Dell Security Management Server

Technical Advisories v11.18

March 2026
Rev. A01

DELL Technologies

Notes, cautions, and warnings

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

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

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

Contents

1

Dell Security Management Server Technical Advisories

Contact Dell ProSupport for Software

Before contacting Dell Support, run SupportAssist for a quick self-diagnostic test. Run SupportAssist Quick Test.

For additional assistance, visit dell.com/support. Online support at dell.com/support provides access to drivers, manuals, technical advisories, FAQs, and information on emerging issues.

When contacting Dell Support, keep your Service Tag or Express Service Code ready. This helps route your request to the appropriate technical expert quickly.

For international contact details, see Dell ProSupport for Software international phone numbers.

New Features and Functionality v11.18

Dell systems with Intel Core Ultra Series 3 processors with vPro are currently not compatible with DDPE. On these systems, Intel Total Storage Encryption (TSE) is enabled by default in the BIOS and is therefore also enabled in Windows.

When TSE is enabled, Pre-boot Authentication (PBA) activation fails. As a result, DDPE installation on these systems is blocked until the incompatibility is resolved.

Workaround: If DDPE installation is required, disable Intel TSE in the BIOS, reinstall the Windows operating system, and then install and activate DDPE.

Resolved Technical Advisories v11.18

Resolved Security Advisories

- Not applicable.

Resolved Technical Advisories

- Not applicable.

Technical Advisories v11.18

Not applicable.

New Features and Functionality v11.10

- Increased the Core server proxy memory to 1024 from 384.
- Upgraded the Encryption Enterprise installer to fix the security vulnerability issue.
- Added new policies such as Enable Certificate Pinning and Server Certificate Public Key Hash under the PBA Advance Settings.
- Upgraded the Wix version to 4.0.5 in Server installers.

- Upgraded the Jetty Version to 9.4.54 in DDP Server.
- Migrated Java to 8u391 in DDP Server.
- Migrated Java Spring version to 5.3.31.

Resolved Technical Advisories v11.10

Resolved Security Advisories

- An issue is resolved where the PostgreSQL is upgraded to latest 16.2 version to protect Dell Encryption from High Severity Security Vulnerability. [DDPS-11091]

Resolved Technical Advisories

- Not applicable.

Technical Advisories v11.10

- Not applicable.

New Features and Functionality v11.9

- Bug fixes to improve user experience.
- The Encryption Enterprise is enhanced to email the scheduled reports in CSV format along with the default XLSX format.

Resolved Technical Advisories v11.9

Resolved Security Advisories

- An issue is resolved where the Apache Active MQ version is upgraded to the latest version to protect Dell Encryption from High Severity Security Vulnerability. [DDPS-11005]

Resolved Technical Advisories

- An issue is resolved where the Dell Encryption support page navigates you to the US chat support article instead of the Dell Data Security International Support Phone Numbers page. [DDPS-9730]
- An issue is resolved where incorrect data is displayed in the application properties of Dell Security Management Server Virtual. [DDPS-10919]
- An issue is resolved where a temp folder is created during the Dell Encryption installation as the Access Control List is not configured properly. [DDPS-11027]

Technical Advisories v11.9

- Due to weak Access Control List, Dell Encryption Installer allows you to change the default installation path to any non-restricted folder and complete the installation. [DDPS-10995]

New Features and Functionality v11.8.1

- Bug fixes to improve user experience.

Resolved Technical Advisories v11.8.1

Resolved Security Advisories

- An issue is resolved where the Dell Encryption Installer does not verify if Symlink is available in the ProgramData folder, resulting in creation of random files. [DDPS-10994]

Resolved Technical Advisories

- No technical advisories exists.

Technical Advisories v11.8.1

- No technical advisories exists.

New Features and Functionality v11.8

- Upgraded the EE and VE Open SSL from 0.9.8.11 to 1.1.1.

Resolved Technical Advisories v11.8

Resolved Security Advisories

- No security advisories exists.

Resolved Technical Advisories

- No technical advisories exists.

Technical Advisories v11.8

- When upgrading Dell Security Management Server Virtual that is in disconnected mode, an additional key file is needed. While upgrading, contact Dell support center for assistance. For more information, see Dell Data Security International Support Phone Numbers.

New Features and Functionality v11.7

New features and functionality include:

- Upgrades
- Management Console
- Management Console policies

Upgrades

- The Jetty version running on the Dell Security Management Server has been migrated to 9.4.50.v20221201.

Management Console

- An error message now lists all the requirements for the superadmin password when the administrator attempts to update the password to a value that does not meet those requirements.

Management Console policies

- An issue is resolved with the *User PIN lifetime* policy so that the administrator can enter *0* days.

Resolved Technical Advisories v11.7

Resolved Security Advisories

- The Dell Security Management Server v11.7 includes a security update addressing an OpenSSL vulnerability (OpenSSL CVE-2022-3602).

Resolved Technical Advisories

- Changes have been made to reduce the database size.
- Inventory processing has been improved.
- In the Management Console for BitLocker Manager, *Endpoint Detail > States > Last Seen in System*, an issue is resolved so that all timestamps reflect the appropriate time zone. [DDPSUS-3237]
- An issue is resolved with the *User PIN lifetime* policy so that the administrator can enter **0** days. [DDPS-10857]

Technical Advisories v11.7

Management Console

- In *Client Firewall > Settings and Rules*, the *OK* button is now activated only after the administrator makes valid updates. See *Populations > Enterprise > Security Policies > Threat Prevention > Client Firewall (On) > Show advanced settings > Firewall settings*. [DDPS-10788]

New Features and Functionality v11.6

New features and functionality include:

- Management Console
- Management Console policies

Management Console

- The Recovery Server now allows for curly brackets {} in the Recovery ID field.

Management Console policies

- In *Advanced Windows Encryption > BitLocker Encryption > Operating System Volume Settings*, the *PIN Prompt Delay* policy is new. This policy allows administrators to set the number of minutes to delay the *BitLocker PIN prompt* before it is displayed to the user.
- *Authentication > Pre-Boot Authentication* has the following:
  - The *Cached PIN User Login Attempts Allowed* policy allows the administrator to specify the number of times that a cached PIN user can attempt to log in.
  - The *Number of Characters Required in PIN* policy allows the administrator to configure the minimum PIN length for PBA authentication. Options can be 4 to 126 characters.
  - The *Authentication Method* policy now has a *Password+PIN* value. However, for v11.6, the Password+PIN value is being revised so avoid use until further notice.

Resolved Technical Advisories v11.6

Resolved Security Advisories

Management Console

- An issue is resolved with saving the *Firewall settings* in the *Advanced Threat Prevention > Client Firewall* policy. [DDPS-10782, DDPSUS-3193, DDPSUS-3195]

Resolved Technical Advisories

- The Dell Security Management Server now accepts appropriate wildcards for the client firewall. [DDPS-10400]
- An issue is resolved so that the encryption client now activates when using the front-end Security Server proxy. [DDPS-10655, DDPS-10741]

Technical Advisories v11.6

- No technical advisories exist.

New Features and Functionality v11.5

New features and functionality include:

- Management Console
- Management Console policies
- Dell Server

Management Console

- The administrator can manually set the BitLocker Managed PIN on a device at the *Enterprise*, *Endpoint Group*, or *Endpoint* level to ensure that access to a device is restricted to only individuals who know the PIN. The administrator can later update the PIN with a new value or reset it to nothing. When the value is empty, no Managed BitLocker PIN is forced or sent to the client.
- In *Endpoint Groups > Details and Action*, for devices that are protected with SED or FDE, the administrator can now select **Lock**, **Unlock**, and **Remove Users**. The *Group Type* can be *Rule Defined, Admin Defined, or Active Directory*.
- When the administrator modifies the Multi-factor authentication (MFA) state in *Users* or *User Groups*, the administrator can go to **Management > Log Analyzer** and select **Admin Actions** from the *Category* field. The *Message* column displays what changed, the administrator role that performed the action, and the Google auth resets. [DDPS-10438]
- On the *Endpoints > Endpoint Detail* screen > *States > Protection Status* section for each disk, a column has been added for the *Disk Serial Number*. This number is for the protected volumes for a specific device.

Management Console policies

These policies in *Advanced Windows Encryption > BitLocker Encryption - Operating System Volume Settings* have changed:

- The *User PIN lifetime* policy value is now in days, not hours. The default setting is 90 days.
- The *User PIN lifetime* policy now allows for a value of 0 to be set. This value represents to the endpoint that a PIN rotation is not required on the device.

Dell Server

- The `application.properties` file now contains default timeout and warning properties for the Management Console. The administrator can modify these values to lengthen or decrease the warning time and the timeout. Default values are:
  - `idle.warn.seconds=1080`
  - `idle.timeout.seconds=1200`
- Encryption Enterprise v11.5 contains updates to third-party dependencies.
  - Full Disk Encryption v11.5 or later requires the Dell Security Management Server v11.5 or later to maintain client and server communication.
  - SED Manager v11.5 or later requires the Dell Security Management Server v11.5 or later to maintain client and server communication.

- The default value of `ssos.domainadmin.verify` has been changed to **false** to allow the administrator to properly register SSOS and to reduce troubleshooting.

Resolved Technical Advisories v11.5

Resolved Security Advisories

To resolve security issues, the following have been updated.

- The SSL and TLS cipher list has been updated.
- Java has been updated to version 1.8.0.291.
- Spring Framework has been updated.
- JQuery that is used for the Dell Security Management Server console has been updated to version 3.5.0. [DDPS-10516]

Technical Advisories v11.5

New Features and Functionality v11.4

Management Console

- Self-Encrypting Drives and Dell's software-based Full Disk Encryption now support Multi-Disk encryption, allowing administrators to protect all fixed disks on endpoints that contain either all Self-Encrypting drivers or all traditional disks. These policies are available at the Enterprise, Endpoint Group, and Endpoint levels.

