Fix Notes for Symantec Endpoint Protection 12.1 Release Update 1

# Component Versions

|  |  |
| --- | --- |
| AutoProtect | 12.3.3.14 |
| AutoProtect Driver | 12.3.3.13 |
| AV Engine | 20111.2.0.82 |
| AV Engine Driver | 20111.2.0.82 |
| BASH Defs | 6.5.0.7 |
| BASH Defs Driver | 6.5.0.7 |
| BASH Framework | 6.2.100.27 |
| CIDS Defs | 10.0.4.57 |
| CIDS Defs Driver | 10.0.4.51 |
| CIDS Framework | 9.8.3.6 |
| Common Client | 10.2.0.7 |
| DecABI | 2.1.2.12 |
| DefUtil | 4.4.1.7 |
| DuLuCallback | 1.3.1.10 |
| ECOM | 111.2.0.72 |
| ERASER | 111.2.0.38 |
| ERASER Driver | 111.2.0.38 |
| Iron | 1.7.0.9 |
| Iron Driver | 1.7.0.8 |
| LiveUpdate (server) | 3.3.1.23 |
| LiveUpdate Express (client) | 2.0.2.5 |
| MicroDefs | 3.2.0.24 |
| SymDS | 1.2.1.6 |
| SymDS Driver | 1.2.1.5 |
| SymEFA | 2.2.1.4 |
| SymEFA Driver | 2.2.1.4 |
| SymEvent | 12.9.0.22 |
| SymEvent Driver | 12.9.0.18 |
| SymNetDrv | 11.1.3.3 |
| SymNetDrv Driver | 11.1.3.2 |

# Product Changes in this Release

The following changes are highlighted, as they may require the Symantec Endpoint Protection (SEP) administrator to make a policy or procedural change to match the behavior of the previous release. Some changes may allow the administrator to add functionality that was not present in the previous release.

**The network application monitoring feature is configured to "ask" by default on SEP 12.1 Small Business Edition**

**Fix ID:** 2515014

**Symptom:** In SEP 12.0 Small Business Edition (SBE), the network application monitoring feature was set to "allow" by default. In SEP 12.1 Small Business Edition it is configured to "ask" by default. In both products it is not possible to change the value on the client.

**Solution:** The network monitoring feature is now disabled on installation or migration to 12.1 SBE.

**Administrator cannot set the heartbeat to longer than 60 minutes**

**Fix ID:** 2492263

**Symptom:** Upon installing SEP 12.1, the Symantec Endpoint Protection Manager (SEPM) administrator cannot set the heartbeat longer than 60 minutes.

**Solution:** The maximum number of heartbeat minutes was increased to 2,880.

**Small Business Edition client reboots without prompting**

**Fix ID:** 2437682

**Symptom:** After auto-upgrade, Small Business Edition clients automatically reboot when no user is logged in.

**Solution:** On server class operating systems, SEP Small Business Edition no longer automatically reboots. There is no reboot prompt, and the computer does not reboot. The status "needs reboot" is passed to the management server.

**Purging of stale clients cannot be configured by domain**

**Fix ID:** 2424460

**Symptom:** The ability to purge stale clients cannot be configured by domain.

**Solution:** Purging of stale clients can now be configured per domain.

**SEPM installation automatically creates database maintenance jobs, which may conflict with previously-created jobs**

**Fix ID:** 2428340

**Symptom:** During the installation of SEPM, the installer creates several database maintenance jobs. These jobs may conflict with other jobs that were previously created by the database administrator.

**Solution:** The SEPM installation and configuration wizard was modified to allow the administrator to enable or disable the database maintenance jobs when creating a new site.

**Administrator is prompted for credentials after logging on to the SEPM console**

**Fix ID:** 2533910

**Symptom:** After logging on to the SEPM console, accessing any Reporting page prompts the administrator to enter the password again. This issue occurs when the server host name contains an underscore (\_) character. The message displayed is "Login failed due to invalid user name or password." The reporting.log file contains the entries:

