS-518]
- The Bitlocker Manager client can now activate against VE. [DDPS-520]
- Although VE was not susceptible to the Heartbleed vulnerability (OpenSSL CVE-2014-0160), as a precautionary measure, the software stack was updated. As a matter of best practice, customers (and field teams) should always take VE updates or sustaining releases. [DDPS-595]

Technical Advisories v8.2.3

- Added 02/2016 - When upgrading VE with a database password that was set to non-default before upgrade, regenerating a self-signed certificate or importing a new certificate fails. To work around this issue, after upgrade, reset the database password. [DDPS-3047]

Resolved Technical Advisories v8.2.2

- iOS policies are now properly applied in VE. [DDPS-48, 28287]
- It is no longer possible to type text on the Check for Update and Download Update windows. [DDPS-45]
- If an attempt to add an endpoint group fails due to an invalid parameter, the name used with the invalid group entry can now be reused. [DDPS-49, 28307]
- When the task to enable remote database access is canceled with no changes, the VE Server no longer inadvertently restarts. [DDPS-54]
- Users are now prompted to re-enter passwords to enable database remote access or change the database password, which helps prevent incorrectly typed passwords from being unintentionally committed. [DDPS-56]
- A few screens that were previously not localized are now localized. [DDPS-64]
- After an update is applied, the VE Server now correctly restarts. [DDPS-77]
- VE Server policies for Cloud Edition now include the new Box sync client IP address range. [DDPS-88]

- During a manual backup, the backup script no longer displays on the VE Terminal menu. [DDPS-126]
- Events involving the VE Secure FTP server are now properly logged. [DDPS-127]
- After the IP address is changed in the VE Terminal, the updated IP address now correctly displays on the VE Terminal menu. [DDPS-128]
- When restoring from backup, the Inventory Server service now properly restarts without dependence on a VE Server reboot. [DDPS-132]
- When VE Server is started, if a VE Server update is available, a notification of the update displays. [DDPS-139]
- The update notification and password change emails now include the correct hostnames of the VE Servers from which they originate. [DDPS-144, DDPS-145, DDPS-303]
- The tasks of changing the database password and enabling database remote access can now be performed in the VE Terminal. [DDPS-156]
- The VE Terminal now displays update download completion, update progress, and update applied success or failure. [DDPS-174, DDPS-175, DDPS-176, DDPS-181]
- The Support Tools option in the VE Terminal, Generate System Snapshot Log, now properly compiles all system logs rather than including only the Mail Log. [DDPS-294]
- Enterprise Edition for Mac Shields with computer names containing the apostrophe character now properly activate. [DDPS-350]
- When the VE Server starts for the first time, the prompt to change the password now displays the user account for which the password will be changed. [DDPS-363]
- Improvements related to policy enforcement and recovery have been made to the policy delivery engine. [DDPS-365, DDPS-376, DDPS-378, DDPS-380, DDPS-474]
- A password update email is now generated when the password for the ddpconsole user account is changed. [DDPS-374]
- On the Endpoint Details page, Cloud Device Control commands now correctly display when a self-encrypting drive (SED) is activated. [DDPS-379]
- Full Release Notes for updates are now available in the VE Secure FTP server, as Release-Notes, in addition to the update notification email. [DDPS-389]
- VE backup no longer fails after changes are made to SSH access and before a reboot. [DDPS-406]

Technical Advisories v8.2.2

- When a recovery package is generated, it is stored in the installation path of the Server for which it was generated rather than being stored in a common directory. [DDPS-136]