  In the *Advanced Windows Encryptions* technology group, FDE policies are:
  - Encrypt all Self-Encrypting Drives (Multi-Disk)
  - Multi-Key Encryption (Multi-Pass)
  - Encrypt Used Space First (Multi Sweep)

  In the *Advanced Windows Encryptions* technology group, the SED policy is:
  - Encrypt all Self-Encrypting Drives (Multi-Disk)

- Multi-factor authentication is now available in the **Management Console > User Admin** and **User Group Admin**. This option displays for super administrator and account administrator roles.
- In **Management > Notification Management**, a *Configure SMTP* tab has been added to allow the administrator to quickly configure and test SMTP settings within the Management Console.

Resolved Technical Advisories v11.4

Management Console

- In *Populations, Domains > Settings tab > Passwordless Authentication*, an excessive log output is resolved. This excessive output occurred in rare situations when Passwordless Authentication was not properly configured.
- An issue is resolved in **Advanced Threat Prevention > Client Firewall** policies to allow for wildcards in the *DNS Blocking* setting. The administrator can specify all domains higher, for example **.dell.com*, instead of just the domain name. [DDPS-10433]
- In *Managed Reports*, an issue is resolved so that administrators can modify the csv.export.maxsize property for the number of rows, and the property value is no longer ignored. [DDPS-10441]
- In *Managed Reports*, an issue is resolved so that administrators can modify the email.export.maxsize property for the maximum number of rows to export to email for scheduled reports, and the property is now properly consumed by the Server. [DDPS-10442]
- A missing policy ID is resolved so that a fresh install of the Server on Windows no longer logs errors on policy templates after a commit. This relates to the *User PIN lifetime* policy in *Advanced Windows Encryptions > Bitlocker Encryption > Operating System Volume Settings*. [DDPS-10451]
- For multi-factor authentication, the tooltips clarify that the OTP must have a maximum of six characters in the *Dell Data Security* field and *Configure Google Authenticator* field. [DDPS-10458]

- An issue is resolved with the default configuration so that the Security Server now starts. [DDPS-10571]

Technical Advisories v11.4

- The input fields for domain configuration have been restricted to only allow for a hostname to be set. Direct distinguished name lookups have been removed to avoid LDAP lookup failures. [DDPS-10388]

Management Console

- When Multi-Factor Authentication is set to send an email, the email attribute must be set for the user within Active Directory. [DDPS-10363]
- The *User PIN lifetime* policy in *Advanced Windows Encryptions > Bitlocker Encryption > Operating System Volume Settings* does not currently allow for a disabled value. [DDPS-10450]

New Features and Functionality v11.3

- Dell Encryption on server operating systems now supports Windows Server 2022 Standard and Datacenter editions.
- The log4j libraries have been updated to versions unaffected by recently disclosed vulnerabilities such as CVE-2021-44228.
- The Compliance Reporter has been removed from the Security Management Server. Manage Reports now handles the functionality that was previously performed with Compliance Reporter.
- In the Server Configuration Tool, when the administrator imports a certificate, a dialog confirms that the certificate import was successful.
- DiagnosticInfo collects additional information including:
  - Class filter drivers in use
  - Dell Data Security product versions
  - Hardware serial numbers
  - Installed servers and their availability status
  - Windows build versions
  - Logs for the following:
    - Component-Based Servicing
    - Installed applications
    - Deployment Image Servicing and Management
    - Security Management Server installation
    - Server Configuration Tool and server migration
    - Threat Defense
    - VMware Carbon Black
    - Windows Updates

Management Console

- In **Management > Services Management > Events Management** tab, a checkbox allows the administrator to disable or enable the *Advanced Threats* and *Advanced Threat Events* tabs.
- The default value for the policy, *Use Hardware-Based Encryption for Operating System Drives*, is now disabled or cleared for new installations. The policy is in *Advanced Windows Encryption > BitLocker Encryption - Operating System Volume Settings*.

Resolved Technical Advisories v11.3

- The Windows Port Control Policy icon properly updates to match the primary policy switch value.
- When logging in to the Management Console, if an administrator specifies http:// instead of https://, the system automatically redirects. [DDPS-10071]

Technical Advisories v11.3

- No technical advisories exist.

New Features and Functionality v11.2

- Jetty has been updated to 9.4.43.

Management Console

- A policy name changed in *Advanced Windows Encryption > BitLocker Encryption*. *Disable BitLocker on Self-Encrypting Drives* is now *Block BitLocker when other Dell Encryption policies are present*.
- In *Advanced Windows Encryption > BitLocker Encryption > BitLocker Encryption > Operating System Volume Settings*, a new policy forces users to reset their PIN in case the PIN has been compromised. The User PIN lifetime policy sets the duration of the BitLocker PIN lifetime before recreation of the PIN is required. The value is in hours, and the default value is 2160.
- In *Manage Reports > EMS Event* report, the per-device Plug and Play identifier (PNPDeviceID) is now present.

Resolved Technical Advisories v11.2

- An issue is resolved so that if the Server Hardware ID contains blank spaces, the Server does not activate. [DDPS-10277]

Management Console

- An issue is resolved so that administrators can modify policies with dropdown menus and save them. *Save* no longer results in an *Error Validating Policy* dialog. [DDPS-10225]
- An issue is resolved so that all columns display in the *Manage Reports* page > *Device Detail* report. [DDPS-10229]
- An issue is resolved in *Populations > Users > User Detail > Endpoints*, so that the administrator can now select the number of items per page to display. [DDPS-10258; DDPSUS-30249]
- On the *Manage Reports* page > Endpoint Groups, a column now allows administrators to view all the Endpoint Groups in which an endpoint is a part. Records can be filtered based on the Endpoint Group name. [DDPS-10261]
- For the Server Configuration Tool, the keytool syntax is corrected so administrators can now import an internally signed certificate and no errors appear in the logs. [DDPS-10267]
- In Threat Prevention > Client Firewall Rules, an issue is resolved so that custom ports defined for TCP or UDP can be saved or committed. [DDPS-10268; DDPSUS-3030]
- In *Populations > Enterprise > Advanced Threat* tab, Threat files can now be downloaded. [DDPS-10275]

Technical Advisories v11.2

- No technical advisories exist.

Resolved Technical Advisories v11.1.1

- For enterprises that use the EMS Device Allowlist policy, this patch release resolves an issue where modifying that policy blocks any policy updates, particularly if those additional policies have a dropdown menu. To identify this as the issue, view the additional policy change in the Log Analyzer. The log for the additional policy lists the contents of the EMS Device Allowlist policy instead of the additional policy setting. [DDPS-10225]

New Features and Functionality v11.1.0

- In the Endpoint Detail pages in the Management Console, the administrator can now search on Hardware ID.

Technical Advisories v11.1.0

- Currently, with the Dell Server, a scenario occurs where large policies, such as large SDE, Common, or User PBE rule sets or many EMS allowlist items, are not able to make it to the Dell Encryption clients. [DDPSUS-2980, DDPC-12553]

Resolved Technical Advisories v11.1.0

- On the Dashboard of the Management Console, the Advanced Threat Protection Events are now correctly redirecting to their appropriate Detail pages. [DDPS-10135]
- EMS Device Allowlist entries are now converted to uppercase letters so that what displays in the logs matches what must be applied. [DDPS-10169]
- An issue during activation of the Encryption Client is resolved so that the Hardware ID check validates adequately. [DDPS-10174]

Resolved Security Advisories v11.1.0

- Strict-Transport-Security header (HSTS) headers are now presented from the Dell Server, enforcing HTTPS communication for all traffic. [DDPS-10140]
- The Jetty version running on the Dell Server has been migrated to 9.4.39.v20210325. This version prevents being susceptible to a vulnerability after receiving an invalid large TLS frame. [DDPS-10147, DDPS-10150]

New Features and Functionality v11.0.1

- For Passwordless Authentication and information about configuring Dell Encryption Enterprise to authenticate with Windows Hello, see KB article 188216.

Management Console

- In *Populations* > *User Groups*, after clicking a group name and selecting the **Members** tab, the administrator can now click an **Export File** button to export the list of members within a User Group. This option allows the administrator to cross-compare and then leverage that to build a list for an admin-defined user group. This export option provides details under *User*, *Distinguished Name*, and *Common Name* columns.
- In *Populations* > *Endpoint Groups*, after clicking a group name and selecting the **Members** tab, the administrator can now click an **Export File** button to export the list of endpoints within that endpoint group. This option allows the administrator to cross-compare against other utilities, build additional admin-defined user groups, and export lists of endpoints to a third-party systems management utility like SCCM. The export provides data in the *Category (OS Type)*, *Hostname*, and *OS/Version* columns.
- In the *Dashboard* > *Endpoint Protection Status* screen, to facilitate identifying protection gaps, the administrator can now select an option and click an **Export File** button. This option exports the list of endpoints that are present within the *Protected*, *Not Protected*, or *Total* listing of endpoints. Data displays in the *Platform*, *Endpoint ID*, *Protected Status (Yes/No)*, *Shield Inventory Received*, *Shield Inventory Processed*, *Agent Inventory Received*, and *Agent Inventory Processed* columns.

Technical Advisories v11.0.1

- No technical advisories exist.

Resolved Technical Advisories v11.0.1

- No resolved technical advisories exist.

Resolved Security Advisories v11.0.1

- The PostgreSQL version has been updated to 11.12, resolving several security vulnerabilities, including CVE-2019-10164. [DDPS-10148]

New Features and Functionality v11.0.0

- New Passwordless authentication for the users who are using Windows Hello Authentication. In the *Management Console > Domains > Domain Settings*, additional fields provide configuration for ADFS or Microsoft Azure. [DDPS-9969, 10067]
- Server code migration to Visual Studio 2019.