*ERROR 0002: user\_name does not exist.*

*ERROR 0002: user\_name does not exist.*

**Solution:** Server reporting was modified to allow host names with an underscore (\_) character.

**SEPM Configuration wizard fails if the SEM5 user already exists**

**Fix ID:** 2435859

**Symptom:** SEPM cannot reuse the existing DB user account when running a fresh install with a new SQL Server database.

**Solution:** Reuse of an existing DB user account is now allowed when installing SEPM and creating a new database.

**"Remote host name" column is not present in the exported NTP Traffic Log**

**Fix ID:** 2513023

**Symptom:** The "Remote host name" column is missing from the exported NTP Traffic log. This column exists in SEP 11.0.

**Solution:** The "Remote host name" column was restored for exported NTP traffic logs.

**Application and Device Control will incorrectly block a USB device when connected for the first time**

**Fix ID:** 1284681

**Symptom:** USB hub devices are incorrectly blocked and devices attached to the hub are not recognized.

**Solution:** USB hub devices are no longer blocked by default. SEP only blocks child devices of USB hubs. If the Application and Device Control policy is specifically configured to block the USB hub, all child devices are also blocked.

**Firewire device is incorrectly listed as "1394 FireWire Host Controller"**

**Fix ID:** 2336000

**Symptom:** In a policy component, the Firewire hardware device is incorrectly shown as "1394 FireWire Host Controller."

**Solution:** The device text was changed from "1394 FireWire Host Controller" to "1394 FireWire Devices."

**Download Insight does not display a system tray notification**

**Fix ID:** 2427271

**Symptom:** When Download Insight detects a threat, there is no immediate notification to the user.

**Solution:** Download Insight now displays a system tray pop-up notification to alert the user that a remediation is in progress.

**When File System AutoProtect non-viral threat actions are set to Quarantine/Deny Access, AutoProtect always denies access and never tries to quarantine. If the file is newly created, AutoProtect deletes the file.**

 **Fix ID:** 1954266

**Symptom:** You configure File System AutoProtect actions to Quarantine/Deny Access on non-viral threats. When a non-viral threat is accessed, AutoProtect denies access but does not attempt to quarantine per your configuration.

**Solution:** The interaction between the SEP client and File System AutoProtect was modified to better process these types of threats. Specific changes:

* The UI option "Block security risks from being installed" was removed.
* New UI options have been added to File System AutoProtect > Advanced settings. "Delete newly created infected files if the action is 'leave alone (log only)'" has a new sub-option, "Delete newly created security risks if the action is 'leave alone (log only).'"
	+ If the parent option, “Delete newly created infected files if the action is ‘leave alone (log only)’” is checked, this option is checked by default.
	+ If the parent option is unchecked, "Delete newly created security risks if the action is 'leave alone (log only)'" is unchecked and disabled.

**SEPM does not block installation on a hostname with an underscore character**

**Fix ID:** 2436942/ 2436959

**Symptom:** The SEPM installer does not block installation when the server’s hostname contains one or more underscore (\_) characters.

**Solution:** The SEPM installer was modified to warn the user before migration if the hostname contains an underscore character.

**Unable to determine the Release Update number from Help > About**

**Fix ID:** 2355966

**Symptom:** The Help > About window displays a version, for example 12.1.671.4971. It does not display the Release Update number.

**Solution:** Added a Release Update number to the Help > About window, for example “RU1.”

# Top Impacting Issues Resolved in this Release

**Clients lose protection technologies after SEPM is migrated from 11.x to 12.1**

**Fix ID:** 2436468

**Symptom:** Symantec Endpoint Protection Manager is migrated from 11.x to 12.1. Existing 11.x clients receive a policy that incorrectly instructs them to change feature states, removing some or all protection technologies. This problem is encountered only if an 11.x package is previously deployed with the "maintain existing feature states" option.

**Solution:** The 11.x client installation feature states were not correctly mapped to the 12.1 feature states in the policy file. The mapping was modified to resolve this issue.

**Content appears “out of date” when clients have up-to-date content**

**Fix ID:** 2436471

**Symptom:** TheDownload Protection Content report shows a failure, with out-of-date content, when the clients have up-to-date content.

**Solution:** The method that SEPM uses to calculate content dates was modified to correct this issue.

**Cannot open the SEP 12.1 user interface after migration from SEP 11.x to 12.1**

**Fix ID:** 2491486

**Symptom:** When the Application and Device Control rule "Protect client files and registry keys" is enabled before migration, after migration to SEP 12.1, the client user interface cannot be opened. Attempting to open the user interface results in the message "Symantec Endpoint Protection cannot open because some Symantec Services are stopped. Restart the Symantec services, and then open Symantec Endpoint Protection."

