TPM device does not display in SEPM

Fix ID: 1536046

Symptom: SEPM displays the message No TPM device when the client is installed on certain computers with newerTPM hardware types.

Solution: The Broadcom TPM chipset is now supported.

Manual scan aborts prematurely

Fix ID: 1810080

Symptom: When virus definitions are reloaded during a manual scan or a scheduled scan, the scan aborts prematurely.

Solution: ccScan (Common Client) was modified to update definitions properly while a scan is in progress.

The firewall does not detect traffic on mobile broadband interfaces

Fix ID: 1928964

Symptom: The Symantec Endpoint Protection firewall does not detect traffic on a mobile broadband adapter. In addition, the adapter does not display Teefer2 Miniport entries in the device manager.

Solution: A new Teefer3 firewall driver was created to detect and monitor mobile broadband interfaces. Teefer3 provides better compatibility with other NDIS6 interfaces. Symantec Endpoint protection installs the new driver, Teefer3.sys, only on NDIS6-based operating systems (Windows Vista and above). The Teefer2.sys driver installs on legacy operating systems.

Lotus Notes email scanning performance

Fix ID: 1990686

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. In this case, the attachment is not rescanned if it has not changed. In addition, emails with multiple attachments are now passed to the virus scanner in one batch transaction.

Virus definitions out-of-date notification is not accurate

Fix ID: 1998671

Symptom: The Virus definitions out-of-date notification does not properly reflect the filter condition "include only clients which are currently online" This causes more clients than expected to display.

Solution: The client time stamp in the database was updated when a client is offline. In addition, replication of this state has been improved between servers.

A manual or scheduled scan causes demigration of offline files

Fix ID: 2000976

Symptom: In conjunction with some file storage solutions, a manual or scheduled scan results in demigration of offline files.

Solution: Symantec Endpoint Protection was modified to detect the file attribute FILE_ATTRIBUTE_REPARSE_POINT and to handle it properly.

Client installation rolls back if downloaded via LiveUpdate

Fix ID: 2006121

Symptom: Client installation on Windows 2008 R2 and Windows 7 rolls back if the package was downloaded by the server via LiveUpdate. The version of LiveUpdate (lusetup.exe) in Symantec Endpoint Protection 11.0 prior to RU5 is not compatible with Windows 7 and Windows 2008 R2. When the server downloads RU5 patches from LiveUpdate, the patch does not include lusetup.exe and SEPM uses the existing lusetup.exe from the database. This combined package of new RU5 + older lusetup.exe fails to install on Windows 7 and Windows 2008 R2.

Solution: Lusetup.exe is now included in the MSI installer file. It will also be included in future patches deployed via LiveUpdate.

BugCheck 50 (PAGE_FAULT_IN_NONPAGED_AREA) references SysPlant.sys

Fix ID: 2028463

Symptom: The computer crashes with BugCheck 50, {b12c8b80, 0, f8132ec2, 0} PAGE_FAULT_IN_NONPAGED_AREA (50) when Symantec Endpoint Protection 11.0 RU5 is installed. The BSOD references sysplant.sys.

Solution: The sysplant.sys driver was receiving an incorrect image size from the executable PE header. The driver was modified to prevent the crash.

Tamper protection and POP3 email scanner features are not documented as 32-bit only

Fix ID: 2037006

Symptom: The tamper protection and POP3 email scanner features are not documented as 32-bit only.

Solution: The "Read Me.html" file contains an update for this issue:

Some features / msi codes are only available on 32-bit systems.

The table on page 194 of the Installation Guide for Symantec™ Endpoint Protection and Symantec Network Access Control, entitled Symantec Endpoint Protection client features, has omissions. It fails to specify that the following capabilities are only available on 32-bit systems:

- SymProtectManifest
- POP3SMTP

Centralized exceptions for the file/folder window do not always appear on 64-bit computers

Fix ID: 2038170

Symptom: When adding a security risk exception, the file/folder window does not appear.

Solution: The file system redirection logic was modified to properly display this window.

SEPM incorrectly shows that the client needs a reboot after an AV/AS-only migration

Fix ID: 2057158

Symptom: A client with only the AV/AS feature installed is migrated to a new release of Symantec Endpoint Protection. After migration, SEPM displays that the client requires a reboot, when in fact, a reboot is not required.

Solution: The installation reboot logic was modified to prevent this error for AV/AS-only migrations.