Resolved Technical Advisories v11.0.0

- An issue is resolved with an HTTP option method not being properly set, that had resulted in false-positives within vulnerability scanners when the Server was scanned. [DDPSUS-2944]
- The Portuguese documentation now displays properly in the Help menu. [DDPS-9960]
- Modified language to move to a more inclusive syntax. [DDPS-10031]
- Copyrights have been properly updated to 2021 for the Server. [DDPS-10060]
- IPv6 address approvals are now being properly retained for the Denial-of-Service filter. [DDPS-10133]
- **Management Console**:
  - The Device Detail report export was failing due to DoS filter thresholds. This issue has been resolved. [DDPS-10050]
  - Several performance improvements have been implemented for Searches within the Management Console. [DDPS-10065]
  - BitLocker keys are now properly populating by default. [DDPS-10085]
  - In *Services Management > Events Management* tab, an *Enable Threat Events* checkbox ensures that the Threat Events tab displays in *Populations > Enterprise* or *Populations > Endpoints > Details & Actions tab > Endpoint Detail*. Under the Threat Events tab, Web Protection and Client Firewall are listed under the Threat Prevention group. [DDPS-10095]
  - An issue is resolved so that when attempting to load an existing domain within the Dell Security Management Server running 11.0.0, the existing domain no longer fails to load. [DDPS-10114]
  - The *Domain Settings* page now properly reflects the appropriate LDAP connection URL when Secure LDAP (LDAPs) is in use. [DDPS-10117]

Resolved Security Advisories v11.0.0

- No security advisories exist.

Technical Advisories v11.0.0

- Added 6/2021 - After policy are committed, an issue with Jetty changes within the Message Broker service result in failures to delivery policy to the Policy Proxy services. Thus, the Encryption Client may not receive the latest policies. [DDPS-10171]

New Features and Functionality v10.2.14

- With a global shift to inclusive language, several terms and expressions have been updated.
- Lengthy lists of policies within policy groups have been restructured to improve readability and access. [DDPS-9667]
- For the Dell Data Security - Self-Service Recovery Portal tool's *Recovery ID* field, a dialog displays with *Invalid Recovery Id* if an administrator enters a space or any special characters apart from underscore or hyphen.

Resolved Technical Advisories v10.2.14

- For the Recovery Portal, an issue is resolved where the portal automatically logs out when an administrator enters a space or any special characters apart from underscore or hyphen in the Recovery ID field and then clicks Get Recovery Password. [DDPS-9968]
- **Management Console**:
  - Administrators can now enter custom ports with Client Firewall policies. [DDPS-9779]
  - Importing devices into an Admin-Defined Endpoint Group is no longer case sensitive. [DDPS-9967]

- A display issue has been resolved so that the LDAPs notation now properly updates the Directory URL in the Domain Settings tab to display LDAPS when a Secure LDAP connection is being leveraged. [DDPS-9984]
- For Managed Reports, users no longer receive duplicate scheduled report emails when multiple recipients are defined. [DDPS-10015]

- **Recovery Portal**
  - The Log Analyzer now displays logins through the Recovery Portal separately from logins to the Management Console. [DDPS-9941]

Resolved Security Advisories v10.2.14

- No security advisories exist.

Technical Advisories v10.2.14

- When logging in to the Self-Service Recovery Portal with a SAM-Account name (domain\user), an error displays. The workaround is to log in with the UPN (user@domain.com). [DDPS-9974]
- Currently, when a BitLocker Recovery is performed in the Management Console, braces are automatically set in the Recovery ID field. A dialog states *Invalid Recovery ID*. The workaround is to remove the braces from the GUID in the Recovery ID field. [DDPS-10085]

New Features and Functionality v10.2.13

- A web-based portal, the Dell Data Security - Self-Service Recovery Portal tool that is hosted by the Dell Security Management Server, allows administrators with specific roles to recover devices that are managed by BitLocker. Roles include Self-Service Recovery, System, Security, and Help Desk administrators.

Resolved Technical Advisories v10.2.13

- In the Security Server, SSOS activation is no longer failing for v 10.2.11 and later. [DDPS-9843]
- An issue has been resolved so that the Server Configuration Tool is now updating service configuration files and the files are properly signed. [DDPS-9904]
- **Management Console**:
  - Null Pointer Exception handling has resolved an issue where a blank search or search for a specific device returns NaN for the number of endpoints. Now, information displays. [DDPS-9769, DDPS-9910]
  - An issue has been resolved for a user in a User Group with the role of Report Administrator, Report Owner, and Report User. After logging in, the user with those roles can now view the Dashboard. [DDPS-9773]
  - On an *Endpoint Detail page > Users tab*, the *User, Last Successful Login*, and *Last Unsuccessful Login* columns can now be sorted. [DDPS-9819]
  - On the *Recover Data* page in the *TPM > Hostname* field, an issue is resolved. If an administrator enters a space only, the buttons are not enabled. [DDPS-9829]
  - For email configuration, support was added for Anonymous Auth and an issue was resolved related to TLS-enabled authentication. Now, sending email, notifications, and periodic reports works as expected. [DDPS-9832]
  - In *Populations > Users*, the sorting arrow in the *Last Reconciled* column now displays. [DDPS-9833]
  - An issue has been resolved so that Notification Summary email messages now link to the Management Console. [DDPS-9908]
  - An issue has been resolved so that, after an upgrade, the Endpoints page now lists the endpoints. [DDPS-9910]
  - On the Domain Settings tab, an issue has been resolved so that if the administrator selects the Secure LDAP check box and saves changes to the domain settings, no internal error displays. [DDPS-9911]
  - An issue has been resolved so that the *Shield Detail* page in Manage Reports can filter and data is returned. [DDPS-9915]
  - An issue has been resolved so that the *Device Detail* report can be exported. [DDPS-9983]

Resolved Security Advisories v10.2.13

- No security advisories exist.

Technical Advisories v10.2.13

- **Management Console**:
  - Currently, when the administrator performs a mass import to an administrator-defined Endpoint Group and case does not match exactly, the import fails. [DDPS-9967, DDPSUS-2891]
- **Recovery Portal**:
  - Currently, if an administrator copies the logged-in URL of the Recovery Portal and pastes it in another browser, the administrator is not prompted to log in again. [DDPS-9961]
  - Currently, if logging in on same the browser as superadmin to the Management Console and then on a separate tab to the Recovery Portal, an Access Denied dialog displays. The work around is to log out and then log in on separate browsers or to log in first to the Recovery Portal. [DDPS-9965]

New Features and Functionality v10.2.12

- Cryptographic Next Generation certificates are now supported.
- For customers who have purchased VMware Carbon Black and Dell Encryption per-device from Dell, support is now available for on-the-box entitlements.
- This functionality applies to the Management Console:
  - The legacy management console has been deprecated. The legacy login and corresponding URLs are no longer available.
  - Microsoft Edge (Chromium) is supported.
  - For newly deployed Security Management Servers, the *Sync Users at PBA Activation* policy in the *Pre-Boot Authentication* policy group is now enabled by default to sync all active user accounts to the PBA during activation. This helps to ensure that users can log in after PBA activation and reduces occurrences where users must perform a manual recovery.
  - In *Windows Encryption* > *BitLocker Encryption*, the *Disable BitLocker on Self-Encrypting Drives* policy has been renamed to *Block BitLocker when other Dell Encryption technologies are present*, and the hover text has been clarified.
  - The Device Detail report in *Reporting* > *Manage Reports* > *Create New Report* > *Device Detail*, contains a new column titled *Enabled Technologies*.

Technical Advisories v10.2.12

- Currently, Server Encryption devices may fail to activate after a Server is upgraded to 10.2.11 or later. Existing devices remain encrypted. [DDPSUS-2839, DDPS-9843, DDPC-12115]

Resolved Technical Advisories v10.2.12

- **Management Console**:
  - On the *Endpoint Detail page* > *Details & Actions* tab, the *States* section now displays only the disks present in the last inventory that is received from the endpoint. Historical data regarding disks is retained but no longer displays. [DDPS-4239]
  -
  - On the *Endpoint Detail page* > *Details & Action tab* > *Plugins & Agent* section > *Endpoints Plugin* column, a hover text description has been added for each *Plugins & Agents* column value. [DDPS-5580]
  - In *Endpoint Detail* > *Details & Action* > *Plugins & Agent*, only those plugins from the last check-in on the endpoint display. The plugins displayed change when the plugin's state is changed from **any State (Active, Available)** to **Not Present** or the reverse. [DDPS-7421]
  - In *Management* > *Services Management* > *Events Management*, when enabling the *Export to Local File* check box under *Export Events to a SIEM System*, the administrator must now enter an absolute path in the *File Location* field in order to save preferences. [DDPS-9616]
  - With SQL authentication, when modifying the database settings in the Server Configuration Tool, the database password is now written to disk in encrypted form rather than in cleartext. Previously the database password was encrypted once the services started. [DDPS-9627]
  - The Security administrator now has access to the Log Analyzer. [DDPS-9701]

- An issue has been resolved where, after an update, notification email messages would not properly send if **ALL** was selected for the TYPE and PRIORITY, resulting in an incorrectly NULL filter field. This field is now be properly handled, and the notification is sent. [DDPS-9725]
- An issue where the Manage Report's Shield Detail report would time out with a large number of endpoints and when pulling during peak hours has been resolved. [DDPS-9727]
- An issue has been resolved so that if a Server is encrypted and a sweep has completed, the Protected Status and Date display in the Management Console. [DDPS-9757]
- An issue has been resolved where administrators in roles with insufficient access to see the *Management > Recover Endpoint* page will no longer be able to click the link then get logged out. The link only displays to administrators whose roles include recovering endpoints. [DDPS-9772]
- On the *Endpoint Details > Details & Actions* page, sorting is now working in the Server Device Control section of applicable endpoints. [DDPS-9800]
- In *Populations > User Groups > Edit Priority > Modify User Groups Priority Page*, sorting the priority column is now disabled, which is the previous behavior. [DDPS-9802]
- An issue has been resolved where, in rare situations, Threat Protection licenses were consumed when Advanced Threat Prevention was also installed. [DDPS-9808, DDPSUS-2816, DDPSUS-2590]

Resolved Security Advisories v10.2.12

- No security advisories exist.