**Solution:** The Application and Device Control rule is now converted from SEP 11.x format to SEP 12.1 format during migration. This allows the user interface to open correctly.

**Check Point VPN cannot start or terminates unexpectedly when SEP 12.1 is installed**

**Fix ID:** 2494474

**Symptom:** The Check Point VPN cannot start or terminates unexpectedly when SEP 12.1 is installed on the client.

**Solution:** The SymTDI driver was modified to prevent this crash.

**Unable to disable the "Threats were detected while you were logged out" message**

**Fix ID:** 2608606

**Symptom:** When a virus is discovered as part of a scheduled scan while the user is logged out, they are notified that threats were discovered when they log in, even if notifications are disabled. It is not possible for the administrator to disable this message.

**Solution:** The SEP client was modified to honor the notification settings that are configured by the administrator. If notifications are disabled, the message no longer appears.

**SONAR definitions display as “out of date”**

**Fix ID:** 2522692

**Symptom:** When SONAR definitions are up-to-date, they display as “out-of-date” on the SEPM server.

**Solution:** The SONAR definition version was not formatted correctly in the database. The formatting was resolved to prevent this issue.

**SEPM uninstall deletes an ODBC entry in the System DSN**

**Fix ID:** 2522832

**Symptom:** Uninstallation of SEPM incorrectly deletes a System DSN ODBC entry that is not used by SEPM.

**Solution:** The SEPM installer was modified to only remove the SymantecEndpointSecurityDSN registry key during uninstallation.

**SEPM client view does not display all pages correctly**

**Fix ID:** 2568046

**Symptom:** In the SEPM client view, some pages are blank in all views except Network Information or Client System. The "missing" clients are able to check in and communicate with the server.

**Solution:** The SEPM console was modified to prevent a condition where the client reboot status prevented it from appearing in the view.

**SEP clients cycle through Management Server lists continuously**

**Fix ID:** 2569442

**Symptom:** SEP clients continually cycle through the Management Server Lists. The client will connect to one SEPM, then another, and repeat.

**Solution:** The profile time is now converted to GMT to resolve a scenario where the profile does not match.

# All Resolved Issues

**CPU load is high on the host in a virtual environment when guest virtual machines are idle**

**Fix ID:** 2413588

**Symptom:** CPU usage of WmiPrvse, “SvcHost –netsvcs” and System are significant when the client is idle. The result is high overall CPU of the host computer in a virtualized environment.

**Solution:** To reduce resting CPU usage, the SEP client was modified to reduce polling intervals and register for additional notification changes when appropriate.

**Some applications fail to launch on Windows XP 32-bit when Application and Device Control is enabled**

**Fix ID:** 2423743

**Symptom:** ThinApp version of Internet Explorer 8 and Adobe Updater fail to launch on Windows XP 32-bit operating systems when Application and Device Control is enabled.

**Solution:** The Sysplant.sys driver (Application and Device Control) was modified to correct an issue that prevented these applications from launching correctly.

**Unable to upgrade SEPM from 11.x to 12.1**

**Fix ID:** 2436198

**Symptom:** Upgrade of SEPM from version 11.x to 12.1 fails. The upgrade log contains the following entries:

*WARNING: AgentManager>> deleteComputerAndAgentByComputerId: Done! can't delete because there are some attached clients! count=1*

*WARNING: java.sql.SQLException: Network error IOException: Address already in use: connect*

**Solution:** Ephemeral ports were exhausted during upgrade due to multiple SQL database connections. The migration process was modified to reuse the USN during upgrade so a new database connection is not created for every record update.

**Reboot prompt does not appear on the client when migrating from 12.0 SBE to 12.1 SBE**

**Fix ID:** 2436381

**Symptom:** When using the Client Deployment Wizard to migrate from 12.0 Small Business Edition to 12.1 Small Business Edition, the client does not correctly display the reboot prompt.

**Solution:** The Client Deployment Wizard was modified to prevent a situation where the some installation files could be removed before the end of the setup. The Client Deployment Wizard was also modified to prevent a situation where incorrect switches were passed to msiexec.