Antivirus detection display the message: Location: Unknown storage

Fix ID: 2059120

Symptom: When a threat is scanned and detected, the location of a threat displays the message Unknown Storage in the notification window.

Solution: The threat detection logic was updated to properly display the threat location in the notification window.

SEPM encounters frequent datastor errors while it processes AV logs

Fix ID: 2062984

Symptom: After configuring a system event notification, you receive a large number of notifications regarding a datastor error. The scm-server.log file contains the message: SEVERE: Datastore error in: com.sygate.scm.server.task.AgentLogCollector java.lang.NullPointerException.

Solution: An issue processing PTP logs was corrected to prevent the occurrence of this error message.

The startup scan type changes from active scan to full scan when a user logs into the computer

Fix ID: 2073440

Symptom: When one user logs off the computer, and a different user logs into the computer, the startup active scan may incorrectly change to a full scan and scan all files and folders.

Solution: During the log off process, a second copy of SmcGui.exe executed incorrectly and overwrote user scan settings with the default values. This caused the next startup scan to become a full scan. SmcGui.exe was modified to disallow a second startup scan within a single session.

Traffic logs viewed in SEPM are unresponsive or return inconsistent data

Fix ID: 2074036

Symptom: When traffic logs are viewed in SEPM, the query may time out or log retrieval may take long time when there are a large number of records in the database.

Solution: The queries used for retrieving log data were optimized.

Broadcast traffic to 00-00-00-00-00-00 and FF-FF-FF-FF-FF-FF are blocked

Fix ID: 2076184

Symptom: Broadcast traffic to 00-00-00-00-00-00 and FF-FF-FF-FF-FF-FF are blocked for all adapters (LAN, wireless, dial-up) if there is a rule blocking all traffic on a wireless device.

Solution: Broadcast traffic to these addresses is allowed to other adapters even if there is a block all rule for one adapter.

The documentation for Quarantine Server supported operating systems is incorrect

Fix ID: 2076637

Symptom: The documentation for Quarantine Server supported operating systems is incorrect.

Solution: The Read Me.html file now clarifies the supported operating systems:

Quarantine Server operating system support is not fully documented.

The operating system requirements listed on page 16 of the Symantec™ Central Quarantine Implementation Guide have been updated as follows:

The console is supported on the following operating systems:

- Windows 2000 Professional/Server/Advanced Server/Datacenter Server with Service Pack 3 or later
- Windows XP Professional with Service Pack 1 or later
- Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition

Note: The Quarantine Console was not tested on 64-bit operating systems.

The server is supported on the following 32-bit operating systems:

- Windows 2000 Professional/Server/Advanced Server/Datacenter Server with Service Pack 3 or later
- Windows XP Professional with Service Pack 1 or later
- Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition

Note: The Quarantine Server was not tested and is not supported on 64-bit operating systems.

The search client performance in SEPM is slow for limited administrators after upgrading to Symantec Endpoint Protection 11.0 RU6a

Fix ID: 2080254

Symptom: The search client performance in SEPM is slow for limited administrators after upgrading to Symantec Endpoint Protection 11.0 RU6a.

Solution: An issue with limited administrator privileges was resolved to improve search performance.

Symantec Protection Center 1.0 fails to edit multiple policy options for Symantec Web Gateway

Fix ID: 2081265

Symptom: Some properties of Symantec Web Gateway policy configuration cannot be saved through Symantec Protection Center 1.0.

Solution: Content lengths longer than 8192 bytes were being truncated. The HttpServletRequest was modified to improve stream input processing.

The System Log as exported by the Symantec Endpoint Protection client contains incorrect event categories

Fix ID: 2082984

Symptom: When the System Log is exported to a text file, the critical event in System Log is written as Information instead of Critical.

Solution: The System Log export code was modified to properly export the event categorySysLog.log file.

Account locked events are recorded as Login failed events in the SEPM database

Fix ID: 2084454

Symptom: When a SEPM administrator account is locked there is no specific account locked log entry in the database. It is logged as the generic message: login failed event.

Solution: A specific log message, account locked, was added for this situation.

Clients automatically switch from Computer mode to User mode and may automatically switch groups

Fix ID: 2084474

Symptom: A Computer-mode client is registered as a User-mode client, which may cause it to change groups inadvertently.

Solution: When a client is switched from User-mode to Computer-mode, all users associated with the record are now deleted.