New Features and Functionality v10.2.11

- SQL Server 2019 is now supported.
- Microsoft Edge is now supported.
- The Security Management Server may have issues with UI elements for Internet Explorer 11. Due to the lack of support for modern web engines, Internet Explorer 11 will no longer be supported.
- The Security Management Server is compatible with the Microsoft requirement for LDAP channel binding and LDAP signing when Active Directory is in use.

  To enable this requirement on the Security Management Server, you must have the root issuing certificate for the domain controller certificates that are imported into the "Trusted Root" store within the Microsoft Certificate Key Store.
- Licenses purchased on-the-box can now be bulk-inserted with a .csv file. To obtain this file, contact your Dell Security sales representative or Dell Security support.
- The Security Server service now automatically adds the Server local IP addresses to ipWhitelist on service startup.
- Management Console:
  - For **Management > Commit Policies**, the embedded help now also includes content for *View Pending Commit(s)*.
  - On the Endpoints page, the PBE and Manager columns are no longer included as part of the endpoint information. An *Enabled Technologies* column now displays all the plugins that are enabled on the endpoint.
  - The EMS Device Whitelist field now accepts a maximum of 150 characters per line and 500 lines.

Resolved Technical Advisories v10.2.11

- The Encryption recovery file that is downloaded from the Security Management Server is no longer wrapped inside an executable file and does not require running a command to extract it. [DDPS-5054]
- The APNS (Apple Push Notification Server) database tables, which are used for iOS device support, have been removed. [DDPS-9453]
- The MDM (mobile device support) database tables have been removed. [DDPS-9454]
- When sending an email through JavaMail in the **Management Console > Notification Management** page, the Console sends the email as anonymous. Updating to the latest version of JavaMail resolved the issue. [DDPS-9494]
- The password used when downloading an endpoint recovery bundle is no longer written in cleartext in output.log file from the Security Server logs when in debug mode. [DDPS-9541]
- In the **Management Console > Notification Management** page, the *Send Test Email* dialog now displays the correct information. [DDPS-9542]
- Due to product deprecation, the `cloud-profile-updater. properties` file has been removed from `'/opt/dell/server/security-server/conf'` and `'/opt/dell/server/security-server/bin'`. [DDPS-9544]

- In the **Management Console > User Groups**, when an administrator tries to grant to a group a higher administrator role than the administrator account itself possesses, an *Access Denied* message displays rather than an *Internal Error* message. [DDPS-9548]
- When updating a Security Management Server's certificate using the **Advanced Configuration > Server Certificates > Create and Install Self-Signed Certificate** option, the system updates the *signingcertificate* table as expected. [DDPS-9549]
- If the Management Console times out and cannot connect to the Security Management Server, a more descriptive *Connection Refused* dialog now displays. Clicking **OK** redirects the user to the login page. [DDPS-9557]
- In the **Security Management Server > DMZ Server Support** field, the Host Name field now accepts any valid FQDN or hostname including those that begin with a number. [DDPS-9561, DDPS-9561]
- Threat Events are now sortable within an individual Endpoint. [DDPS-9568]
- Selecting the option to Bypass for an Endpoint Group now appropriately displays a confirmation dialog. [DDPS-9596]
- An issue where the Effective Policy for an Endpoint or a User would not properly update has been resolved. [DDPS-9621]
- An issue where the Encryption Failure View was not loading within the Security Management Server has been resolved. [DDPS-9622]
- Administrators with the Security Administrator role can now properly Remove and Add Endpoints to Groups within the Security Management Server. [DDPS-9626]
- The Threat Protection Status widget on the Dashboard now properly displays the color indicator per Threat Category. [DDPS-9634]
- The Device ID now links to the endpoint within the *Threat Events* tab. [DDPS-9640]
- When connecting to the Cylance server in the **Management Console > Advanced Threats** tab, a wait message no longer displays. [DDPS-9650]
- In the **Management Console > Management > Services Management > Events Management**, an issue has been resolved where the Security Server logs displayed recent events but would not export events when an unexpectedly older event was discovered. [DDPS-9662]
- Administrators with the Help Desk role can no longer remove endpoints that are presented within an endpoint's *Details and Actions* tab. [DDPS-9698]
- Advanced Threat Events once again can search by hostname or SHA256 hash. [DDPS-9710]

Resolved Security Advisories v10.2.11

- Several Java-based vulnerabilities have been resolved. [DDPS-9101, DDPS-9332]

  Updates are to these versions:
  - Java Version: 1.8.0.241
  - Jetty Version: 9.4.25
-

Technical Advisories v10.2.11

- In the Management Console, if endpoints display without Serial Number, the administrator must set the following:
  - `UseBiosSerialNumber` entries within the InventoryObjects.config (in Core Server for Encryption Enterprise; in Core Server and Inventory Server for Virtual Edition)
  - DeviceInventoryQueueProcessor
  - AgentInventoryQueueProcess

  The client and the agent must then update to use the *AssetTag* field instead of the *Serial* field that is stored in `DeviceData:UseBiosSerialNumber` entries. [DDPS-9619]
- Log Analyzer does not have the ability to filter using a start and end time. [DDPS-9637]
- Report emails scheduled through the **Management Console > Reporting > Manage Reports** feature do not localize the email subject properly for Japanese and Korean languages. [DDPS-9643]
- Currently, the **Uncommitted Policy Changes** notification displays to administrators whose roles do not have permission to commit policy. If they try to commit the outstanding policies, these administrators are logged out of the Management Console. [DDPS-9702]
- In the Management Console, MDM databases have been removed. Therefore, the Endpoints page lists an error: `Exception thrown in webservice controller java.lang.RuntimeException: NOT IMPLEMENTED: MDM_DEVICE`. Currently, this issue will not be fixed. [DDPS-9729]

New Features and Functionality v10.2.10

- The Security Management Server is improved through various security fixes and enhancements. See Resolved Security Advisories v10.2.10 for additional information.
- LDAP query responses are hardened in the Security Management Server.
- The Security Management Server is now signed by a SHA256 signing certificate as the SHA1 signing certificate is deprecated
- The Sync Users at PBA Activation policy is now enabled by default.
- The Security Management Server is now built with InstallShield 2019.
- The Security Management Server v10.2.10 now supports VMware ESXi 6.7
- *First Seen in System* and *Last Seen in System* columns have been added to **Populations > Endpoints > Details and Actions** for each disk in the selected endpoint.
- When communicating to the Cylance SaaS, delays in communication are presented with the following message:

  Attempting to connect to Cylance at this time. Please Check back in a bit.

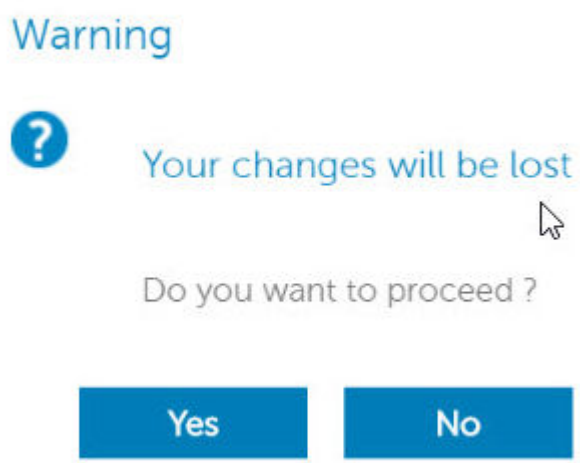
- On upgrade, all users are reconciled by the Security Management Server to ensure all groups and users are accurately reflected in the Management Console.
- The now attempts to clean up the audit database by default and adheres to 80% of the 10 GB assigned database size. This cleaning action prevents critical errors displaying in the *Dashboard Notifications* pane, which previously detailed that the Audit Database exceeded its 95% size limitation.

  The **auditdb.size.NotificationPercentage** property is now included in**Application.properties** of the Security Server to manage the size of the Advanced Threat Prevention Audit database.

  The **auditdb.size.percentage** property is the cleanup threshold. When this percentage of the database is exceeded, after the **auditdb.clear.cron** is activated, the percentage of total space is calculated. The **auditdb.clear.cron** default value is every two hours.

  If the **auditdb.size.NotificationPercentage** value is exceeded, a notification of the cleanup displays the Security Management Server and the duration defined in **auditdb.cleanup.delete.hours** is used to clean up the data in the ddp_audit database below the **auditdb.size.percentage** threshold.

- After upgrading the Security Management Server, the following fields display the current date rather than Null:
  - Shield Activation
  - PBA Authentication
  - WebUI Login
  - User Creation in WebUI
  - Policy Proxy Sync
- When moving from one page to another, the following prompt displays if policy changes have not been saved.