**Upgrading SEPM from 11.x to 12.1 fails with installation rollback**

**Fix ID:** 2440655

**Symptom:** During server upgrade from 11.x to 12.1, the migration fails with a database connection error, and the installation rolls back. The server log contains the messages:

*INFO: Process SQL script file:MSSQLServerAmberMisc.sql*

*SEVERE: SQL Exception*

**Solution:** During migration of databases on SQL Server 2005 and 2008, table indices are temporarily disabled on the computer\_application and sem\_application tables. Table indices are re-enabled after migration.

**Network connectivity is lost after installing SEP 12.1 on a client running Microsoft Windows Live OneCare 2.x**

**Fix ID:** 2479660

**Symptom:** After installation of SEP 12.1 on a computer already running OneCare 2.x, network connectivity is lost. The user cannot connect to the internet or shared drives.

**Solution:** The sysplant.sys driver (Application and Device Control) was modified to allow OneCare 2.x to load correctly.

**Exception policy containing "\n" does not take effect**

**Fix ID:** 2480315

**Symptom:** An exception policy containing the string "\n" does not take effect.

**Solution:** Parsing of the exception policy was corrected to resolve this issue.

**Apache httpd.exe process crashes**

**Fix ID:** 2484177

**Symptom:** The Apache httpd.exe process crashes every few hours after upgrading from SEP 11.x to SEP 12.1.

**Solution:** A string was not terminated correctly. The string is now terminated correctly.

**The Doscan.exe "/list" parameter does not print the list of configured scans correctly on a Japanese operating system.**

**Fix ID:** 2491231

**Symptom:** The Doscan.exe "/list" parameter does not print the list of configured scans correctly on a Japanese operating system.

**Solution:** The locale of DoScan.exe was corrected to convert the Unicode scan name data to the appropriate character set.

**SEPM triggers unnecessary reinstallation or reconfiguration of clients when a client package is applied to a group**

**Fix ID:** 2493977

**Symptom:** A package is deployed with "Full protection." When another package is added to the group with the option "do not maintain existing feature set," this triggers reinstallation and reconfiguration of the client.

**Solution:** The feature list is now calculated correctly when assigning a package.

**SEP client notifies users about blocked devices when the notify option is disabled**

**Fix ID:** 2494090

**Symptom:** The administrator has configured the Application and Device Control policy with the option to disable "Notify users when devices are blocked." On the SEP client, the user is incorrectly notified when a device is blocked.

**Solution:** The default client behavior is now "do not modify." The client was modified to honor the policy setting.

**Application and Device Control policy rule does not work properly on some NEC computers**

**Fix ID:** 2497343

**Symptom:** An Application and Device Control policy rule does not block or allow an encrypted USB device correctly on a NEC computer.

**Solution:** Encrypted USB keys are not added to the Application and Device Control cache until after they are activated.

**Ping time increases every 5-10 pings when SEP 12.1 is installed**

**Fix ID:** 2497875

**Symptom:** When SEP 12.1 client is installed, the ping time increases every 5-10 pings.

**Solution:** The SEP client was modified to increase performance of ping times.

**Cannot change the SONAR setting after migrating from SEP 12.0 to 12.1**

**Fix ID:** 2505139

**Symptom:** After migration from SEP 12.0 to 12.1, it is not possible to change the SONAR setting in the migrated policy.

**Solution:** The SONAR policy object is now configured correctly during migration.

**Symantec Network Access Control (SNAC) Enforcer crashes while generating the server list**

**Fix ID:** 2525069

**Symptom:** When a new management server list is applied to a Gateway Enforcer, the Enforcer may enter a crash loop until the server list is replaced.

**Solution:** A SNAC Enforcer buffer was modified to prevent a spinlock condition.

**SNAC Enforcer disk space is depleted when the debug log is enabled**

**Fix ID:** 2319926/2407167

**Symptom:** When the SNAC Enforcer debug log is enabled, the Enforcer runs out of free disk space and no further entries can be written to the kernel log.

**Solution:** Debug logging now stops automatically if the free disk space is lower than 512 megabytes.

**Apache httpd.exe process consumes 100% CPU after migration from SEP 11.x to 12.1**

**Fix ID:** 2479435/2489380

**Symptom:** Apache httpd.exe process consumes 100% CPU after migration from SEP 11.x to 12.1.

**Solution:** Access to a cache table was modified to prevent a condition in which multiple thread accesses resulted in an infinite loop.