Resolved Technical Advisories v8.2.1

- The IP address and hostname now display on the VE Terminal Main Menu screen after login. [DDPS-38, 27742]
- Application logs are now present in the snapshot log generated for Dell ProSupport using the Generate System Snapshot Log menu option. [DDPS-39, 27998]
- The default selection is now "OK" rather than "Cancel," in VE Terminal screens. [DDPS-40, 28005]
- The Korean VE Terminal correctly displays the Korean language. [DDPS-41, 28080]
- After changing TCP/IP settings, the updated IP address displays in the VE Terminal. [DDPS-42, 28093]
- Policy Proxy now sends new policies after restoring VE from backup. [DDPS-43, 28380]
- Compatibility, Core, and Inventory services now restart after restoring VE from backup, regardless whether the VE database password has been reset. [DDPS-44, 28381]
- A few screens that were previously not localized in the VE Remote Management Console installer are now localized. [DDPS-51, 27881]
- Notification in the VE Terminal that a VE update is available now provides information about the update. [DDPS-113]
- A password change requirement is no longer enforced for DDP and database user accounts. [DDPS-137]
- An email notification error no longer occurs after the server automatically polls for VE updates. [DDPS-138]

Technical Advisories v8.2

- VE uses third-party libraries from "urwid" under the terms of GNU Lesser General Public License. The copyright notice and GNU Lesser General Public License can be found in the AdminHelp on the Attributions, Copyrights, and Trademarks page.

Default Policy Changes

Default policy value changes in new Dell Server versions do not affect Server migrations. This prevents unexpected changes to existing environments. If you need to apply the new default values, you must manually change and commit the policy after migration is complete.

△ CAUTION: **Carefully plan changes to default policy values, taking into account their effects on all groups, endpoints, or users to which the policy applies.**

Global Settings Default Policy Changes

The following Global Settings policies' default values are changed.

Table 1. Security Management Server or Security Management Server Virtual v9.8 - Global Settings Default Policy Value Changes

Technology Group	Policy	Previous Default Value	New Default Value
Global Settings	Custom Support Dialog	\"Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. \nFor more information, <a href=\"http://www.dell.com/us/business/p/ddpe-enterprise-edition/pd\">visit us online</a>\n\nTechnical Support: <a href=\"http://www.dell.com/ddpesupport\">Online Support</a>\n\nProduct Questions and Sales:\nIn the US? Call 877.459.7304 Ext. 4310039\nInternational Support? <a href=\"http://www.dell.com/support/article/us/en/19/SLN297692\">Find the appropriate number here.</a>\"	For questions or concerns with Dell Data Security, contact your system administrator or help desk.

Data Guardian Default Policy Changes

The following Data Guardian policies' default values are changed.

Table 2. Security Management Server or Security Management Server Virtual v9.8 - Data Guardian Default Policy Value Changes

Technology Group	Policy	Previous Default Value	New Default Value
Data Guardian	No policies' default values changed in v9.8.	Not applicable	Not applicable

Table 3. Enterprise Server or VE v9.7 - Data Guardian Default Policy Value Changes

Technology Group	Policy	Previous Default Value	New Default Value
Data Guardian	Enable Callback Beacon	Selected	Not Selected

Endpoint Security Suite Enterprise Default Policy Changes

The following Endpoint Security Suite Enterprise policies' default values are changed.

Table 4. Security Management Server or Security Management Server Virtual v9.8 - Endpoint Security Suite Enterprise policy changes

Technology Group	Policy	Previous Default Value	New Default Value
Advanced Threat Prevention	No policies' default values changed in v9.8.	Not applicable	Not applicable

Table 5. Enterprise Server or VE 9.7 - Endpoint Security Suite Enterprise policy changes

Technology Group	Policy	Previous Default Value	New Default Value
Advanced Threat Prevention	Memory Actions - Exclude Executable Files	\Windows \System32\CmgShieldService.exe \Windows\System32\EMSService.exe	\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

Technology Group	Policy	Previous Default Value	New Default Value
			\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

Technology Group	Policy	Previous Default Value	New Default Value
			\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

Technology Group	Policy	Previous Default Value	New Default Value
			\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

Technology Group	Policy	Previous Default Value	New Default Value
			\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

Technology Group	Policy	Previous Default Value	New Default Value
			\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