Resolved Technical Advisories v10.2.10

- The Management Console's *About* page now properly displays *Disconnected Mode* when Disconnected Mode is in use. [DDPS-9369]
- PBA Device Control commands now function as expected. [DDPS-9373]
- The Management Console now times out as expected after 30 minutes of inactivity. [DDPS-9387]
- Windows Port Control now properly displays a green check mark on the Security Policy tab when enabled. [DDPS-9397]
- User privileges are now properly evaluated after any modification to membership in Active Directory. [DDPS-9401, DDPSUS-2689, DDPSUS-2702]
- The sorting function on the *Dashboard Notifications* now behaves as expected. [DDPS-9405]
- Notifications can now be dismissed as expected. [DDPS-9406]
- Removing a device from an Endpoint Group no longer results in a javascript:null webpage. [DDPS-9421]
- When the Dell PostgresSQL service is inaccessible, the following message displays:

  Cannot reach the database, please ensure the Dell PostgresSQL Service is started. [DDPS-9462]

- The *Third Party* page now properly displays all third party information. [DDPS-9476]
- BitLocker Manager's Details Report now correctly displays drive letters. [DDPS-9496, DDPSUS-2714]
- Policy Logs in the *Commit* page now return valid date and time information in Log Analyzer when using a non-English browser language. [DDPS-9514]
- Users with Administrator privileges can now create Endpoint Groups and devices can be added or removed in the *Members* pane in the Management Console as expected. [DDPS-9515]
- The Security Management Server can now be configured to allow non-domain activations. If your environment requires this activation workflow, see KB article SLN306341. [DDPS-9531, DDPSUS-2578]
- Added 12/2020 - Microsoft Edge is supported. [DDPS-9814]

Resolved Security Advisories v10.2.10

- An issue allowing remote deserialization of data through an RMI interface is resolved. For more information, see KB article SLN320536. [DDPS-9446]
- An issue resulting in users with the Account Administrator role in the Security Management Server elevating their permissions inappropriately is resolved. [DDPS-9516]
- An issue resulting in blank headers incorrectly displaying during a security scan is resolved. [DDPS-9519]

Technical Advisories v10.2.10

- In rare circumstances, unaccepted policies do not display an error. As a work around, check the Security Server logs for Invalid Values. [DDPS-9501, DDPS-9534]
- If the common name of a user is changed at the Domain Controller level, the Management Console does not reflect the new name. [DDPS-9510]
- If an existing email notification is modified then saved, the next new email notification inherits the previous notification's modifications. [DDPS-9527]
- Non-domain activations using the same hostname and username previously activated against a Security Management Server fail to activate and log the following failure in the Compatibility Server.
  `Illegal activation attempt of non-domain User`[DDPS-9531, DDPSUS-2578]
- The **Refresh** button is not available in the Management Console on the following pages:
  - Domains
  - User Groups
  - User
  - Endpoint Groups
  - Endpoint Details and Actions

  As a work around, refresh the browser. [DDPS-9532]

- After the initial activation of Advanced Threat Prevention in the Management Console, the *Advanced Threat Details* page does not properly display. As a work around, log out and back into the Management Console. [DDPS-9533]
- When recreating the self-signed certificates for the Security Management Server Virtual, the Dell Manager policy signing certificate is not recreated. As a work around, import a certificate based on a previously created certificate (see KB article

SLN302996 for more information). Alternatively, select **import an existing certificate** and choose **server.p12** for the Certificate then **server.key** for the private key. The default password for this key is `changeit`. [DDPS-9549]

- The Threat Events tab within Enterprise and per Endpoint can not currently be sorted. [DDPS-9568]
- When modifying the priority list for either Endpoint Groups or User Groups, attempting to sort by Priority in the edit phase results in an internal error message displayeding and the sort does not aupdate. Cancel the operation or refresh the page to return to the Group page. As a work around, do not sort while editing the priority list. [DDPS-9567]
- The *Uncommitted Policies* banner may persist after committing existing policy changes in the Management Console if using Internet Explorer 11 or earlier. [DDPS-9571]

New Features and Functionality v10.2.9

- Policy changes can now be viewed In Management > Commit by selecting **View Logs**. **View Logs** displays an overview of policy changes associated with the selected commit.
- New installs of the Security Management Server now listen on TLS 1.2 by default for all Java-based services, including Dell Security Server, Dell Device Server, and Dell Compliance Reporter Server. Note that the Dell Core Server is not configured by default to use TLS 1.2 on new installs to avoid introducing compatibility issues with other applications that may exist on the same server.

  Upgrading the Security Management Server does not change these by default to avoid any compatibility issues with currently connecting devices. For information on modifying the SSL/TLS accepted protocols for existing Security Management Server installs, and for information on securing the Dell Core server, a Microsoft .NET based service, see KB article SLN313386.

Resolved Technical Advisories v10.2.9

- Removing override prompts for pending policy changes now displays the correct number of changes under Uncommitted Policies. [DDPS-3974]
- The correct error message now displays when adding a domain with an invalid port number. [DDPS-6263]
- In License Management, the correct tooltip now displays when the license pool is exceeded. [DDPS-7176]
- All text now displays properly when adding or modifying Endpoint Groups or User Groups. [DDPS-7177]
- The German and French Event Managements page now properly displays. [DDPS-7249]
- Editing administrator roles in the Management Console now yields an accurate warning message. [DDPS-7300, DDPSUS-2311]
- Threat Protection licenses are now properly consumed when products are installed and deactivated. [DDPS-8925, DDPSUS-2590]
- An issue resulting in a column in Endpoint Groups not displaying is resolved. [DDPS-8832]
- Password validation no longer fails with an error if an administrator's password contains double quotations. [DDPS-8936]
- When installing the Security Management Server on Windows, the ACL service starts as expected if the administrator's password contains a backslash. [DDPS-8938]
- An issue resulting in failed certificate imports to the Security Server is resolved. [DDPS-8939]
- An issue resulting in truncated databases after an upgrade failure is resolved. [DDPS-8940]
- The Management Console now displays the correct number of protected endpoints on the Dashboard page and Endpoints page. [DDPS-8868]
- The Security Management Server installer now calculates the space required for the Postgres Audit database on the system drive. [DDPS-9059]
- An issue resulting in Digicert root not being imported after upgrading the Security Management Server is resolved. [DDPS-9246]
- In Manage Reports > Email Report Schedules, the page title now displays properly. [DDPS-9275]
- An issue caused by an incorrectly defined syslog/SIEM server in Events Management in the Management console which resulted in a loop in the Audit Event export job and excessive CPU usage is resolved. [DDPS-9307]
- An issue resulting in the *Bypass Login* command being incorrectly defined as the *Unlock* command for devices with a Pre-boot Authentication environment is resolved. [DDPS-9308]
- Encryption Technology now properly displays in the Device Detail pane when a specific endpoint is selected. [DDPS-9310]
- Modifications to syslog configuration in Services Management > Event Management is now logged in Security Server logs and Administrator Action logs as expected. [DDPS-9329]
- Advanced Threat Event Data now exports at the Endpoint level as expected. [DDPS-9327, DDPSUS-2658]

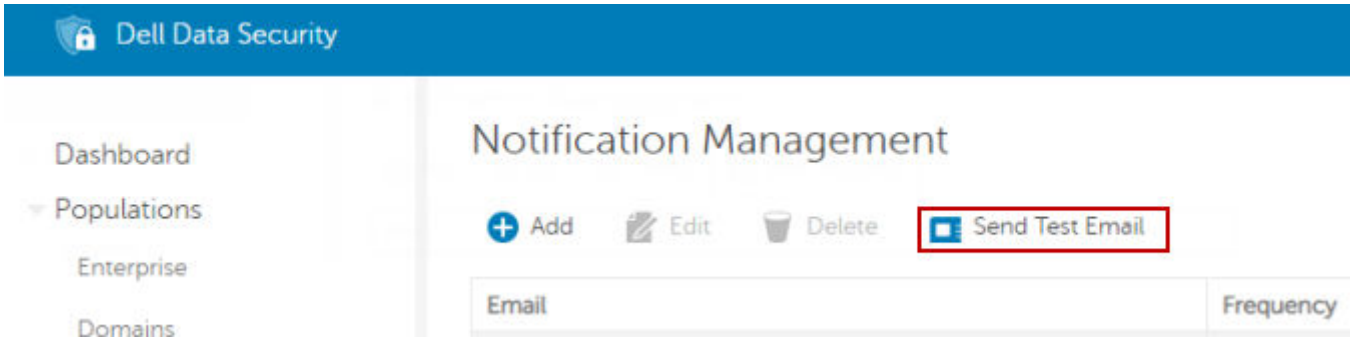
Technical Advisories v10.2.9

- No technical advisories exist.

New Features and Functionality v10.2.7

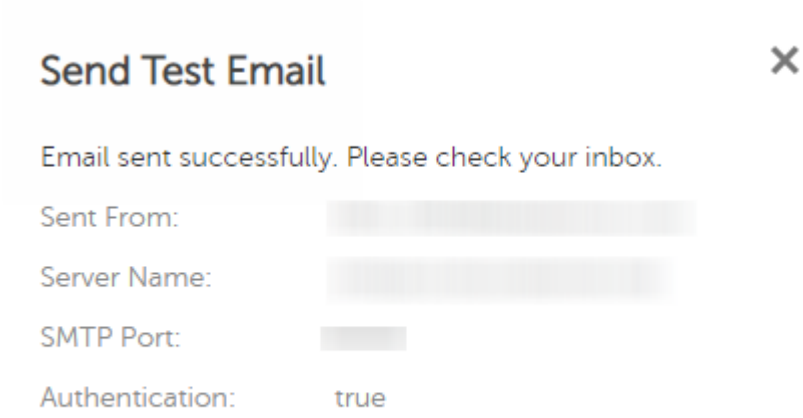
- In Populations > Endpoint Groups, groups now display by policy priority.
- Endpoint groups have a new option to build groups based on a TPM being Present or a TPM being Active on a device with Dell Encryption installed.
- Test emails can now be sent in the Management Console to validate email workflows.

  To test the email workflow:
  1. Navigate to **Management > Notification Management**.
  2. Select **Send Test Email**.