**A notification for "new risk detected" is triggered repeatedly, despite longer damper setting**

**Fix ID:** 2497657, 2212158

**Symptom:** The damper setting on a notification for new risks is configured for a specific time value. The first risk triggers the notification correctly. Subsequent risks before the damper period time incorrectly trigger the notification.

**Solution:** The damper option on notifications was modified to prevent this issue.

**SEPM application control log filter 'caller process' does not affect the data returned**

**Fix ID:** 2535320/2536938

**Symptom:** When filtering the application control log in SEPM, supplying a value for the caller process does not filter the resulting log data.

**Solution:** The caller process name is now inserted correctly into the DB query.

**Gateway Enforcer blocks traffic in learning mode**

**Fix ID:** 2517954

**Symptom:** When the Gateway Enforcer is in "learning mode," it incorrectly blocks traffic that should be allowed.

**Solution:** A driver was modified to resolve an issue with the packet length.

**“Download Insight is malfunctioning” appears after upgrade from SEP 11.0 to SEP 12.1**

**Fix ID:** 2496842

**Symptom:** When a SEP 11.0 client is upgraded to SEP 12.1, the following message appears in SEP UI:

*Download Insight is malfunctioning*

In addition, the event log contains the following error:

*Event ID 74 "SONAR generated the error: code 0: explanation: Definition error"*

**Solution:** If the SEPM database does not yet include LiveUpdate content, the auto-upgrade process copies the content from the full package to create a delta for the client.

**SEPM client view does not sort clients correctly**

**Fix ID:** 2579317

**Symptom:** In the SEPM client view, sorting does not work correctly on some columns, such as Policy Serial Number and IP address.

**Solution:** The SEPM console was modified to sort the columns correctly.

**Some clients cannot pass authentication in "Built-in" transparent mode after upgrade from SEP 11.0 to SEP 12.1**

**Fix ID:** 2579709

**Symptom:** After migration from SEP 11.0 to SEP 12.1, a client cannot pass authentication in "built-in" transparent mode. During migration, SNAC incorrectly restores the settings from

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\NAC\SNAC*

to

*HKEY\_LOCAL\_MACHINE\system\currentcontrolset\services\RASMAN\ppp\EAP*

**Solution:** SNAC no longer restores the transparent mode registry during migration. The transparent mode settings have been moved to the SymRasMan component.

**SEPM command status and details windows alternate focus back and forth**

**Fix ID:** 2406154

**Symptom:** In the SEPM command status screen, when auto-refresh is configured and a details window is open, focus of the two windows may alternate back and forth.

**Solution:** The SEPM console was modified to refresh each page without alternating focus.

**Estimated package size does not change between "all" and "basic" content types**

**Fix ID:** 2406187

**Symptom:** When exporting a package from SEPM, there is a choice to select content for the package. For both "all content" and "basic content" the size is constant and does not change.

**Solution:** SEPM now correctly shows the estimated package’s size, dependent on content type selection.

**Date format is inconsistent in SEPM console**

**Fix ID:** 2406473

**Symptom:** The date format used in the SEPM console inconsistently uses both English (UK) format and English (American) format. English (American) format is used for client properties and the policy serial number. English (UK) format is used for virus definition date on the clients tab.

**Solution:** The SEPM console was modified to consistently use English (American) format when applicable.

**"This webpage you are viewing is trying to close the window" is displayed after adding an application exception from the Tamper Protection log**

**Fix ID:** 2407285

**Symptom:** SEPM displays a message "This webpage you are viewing is trying to close the window" after adding an application exception from the Tamper Protection log. The issue occurs if Internet Explorer 7 or 8 is installed. Both the Java console and the web console are affected.

**Solution:** The SEPM console was modified to use a different JavaScript function to avoid the warning message.

**Enterprise SEPM exports a Small Business Edition client**

**Fix ID:** 2407293

**Symptom:** An Enterprise SEPM has applied a license that supports both Enterprise and Small Business. The Enterprise SEPM exports a Small Business client instead of an Enterprise client.

**Solution:** SEPM was modified to include the server's product type into the license data.

**Number of trusted files shown in the client scan interface is different compared to the Windows event log**

**Fix ID:** 2407331

**Symptom:** The number of trusted files shown in the SEP UI after a scan is different than the number shown in the Windows event log.