Pause and Snooze options during a scan do not honor the setting as configured by policy

Fix ID: 2084865

Symptom: Using the Pause and Snooze options during a scan may incorrectly display the number of remaining sleeps available.

Solution: Pause and Snooze are now treated the same and both decrement the available sleep count number.

Display error in the French localized version of SEPM

Fix ID: 2087213

Symptom: The default client inventory report in the French localized SEPM (Rapports > Inventaire Client > Par Defaut) contains a display error.

Solution: The report was modified to resolve the display error.

Replication fails between two sites

Fix ID: 2087986

Symptom: Replication between two sites may fail if a firewall between the two sites is configured for a low TCP idle session timeout.

Solution: A session keep alive feature was added for replication to ensure the connection remains open for the duration of the replication.

The Upgrade Schedule option does not appear on the Add Client Install Packages page

Fix ID: 2092027

Symptom: The Upgrade Schedule option does not appear on the Add Client Install Packages page. If the window is resized, then the option appears.

Solution: Text components and the size of the window were modified to show all options.

Clients submit install data to Symantec during auto-upgrade even if the feature was disabled

Fix ID: 2093019

Symptom: After turning off data collection in the SEPM, the clients continue to submit their install data to exftpp.symantec.com during auto-upgrade. This issue does not occur if the exported package is installed manually or via the Client Deployment Wizard.

Solution: The setup.ini parsing logic for the CmdLine entry was modified to correctly enable or disable install data collection per policy.

The Change clients view option is global across all SEPM administrators, including limited administrators

Fix ID: 2093960

Symptom: When the client view is changed, it is changed globally for all SEPM administrators.

Solution: The client view settings are now saved per administrator. Each administrator can personalize the client view.

Changing the LiveUpdate content policy does not create an entry in the SERVER_POLICY.LOG

Fix ID: 2097325

Symptom: Changing the LiveUpdate content policy does not create an entry in the SERVER_POLICY.LOG. Other policy modifications are logged correctly.

Solution: A log entry was added to record when the LiveUpdate content policy is changed.

SEPM logs an invalid log record error when processing PTP commercial application detections

Fix ID: 2097874

Symptom: PTP detects a commercial remote control application (for example Winvnc.exe), which is quarantined per administrator policy. The remediation of this application requires a restart to remove related registry information. After reboot, the ERASER reboot processing attempts to log the threat data but, because the file is in quarantine, ERASER is unable to calculate certain details (file size, hash, etc.) and logs them as empty. The empty log data results in the message: invalid log record.

Solution: The application properties are saved before quarantine and reboot. After reboot, the properties are restored and logged properly.

AV log data is not transferred to SEPM from AVMan.log

Fix ID: 2098023

Symptom: AV log data is not transferred to SEPM from AVMan.log.

Solution: Symantec Endpoint Protection 11.0 clients prior to MR4-MP2 could, in some instances, write very large entries to the AVMan.log file. The client was modified to skip the invalid log entry and to resume processing the next entry.

SEPM console performance is degraded when viewing groups with a large number of clients

Fix ID: 2099312

Symptom: When the default filter is set to 1000 clients per page, the console takes a long time to display the results.

Solution: The client query was optimized to enhance performance of the client view.

Administrators with full rights or policy management rights cannot edit or create policies

Fix ID: 2100572

Symptom: Administrators with full rights or policy management rights cannot edit or create policies.

Solution: An internal setting to determine whether the policy is read-only was not correctly set. SEPM was modified to resolve this condition.

Access to network files is slow when Application and Device Control is enabled

Fix ID: 2100901

Symptom: Access to files on network shares, mapped or \\, is slow when the Device Access Check feature of Application and Device Control is enabled.

Solution: Symantec Endpoint Protection was modified to check if the path is a remote drive before accessing certain device parameters.

Unexpected scheduled scans after client migration

Fix ID: 2108139

Symptom: After migrating from Symantec Endpoint Protection 11.0 RU5 to RU6, an unexpected scheduled scan starts.

Solution: The migration process properly invalidates scan randomization values if migrating from a version that does not support the feature.

The registry value AllowManualLiveupdate is not restored to match the applied policy on Symantec Endpoint Protection restart

Fix ID: 2109675

Symptom: The registry value AllowManualLiveupdate is changed when the computer is restarted, and is not restored to match the policy.

Solution: Symantec Endpoint Protection was restoring this key only when the policy changed. Symantec Endpoint Protection now restores this key on every start.