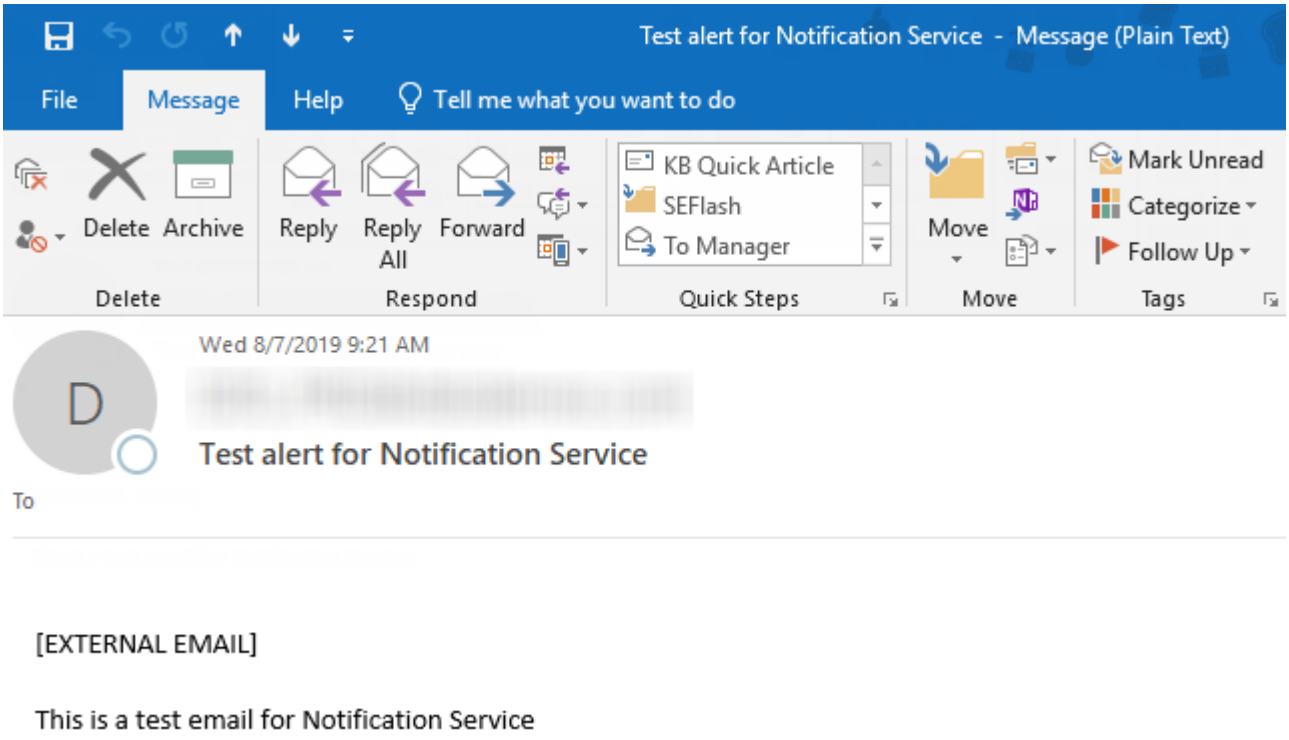


  3. Specify the email to test and select **Send Email**.

  If the email passes through the Dell Server successfully, the following results screen displays.



  The following is an example of successful test email.



Resolved Technical Advisories v10.2.7

- The Server Configuration Tool now updates all required elements when importing SSL and TLS certificates. [DDPS-8450]
- Authentication processes around the Dell Server's message broker is improved. [DDPS-8456]
- Services are hardened to improve security posture. [DDPS-8487, DDPS-8689, DDPS-8740]
- An issue resulting in an inaccurate number of policy overrides displaying is resolved. [DDPS-8492]
- When changing priority values for Content Based Protection, all values populate and remain as expected. [DDPS-8531]
- Selected mobile devices can be removed from Populations > Endpoints as expected. [DDPS-8853]
- In Populations > Endpoints, Export File as an Excel document now functions as expected. [DDPS-8857]
- New email notifications no longer inherit modifications to existing email notifications. [DDPS-8881]
- Scheduled reporting emails now send at their scheduled time. [DDPS-8888]
- Manage Reports now only accepts emails distinguished by comma separated values. [DDPS-8955]

Technical Advisories v10.2.7

- The Postgres Audit database is now installed in C:\ProgramData. The Security Management Server installer currently does not calculate the space required for the Postgres Audit database on the system drive. [DDPS-9059]

New Features and Functionality v10.2.6

- The Dell ACL service is rebranded to Del Access Group service.

Resolved Technical Advisories v10.2.6

- The Security Management Server's built-in help file is now appropriate automatically translated for all supported languages based on browser locale. [DDPS-8566]
- The Security Management Server's applications and resource files are now signed by Dell's SHA-1 and SHA-256 code-signing certificates. [DDPS-8711, DDPS-8712, DDPS-8722, DDPS-8723]

- User Groups and Endpoint Groups no longer accept special characters in the Priority field when using Internet Explorer. [DDPS-8735]
- Fields can be searched as expected in Managed Reports. [DDPS-8737]
- Type and Priority values are now retained after updating the Email field in Edit Notifications. [DDPS-8755]

Technical Advisories v10.2.6

- Selected mobile devices cannot currently be removed from Populations > Endpoints. As a work around, select the mobile device's hostname then select **Remove** on the Endpoint Details page. [DDPS-8853]
- In Populations > Endpoints, Export File as an Excel document fails with a 404 error. [DDPS-8857]
- In Dashboard > Endpoint Protection Status > Protection Status, the Shield column is rebranded to PBE. [DDPS-8771]
- Cloud Device Control commands do not currently generate logs. [DDPS-8866]
- If an existing email notification is modified then saved, the next new email notification inherits the previous notification's modifications. [DDPS-8881]
- Scheduled reporting emails send 30 minutes later than their scheduled time. [DDPS-8888]
- If an administrator's password contains double quotations, password validation fails and the following message displays:

  Credentials are invalid. Please verify the logon and password. [DDPS-8936]
- When installing the Security Management Server on Windows, if the administrator's password contains a backslash, the ACL service fails to start resulting in a timeout. [DDPS-8938]

New Features and Functionality v10.2.5

- No new features or functionality exist.

Resolved Technical Advisories v10.2.5

- Search performance for Advanced Threat Events and Audit Event data has been improved. [DDPS-8342, DDPS-8373]
- The default version of PostgreSQL has been updated to resolve third-party vulnerabilities. The PostgreSQL service leveraged by the Security Management Server is rebranded to Dell PostgreSQL 10.7. [DDPS-8480, DDPS-8985]
- An error is no longer returned to an external user when attempting to pre-share key access to another external user. [DDPS-8664]

Technical Advisories v10.2.5

- When using Internet Explorer and editing priority, User Groups and Endpoint Groups incorrectly accepts special characters in the Priority field. [DDPS-8735]
- Type and Priority values are not retained after updating the Email field in Edit Notifications. [DDPS-8755]

New Features and Functionality v10.2.4

- Windows Server 2019 (Standard/Datacenter) is now supported.

Resolved Technical Advisories v10.2.4

- Updated 6/2019 - Report Administrator, Report Owner, and Report User roles can now log in to the Management Console as expected. [DDPS-6101, DDPS-8625]
- An issue resulting in the *Type* and *Priority* fields persisting after creating multiple notifications in the Management Console is resolved. [DDPS-6779]
- Resolved an issue with malformed dates causing SIEM/Syslog events to improperly output to their network or local destinations. [DDPS-7570, DDPSUS-2325]

- An issue resulting in Managed Reports not displaying EMS events is resolved. [DDPS-8561, DDPSUS- 2532]
- An issue resulting in users with appropriate file rights not displaying in the Pre-Share UI is resolved. [DDPS-8567]
- Resolved an issue where the Security Management Server's Core Server, ACL Service, and Key Server would not start after a reboot. For more information, see https://www.dell.com/support/article/us/en/04/sln316840. [DDPS-8522]

Technical Advisories v10.2.4

- No technical advisories exist.

Resolved Technical Advisories v10.2.3

- An issue resulting in the PostGRESQL database not properly cleaning data during default configured cleanup jobs is resolved. After installation, on subsequent cleanup jobs, all previous jobs are reconciled. [DDPS-8397]
- An issue with data exported to a Syslog or SIEM server through Event Management in the Management Console is resolved. [DDPS-8398]

Technical Advisories v10.2.3

- In rare circumstances, pre-sharing a protected document with an embargo set may not in all cases pre-share the key. To work around this issue, manually share the key through the right-click menu from an internal user or an internal file owner. [DDPS-8567]

New Features and Functionality v10.2.2

- No new features or functionality exist.

Resolved Technical Advisories v10.2.2

- The Security Management Server now validates the version of Microsoft Visual C++ 2013 version 12.0.40660. If this version is not found, the installer exits. Please validate this version is installed before installing the Security Management Server. [DDPS-8010, DDPSUS-2437]
- Translation consistency is improved. [DDPS-8064]
- An issue resulting in service account names being rejected when starting with an escape character such as u and some special characters is resolved. [DDPS-8109]
- Clean installs of the Security Management Server no longer result in ACL service error messages. [DDPS-8149, DDPS-8270]
- Sorting by Classification Path in Audit Events no longer results in an error. [DDPS-8151]
- An issue that resulted in internal errors when transitioning between screens in the Management Console is resolved. [DDPS-8279]

New Features and Functionality v10.2.1

- Audit data for blocked print screen events, blocked processes events, and blocked prints events are now displayed in the Management Console.

Resolved Technical Advisories v10.2.1

- Threat Events tab is now visible when at least one Threat Prevention or Advanced Threat Prevention license is consumed. [DDPS-5728]
- Manage Reports work as expected when special characters are added to the *Report Name* . [DDPS-6362]

- The default setting exclusions for weak ciphers are now preserved when upgrading from v9.10 to the latest Dell Security Management Server. [DDPS-7301]
- Time stamps used for "Commit" date/times are stored as UTC and will be converted to the current time-zone based on the time-zone setting of the system viewing the WebUI. [DDPS-7855]
- Resolved mismatching information for the *Unique ID* for endpoints on the "Endpoint" page, and on the "Device Detail" page. [DDPS-7928]
- Resolved an issue with dependency management, resulting in failures to update the Dell Security Management Server Virtual. [DDPS-7980]
- Resolved an issue with innocuous error messages within the Dell Beacon Service by removing unnecessary dependencies. [DDPS-7981]
- Resolved an incorrect symbolic link that resulted in additional storage overhead for logging. [DDPS-7991]
- Resolved an issue where the Windows Application for Dell Security Management Server may timeout or take an extremely long time to download key data. [DDPS-8121, DDPSUS-1796]

New Features and Functionality v10.1

- A Downloads page has been added to Management Console for downloading Dell Data Security endpoint software.
- Scheduling report emails is now supported. A report must be created under Reporting > Manage Reports in the Management Console before the scheduling option is available.
  - The *Email* field is limited to 1024 characters.
  - *Day of Month* drop down will provide 1 - 31 and Last options to choose.
  - *Time*, will schedule the time based upon your current location.
  - Schedule Details page shows the date sent, schedule, next send, etc.