**Solution:** The number of trusted files is now calculated in a consistent way and matches in all locations.

**Endpoint Status "view details" report shows IP address as X.X.X.255 for all clients**

**Fix ID:** 2409780

**Symptom:** On the SEPM home page, the Endpoint Status "view details" report lists all clients with IP address ending in .255.

**Solution:** The SEPM console was modified to show the correct IP addresses for clients in this report.

**SEPM home page displays out-of-date license information**

**Fix ID:** 2414134

**Symptom:** The SEPM home page may display out-of-date license information after a new license is applied. The license information is corrected on the next automatic refresh.

**Solution:** SEPM was modified to refresh the home page automatically when a new license is applied.

**Client Changes report displays duplicate clients**

**Fix ID:** 2416097

**Symptom:** Clients that change groups are incorrectly shown in the "client changes" report, resulting in duplicate data.

**Solution:** Clients or users that change groups are no longer shown in the "client changes" report.

**SEPM does not use the configured email server**

**Fix ID:** 2417214

**Symptom:** In some cases, SEPM may send email directly to the recipient(s), instead of using the configured email server. The SEPM log may contain the message "Sending Email Failed for following email address…"

**Solution:** SEPM was modified always to use the configured email server.

**Blue screen error referring to "sysplant.sys" occurs when running ThinApp version of Internet Explorer 6**

**Fix ID:** 2424905

**Symptom:** A blue screen error that refers to "sysplant.sys" occurs when running ThinApp version of Internet Explorer 6.

**Solution:** The Application and Device Control Driver, sysplant.sys, was modified to prevent this crash.

**Client inventory details report is truncated**

**Fix ID:** 2425965

**Symptom:** The Quick Report for Computer Status > Client Inventory displays only the first half of the report.

**Solution:** SEPM was corrected to show the entire report.

**Hyper-V host loses network connection when firewall is enabled**

**Fix ID:** 2426193

**Symptom:** On a computer running as a Hyper-V host with a virtual network linked to a physical network card, when the firewall is enabled all network traffic on the host is stopped. Disabling the firewall and resetting the network connection returns the network to normal operation. Only the host is affected; virtual machine network access is not affected.

**Solution:** The Teefer.sys driver was modified to correct a compatibility issue between Teefer.sys and the Microsoft Bridge.sys driver.

**SEP client user interface cannot be launched**

**Fix ID:** 2427019

**Symptom:** After installation of SEP 12.1, the SEP client user interface cannot be started. The user interface stops responding after launch.

**Solution:** A deadlock between two components, SmcGui.exe and SymCorpUI.exe, was resolved to prevent this hang.

**Client receives the auto-upgrade package a second time after being moved between groups**

**Fix ID:** 2427171/2427215

**Symptom:** A client is auto-upgraded from SEP 11.0 to SEP 12.1. The group has the "maintain existing client features" option unchecked. After auto-upgrade, the client is moved to a new group. When the client is moved back to the original group, it receives the package and attempts to install SEP 12.1 again.

**Solution:** TruScan, NTP and Core were added to the pre-defined feature list.

**"Core" feature missing from Config.xml**

**Fix ID:** 2427195

**Symptom:** The "Core" feature is missing from Config.xml when a package is applied to a group and "maintain existing client features" is unchecked.

**Solution:** The Core feature was added to the default feature list.

**Number of trusted files is not visible in the logs**

**Fix ID:** 2427297

**Symptom:** Scan results for trusted files do not show in the client scan log. The number of trusted files is shown on the client scan UI during a scan, and in SEPM when monitoring a scan.

**Solution:** A column for "Trusted files" was added to the AV scan log.

**Proxy settings are not replicated**

**Fix ID:** 2429252/2431717

**Symptom:** Proxy settings are not replicated after reboot if the user is not logged in during the attempt.

**Solution:** The replication job is now executed after the console login.

**Java application loses connection after SEP 12.1 client is installed**

**Fix ID:** 2429404

**Symptom:** Under heavy network traffic conditions, some Java applications that transfer data over the network may lose connection after SEP 12.1 is installed.

**Solution:** An internal buffer cache in the firewall driver, Teefer.sys, was increased to avoid this issue.

**"Symantec CDStart Menu has stopped working" message when running setup.exe**

**Fix ID:** 2430407

**Symptom:** When setup.exe is executed from a very long path, setup fails to start and displays the message "Symantec CDStart Menu has stopped working."

**Solution:** A buffer in setup.exe was increased to allow the setup to run from a very long path.

**Risk Distribution by Detection Method report displays too many Tamper Protection events**

**Fix ID:** 2430571

**Symptom:** The Risk Distribution by Detection Method report displays too many Tamper Protection events.

**Solution:** The query was modified to filter and display only Tamper Protection events.

**Default Install vs. Custom Install of SEPM is confusing**

**Fix ID:** 2430626

**Symptom:** During installation of SEPM there is a choice for "Default configuration" or "Custom configuration." The choices do not have supporting text to describe the options.

**Solution:** The SEPM installation/configuration wizard was modified to display the following:

*Default configuration (fewer than 100 clients)*

*Custom configuration (more than 100 clients, or custom settings)*

**SEPM fails to start after upgrade from SEP SBE 12.0 to SEP SBE 12.1**

**Fix ID:** 2431712

**Symptom:** After migration from SEP SBE 12.0 to SEP SBE 12.1 on a 64-bit computer, the SEPM service fails to start and the administrator is unable to login to the console. The file "SecarsRes.dll" is missing after migration.

**Solution:** The SEPM installer was modified to prevent removal of the "SecarsRes.dll" file during migration.

**Green dot does not display after repairing the SEP client**

**Fix ID:** 2434409

**Symptom:** The client is connected to the SEPM and displays the green dot in the system tray icon. After repairing the SEP client using the Add/Remove Programs Control Panel, the green dot is missing.

**Solution:** The installer was modified to correct a condition where a registry key was set incorrectly during the repair operation.

**Insight and CAT servers landing page are not customer-friendly**

**Fix ID:** 2435551

**Symptom:** When customers try to verify if they can reach the reputation servers, they are greeted with a certificate error, then a blank page.

**Solution:** When accessing these servers via a web browser, a customer-friendly web page now appears.

**Cannot resize the column width on the Clients tab within the SEPM Console**

**Fix ID:** 2435614

**Symptom:** Not all data is visible within the fields on the Clients view within the SEPM Console.

**Solution:** Added tooltips which now show the data in the field being viewed.

**Client shows as offline within SEPM even though it is functional on the endpoint**

**Fix ID:** 2436933

**Symptom:** Within the SEPM console, the client status is showing as "offline". On the endpoint, the SEP client is functioning as expected.

**Solution:** Resolved by changes to the client recognition logic. The "hardware ID" and "known client ID" values are now handled differently within SEPM to ensure that clients are correctly recognized by the Manager.

**Duplicate client entries showing in the SEPM console after cloning an endpoint**

**Fix ID:** 2436935

**Symptom:** After cloning an endpoint, each clone shows in SEPM with two entries. One entry shows the client as offline, and one is online.

**Solution:** Resolved by changes to the client recognition logic. The "hardware ID" and "known client ID" values are now handled differently within SEPM to ensure that clients are correctly recognized by the Manager.

**Higher than normal CPU usage while endpoint is idle**

**Fix ID:** 2436943

**Symptom:** Higher than expected CPU usage is noticed on an endpoint while the computer is idle.

**Solution:** Multiple performance improvements were made to the SEP client to reduce CPU usage.

**"Error 1920. Service Symantec Migration Service (SEPMasterServiceMig) failed to start" when upgrading from SSEP 5.1 client to SEP 12.1 client**

**Fix ID:** 2439998

**Symptom:** When upgrading clients from SSEP 5.1 to SEP 12.1, an intermittent error occurs. This error occurs when an older version of the dll remains on the system and is attempted to be loaded by a newer version of the driver.

**Solution:** Changed the upgrade logic to rename sysfer.dll on upgrade, preventing this error.

**Poor Lotus Notes email scanning performance**

**Fix ID:** 2338687

**Symptom:** Lotus Notes email performance is slow when Lotus Notes email protection is enabled.

**Solution:** Lotus Notes email scanning performance is improved by caching the scan results. Attachments are not rescanned if they have not changed. In addition, emails with multiple attachments are now passed to the virus scanner in one batch transaction.