Resolved Technical Advisories v10.1

- A forensic key bundle download using the Administrative Download Utility (CMGAd) now succeed for endpoints with large key sets based on a high number of activations. [DDPS-6920, DDPSUS-2361]
- An issue resulting with a customer unable to run Advanced Threat Prevention reports while using the compliance reporter due to low memory has been resolved. [DDPS-7386, DDPSUS-2341]
- Dell Enterprise Server v10.1 includes a security update addressing a Jetty Security Bypass vulnerability (CVE-2017-7658). Customers and field teams should take v10.1 and all Dell Enterprise Server updates or sustaining releases as a best practice. [DDPS-7387, DDPSUS-2344]
- Selections made in the Audit Events page are now saved after a user navigates away from the page. [DDPS-7445]
- Servers with large amount of events from Advanced Threat Prevention may experience high memory usage on the Dell Security Management Server or Dell Security Management Server Virtual. This may result in services crashing on the server. Maximum heap space and physical memory can be increased to work-around this issue. [DDPS-7469]
- Compliance Reporter is hidden by default on the Management Console. [DDPS-7717]

Technical Advisories v10.1

- By default the Dell Security Management Server and Dell Security Center consoles will export data in UTF-8 format. In some cases, this data does not display properly if the file is opened and displayed in Unicode, which is done by default for Microsoft Excel. For information on opening files with UTF-8 encoding, see: https://support.office.com/en-us/article/choose-text-encoding-when-you-open-and-save-files-60d59c21-88b5-4006-831c-d536d42fd861?ocmsassetID=HA010121249&CorrelationId=050891fd-c54e-4e23-9e74-c8c75962d07f&ui=en-US&rs=en-US&ad=US. [DDPS-7613]
- When the Security Management Server is configured within an IPv6 environment with no IPv4 support, notification registration fails due to a communications error. To work around this issue, enable IPv4 support in this environment. [DDPS-7655]
- Navigating to the *Enterprise > Advanced Threat Events* tab and selecting the Host Name from the list results in being directed to Endpoint Details & Actions, instead of the Advanced Threat Events tab. To work around this issue, click **Advanced Threat Events** from *Details & Actions*. [DDPS-7739]
- When a recently added user attempts to log in the WebUI with a special character "\" in the user name, the login is unsuccessful and results with an error message displaying "The username or password used is invalid." [DDPS-7768]

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. [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

- 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]

New Features and Functionality v9.11

- Below are the requirements for SQL permissions. The current user performing the installation and the services must have local administrator rights.

Type	Action	Scenario	SQL Privilege Required
Back end	Upgrade	By definition, upgrades already have DB and Login/ User established	db_owner
Back end	Restore Install	Restore involves an existing DB and login.	db_owner
Back end	New Install	Use existing DB	db_owner
Back end	New Install	Create new DB	dbcreator, db_owner
Back end	New Install	Use existing login	db_owner
Back end	New Install	Create new login	securityadmin
Back end	Uninstall	NA	NA
Proxy Front end	Any	NA	NA

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]

Technical Advisories v9.11

- Added 11/2018 - When upgrading from v9.10 to the latest Dell Security Management Server, default setting exclusions for weak ciphers are lost. To disable weak ciphers, seehttps://www.dell.com/support/article/us/en/19/sln301519/how-to-disable-weak-ciphers-in-dell-security-management-server-and-virtual-server-dell-data-protection-enterprise-edition-and-virtual-edition?lang=en. [DDPS-7301]

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.

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]
- Added 7/2019 - Java is updated to resolve a Remote Code Execution vulnerability in RMI Serialization (CWE-502). [DDPS-6200, DDPSUS-2084]

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]
- 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 error message that displays during installation on the Server 2016 when the prerequisite .Net 3.5 is not already installed correctly displays "Server 2016". [DDPS-5591]
- 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]
- 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]
- 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 9.9.2 are now blocked for server versions prior to Dell Data Protection | Encryption Enterprise Server version 9.2. [DDPS-6254]
- During installation or upgrade of the Security Management Server, an active script is run in the %TEMP% directory, which may be blocked by antivirus. To work around this, Dell recommends disabling all antivirus solutions before installing or upgrading the Security Management Server. [DDPS-5832]

- 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

- Advanced Threat Prevention 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.
- Hardware Crypto Accelerator and Mobile Edition are no longer supported. Their policies have been deprecated.
- Enterprise Server is rebranded to Security Management Server.

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]
- The error that displays when an invalid or blank hostname is entered during installation now displays the label of the field in the installer. [DDPS-4466]
- The diagnostic tool, Data Collection Utility, is now included in the Start menu with other Server components. [DDPS-4918]
- 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]
- 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]
- All files are now installed in the expected locations after upgrade on a Dell Server running in Disconnected Mode when previously installed files were stored in a non-default location. [DDPS-5190]
- The "Certificate" type is now populated in the Type of Notification column of the All Notification Report in Compliance Reporter. [DDPS-5217]
- Upgrade no longer fails when the Run As Service account is changed during the upgrade. [DDPS-5226]
- 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.

1. 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>

2. 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

3. 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.

4. 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"
   ,"port":"5540"}}}
   ```

[DDPS-5234]

Resolved Customer Issues

- An issue is resolved that resulted in a license import failure with an error in the Security Server log that the system cannot find the `\AppData\Local\Temp\` folder. [DDPS-4240]

- Installation now proceeds as expected when the Service Runtime Account password that is used during installation contains "**$_**" (dollar sign followed by underscore). [DDPS-4923]
- 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]
- Certificates with passwords that include special characters can now be successfully imported. [DDPS-5396]
- The installer now accepts a period (".") in the SQL service account username with SQL Server 2008 R2 and SQL Server 2016. [DDPS-5418]
- 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]
- As of v9.8, the ESXi vSphere thick client can no longer be used for deployment. Also, previous installs on ESXi 5.1 have not been prevented although they are not supported. Installs on ESXi 5.1 are now prevented. [DDPS-5086, DDPS-5269]
- 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

- Enterprise Server 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.
- Enterprise Server now supports Disconnected Mode, for air-gapped environments.
- Added 7/2017 - Enterprise Server is now supported with VMware ESXi 6.5.
- Active Directory groups and domains can now be specified when adding or modifying Endpoint Groups. Enterprise Server 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 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.

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]
- 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]
- Advanced Threat Event Dashboard Notifications are now properly categorized by Type. [DDPS-4994]
- Localizations of Remote Management Console 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:

  1. On one of the Servers to be federated, edit `<installation folder>\Enterprise Edition\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

  2. Save federatedservers.properties.
  3. Copy federatedservers.properties and save it off the Security Server.

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

  4. 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.

  5. Copy the federatedservers.properties file to the `\Security Server\conf` folder of each Server to be federated.
  6. Restart each Security Server after copying federatedservers.properties to its \conf folder.

  [DDPS-2889]

- An issue is resolved that resulted in an intermittent Internal Error in the Remote Management Console. [DDPS-4446]
- SSL/TLS protocols for Compliance Reporter are now configurable in the eserver.ssl.protocols property in the `reporter/conf/eserver.properties` file and are preserved during backup/restore operations. [DDPS-4547]
- 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]
- Importing a certificate during installation now proceeds as expected when spaces exist in the certificate alias. [DDPS-4770]
- Server Configuration Tool error handling is improved. [DDPS-4786]
- Importing the same certificate for Server Encryption (SSOS) that is imported as the SSL certificate is now blocked, with an error message that the certificate cannot be imported twice. [DDPS-4805]
- 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 Policy Proxy Polling Interval value is now correct in the Compliance Reporter Effective Policy Report. [DDPS-4927]
- Importing a valid certificate with Server Configuration Tool now succeeds after importing an invalid certificate. [DDPS-4928]

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 Enterprise Server v9.7 or later. Before upgrading clients to use these features, Enterprise Server v9.7 or later must be installed and the policy, Memory Action: Exclude executable files, must be ***enforced*** on pre-v1.4 clients. Do not begin client upgrade before the new policy is enforced on the client. [DDPS-5112]
- Amended 7/2017 - SMTP settings are not retained during a Recovery Installation and must be reconfigured using the Server Configuration Tool after recovery is complete. [DDPS-5239]
- Added 7/2017 - Enterprise Server does not support .local domains. [DDPS-5334]

New Features and Functionality v9.6

- Dell Enterprise Server is now supported with the following:
  - Windows Server 2016
  - SQL Server 2016
- Dell Enterprise Server now supports Advanced Threat Prevention and Encryption on persistent and non-persistent VMware and Citrix VDI clients.
- 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]
- An issue is resolved that resulted in an occasional database migration error during a new installation. [DDPS-3792]
- 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]
- 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

- Enabling non-domain activations in the server_config.xml file now succeeds as expected, without regard to case sensitivity of the value entered for the property, accountType.nonActiveDirectory.enabled. Also, Compatibility Server logs now indicate when enabling non-domain activation fails due to case-sensitivity issues with the property name, itself. [DDPS-4068]
- An issue is resolved that resulted in a Security Server Java instance failure with the following error message: EXCEPTION_ACCESS_VIOLATION. [DDPS-4245]
- An issue is resolved that resulted in uncommitted policies that were not initiated by the administrator. [DDPS-4761]
- Added 05/2018- Dell Security Management Server selects policies based on the group in which endpoints are in no longer instead of arbitrated policies. The group with the highest precedence value succeeds, and no other groups are considered. [DDPS-5377]

Technical Advisories v9.6

- If the ProgramData folder is open during an upgrade, an error displays: "C:\ProgramData\Del\GateKeeper is unavailable...." To work around this issue, close the ProgramData folder and click **OK** in the error dialog. [DDPS-4573]
- 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

- Added 8/28 - A new policy is added that enables administrators to force Policy-Based Encryption when a SED is detected.
- As of v9.4.1.6,Dell Enterprise Server 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.

Resolved Technical Advisories v9.5

- When an existing certificate is imported during upgrade, the installer no longer displays an error if the certificate password has been changed from the default password. [DDPS-2644]
- 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]
- After upgrade, the Compliance Reporter reports, SED Authentication Method Policy Detail and Windows Encryption Failures and Sweep Status, are available as expected. [DDPS-4183]
- 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]
- During new database installation, the installer now creates the database in the folder configured in Server Properties Database Settings rather than in the master database folder specified in Database Properties Files. [DDPS-4221]

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:

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

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

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

  2. Change the StrictValidation property value from **true** to **false**: `<property name="StrictValidation" value="false"/>`
  3. Restart the services.
  4. 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.
  5. Correct the policy value formatting, and click **Save**.
  6. In the left pane, click **Management** > **Commit**, enter the policy change description, and click **Commit Policies**.
  7. If desired, change the StrictValidation property value from **false** back to **true**, to re-enable policy validation.

  [DDPS-4779]

New Features and Functionality v9.4.1.6

- Dell Enterprise Server 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 Dell Enterprise Server 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 is 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 no longer occurs during forensic key bundle download from Dell Enterprise Server. [DDPS-3244]
- 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]
- 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.
- Dell Enterprise Server installations are no longer supported on 32-bit operating systems.

Resolved Technical Advisories v9.4

- The installer no longer accepts underscores in host names. An underscore character ("_") in either the Compatibility Server host name or Security Server host name causes connection to that Server to fail. A host name cannot contain an underscore character ("_"), due to a Java platform issue, JDK-6587184. For more information, see http://bugs.java.com/view_bug.do?bug_id=6587184. [DDPMTR-1345, DDPS-3570]
- 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]
- Dell Enterprise Server 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 Enterprise Server 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]
- 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]
- 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]
- An issue that led to Remote Management Console timeouts when searching for endpoints is resolved. [DDPS-3400]
- An issue that caused an error during installation on servers with heavily loaded processors is resolved. [DDPS-3444]
- 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]
- Provisioning the Advanced Threat Prevention service now proceeds as expected when used with a proxy server. [DDPS-3475]
- The backup folder is now preserved following an installation rollback during upgrade. [DDPS-3527]
- Policy template settings that include the Rijndael value now migrate properly during upgrade. [DDPS-3531]
- 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]
- The Save option is now available when the SQL Authentication password is updated in the Server Configuration Tool. [DDPS-3817]
- 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]
- An internal error no longer displays on the Effective Policies page for an Endpoint or User after upgrade from a pre-v9.2 Enterprise Server. [DDPS-4000]

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]
- If either the SQL database or SQL instance is configured with a non-default collation, installation fails. A non-default collation must be case-insensitive. For a list of collations and case sensitivity, see https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx. [DDPS-3355]
- 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 <installation folder>\Enterprise Edition\Security Server\conf\spring-jetty.xml, and comment out the excludeProtocols property:

   <!--

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

   -->

2. In the ..\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]

New Features and Functionality v9.2

- Dell Enterprise Server 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.

Resolved Technical Advisories v9.2

- 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]
- Uninstallation with setup.exe no longer requires reboot. [DDPS-1839]
- At the end of Server installation, the check box next to Show windows installer log is now visible. [DDPS-1840]
- 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]
- The error message that displays when the Core Server is running during Server Configuration Tool startup no longer states that the Compatibility Server must be stopped. The Server Configuration Tool functions properly when the Compatibility Server is running. [DDPS-1863]
- 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]
- The Cloud Storage policy, OneDrive Message, is no longer applicable and is now removed from the Remote Management Console. [DDPS-1917]
- An upgrade now proceeds as expected after a previous upgrade is canceled. [DDPS-2065]
- 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]
- An issue that caused some failures of services startups, on-the-box entitlement retrievals, and Compliance Reporter startups after installation or upgrade when configuration changes are made through the Server Configuration Tool has been resolved. [DDPS-2755]
- 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]

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]
- 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]
- 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 AdminHelp icon is not available from the Remote Management Console login screen. [DDPS-2858]
- 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 Server 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]
- 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]
- When adding a User in the Remote Management Console, searches for users who belong to a large number of Active Directory groups may take longer than expected. If this occurs, clicking the Search button more than once on the Add Users by Domain dialog can cause the Security Server to crash. Do not click the Search button more than once on the Add Users by Domain dialog. [DDPS-3010]
- 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]

Resolved Technical Advisories v9.1.5

- In Compliance Reporter, the Mobile Policy report now includes results for all activated mobile devices. [DDPMTR-838]
- During an upgrade when the SQL database is unavailable, the upgrade now continues without delay. The Server Configuration Tool can be used to migrate the database when it is available. [DDPMTR-1226]
- When the option Re-use SSL certificate for SSOS is selected during a new installation, the SSL certificate is reused as expected. [DDPMTR-1243]
- The Compliance Reporter Email Recipients field now accepts only a comma (",") as a separator rather than accepting special characters. [DDPMTR-1257]
- The setting field of the Threat Protection policy, Exclude Processes, no longer accepts invalid values in the Remote Management Console. [DDPMTR-1346]
- Dell Enterprise Server v9.1.5 includes a security update addressing an OpenSSL vulnerability (OpenSSL CVE-2015-4000). Customers and field teams should take v9.1.5 and all Dell Enterprise Server 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]
- Import of certificates with spaces in alias names is improved. [DDPMTR-1611]

Technical Advisories v9.1.5

- Migration to a version later than v9.0 fails when using a Microsoft SQL 2005 database. [DDPMTR-1633]

- 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.
- Server Encryption is now supported, featuring port control and removable storage encryption as well as support for maintenance scheduling, which allows control over enforcement of policies that require reboot.
- 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]
- 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]
- After uninstallation, wrapper logs are now removed as expected. [DDPMTR-913]
- 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]
- The upgrade error that occurred with an error logged regarding the UserEntity table, EID column is now resolved. [DDPMTR-1237]
- 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, DDPMTR-1011]

Technical Advisories v9.1

- In the Remote Management Console, fields for policies with numeric values accept a "+" or "-" character immediately preceding the policy value. To work around this issue, ensure that these characters are not included in policies' values before the policies are committed. [DDPMTR-765]
- If Compliance Reporter default reports have been customized prior to upgrade, the previous version of customized reports must be restored in order to continue to use them. However, after the previous version is restored, new reports included in the upgrade are not available. [DDPMTR-870]
- When a self-signed certificate is created at installation, the certificate is valid from a time approximately six hours later than the installation time, rather than being immediately valid. To work around this issue, on the Settings tab of the Server Configuration Tool, check Disable Trust Chain Check. [DDPMTR-1195]

- Added 09/2015 - The CIDR format must be used to specify a subnet in Firewall Settings in the Remote Management Console. [DDPMTR-1253]
- In the Remote Management Console, when Client Firewall rules are added or edited and ICMP Transport Protocol is selected from the Transport drop-down menu, the Message Type displays the default message type as "Echo-Replay" instead of "All," as expected. [DDPMTR-1254]
- When using Windows Authentication to perform a new installation or upgrade, if the credentials of the logged on user differ from the credentials of the domain services account and a certificate from a signing authority is used, the certificate must be stored in a folder that is accessible during installation to both the domain services account and the logged on user. If the credentials of the logged on user differ from the credentials of the domain services account and a self-signed certificate is used, before beginning installation or upgrade, you must log in with the domain services account credentials. [DDPSUS-406]

New Features and Functionality v9.0

- Dell Enterprise Server 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

Resolved Technical Advisories v9.0

- AdminHelp now correctly states that the value OneTimePassword rather than One-time Password can be set for the logon and in-session policies. [DDPS-1594]
- In localized versions of the Remote Management Console installer, the Host dialog banner is now properly sized. [DDPSTE-275]
- When Enterprise Server is uninstalled, the LSARecovery.log file is now removed, as expected. [DDPSTE-308]
- AdminHelp now correctly states the default Server Polling Interval for TPM and SED System Settings as 720 minutes, and the Cloud Storage Server Polling Interval range is now specified as 1-1440 minutes. [DDPSTE-486, DDPSTE-586, DDPSTE-591]
- A few previously unlocalized areas of Remote Management Console screens are now localized. [DDPSTE-501, DDPSTE-502, DDPSTE-503]

Technical Advisories v9.0

- In Compliance Reporter EMS Event and Mobile Device Detail Report Result pages, some columns and the bottom scroll bars are not visible. [DDPMTR-969]
- 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 performing a Remote Wipe on an iOS device that is managed through EAS, although the Remote Wipe is successful and an Acknowledged time and date stamp display in Enterprise Server, an error is logged in Policy Proxy and EAS server logs. [DDPSTE-529]
- A Mobile Edition license is not consumed when a mobile client is activated. [DDPSTE-549]
- The Key Server log file, log.txt, is stored in `C:\<installpath>\Dell\Enterprise Edition\Key Server` rather than in C:\<installpath>\Dell\Enterprise Edition\Key Server\logs, as expected. [DDPSTE-637]

- If a custom value is used for the Message Broker TCP Port, after a new installation or upgrade from a pre-v8.5 Enterprise Server, the value must be manually configured. For a new installation, open <Compatibility Server install dir>\conf\server_config.xml and change the broker.port value to the correct port number. For an in-place upgrade from a pre-v8.5 Enterprise Server, change both the broker.port value in the server_config.xml file and the activemq.port.tcp value in Message Broker\conf\application.properties to the correct port number. [DDPSTE-654]