Issuing command from SEPM to a single client results in a "null error

Fix ID: 2109735

Symptom: When logged in to SEPM as a Limited Administrator, an attempt to run a command on a specific client results in a null error." After acknowledging the error, a success dialog box appears, but the command is not executed or displayed on the Monitors page. The SEPM log may show the following errors:" duplicated primary key"(SQL Server) or "Primary key is not unique" (embedded DB) or "SEVERE: Command [ScanNow_Quick] doesn't contain hardware keys".

Solution: This error occurred when two clients had the same hardware key, or when a group has a stale deleted entry in the database. SEPM now prevents the error by removing the duplicate hardware key or by properly marking the group as deleted.

Juniper SSL VPN connection is not detected correctly by location awareness

Fix ID: 2114448

Symptom: The client switches to an incorrect location when connected via Juniper SSL VPN.

Solution: Juniper SSL VPN is no longer treated as Ethernet. It is now properly filtered by description.

Auto-upgrade fails after day 1 of a multi-day schedule

Fix ID: 2114757

Symptom: Auto-upgrade stops after the first day of a multiday schedule, after which clients fail to process the upgrade package.

Solution: SEPM was incorrectly regenerating client packages and deltas if it was restarted during the multi-day schedule. This caused clients to download incorrect deltas that failed to apply correctly. SEPM no longer modifies packages and deltas on restart, unless the install data collection setting is changed. In addition, the client now checks to see if the download package is larger than expected. If this occurs, the client requests a new download.

Unable to view packet data in the traffic logs. The raw packet log information is not displayed in the packet log details

Fix ID: 2118054

Symptom: Log onto the SEPM console, go to Monitors – Logs Network Threat Protection – Packet Logs. View the details of one of the records. All content from the Packet Viewer and below is missing when you view the details.

Solution: SEPM uses ODBC functions to retrieve binary data from SQL server database. In some environments the ODBC functions fail. In this case, the administrator can configure the Microsoft PHP driver for SQL Server instead of ODBC. When the PHP driver (extension name 'sqlsrv') is enabled, SEPM uses the new driver to access the database. To enable the new driver:

1. Install the Microsoft SQL Server 2008 Native Client:

For X86 OS: http://go.microsoft.com/fwlink/?LinkID=188400&clcid=0x409

For X64 OS: http://go.microsoft.com/fwlink/?LinkID=188401&clcid=0x409

2. Download the Microsoft Drivers for PHP for SQL Server:

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=80e44913-24b4-4113-

8807-caae6cf2ca05

3. Unzip SQLSRV20.exe and copy “php_sqlsrv_53_ts_vc6.dll” and “php_sqlsrv_53_nts_vc6.dll” to the directory “<SEPM Install Folder>\Php\ext

4. Open “<SEPM Install Folder>\Php\Php.ini” and add the following two lines:

extension=php_sqlsrv_53_ts_vc6.dll

extension=php_sqlsrv_53_nts_vc6.dll

5. Restart the SEPM service.

Ping Flood DoS detection on valid application traffic

Fix ID: 2118136

Symptom: False positive ping flood attack.

Solution: The ICMP packet rate and length were increased to avoid Ping Flood Attack false positives.

Saved Outlook attachments result in 0-byte files

Fix ID: 2118585

Symptom: File attachments with certain characters are saved with a size of 0 kB. This occurs when a message is sent from a Chinese simplified computer to a Japanese or Chinese traditional computer.

Solution: A check was added for certain characters in the file name to prevent 0-byte files from being created.

Syslog risk events are missing source IP address for infected client computers

Fix ID: 2119243

Symptom: Syslog risk events have missing source IP address, or the source IP address is 0.0.0.0.

Solution: When the IP address cannot be determined, or is reported as 0.0.0.0, it is replaced with a blank string.

The Next Scheduled Scan date is displayed incorrectly

Fix ID: 2119571

Symptom: If a scheduled scan retry window is set to seven days, and the scan starts but is aborted, the Next Scheduled Scan date is shown as two weeks later.

Solution: The upper limit for the weekly scan retry time is three days. A value greater than three is not permitted. This limit is now enforced.

Infected and at-risk computers report is empty

Fix ID: 2125633

Symptom: When filtering the Infected and at-risk computers report by the action taken = quarantine, the resulting report is empty.

Solution: The underlying SQL query was modified to resolve this issue.

Commas in risk names or directory paths will corrupt exported .csv reports

Fix ID: 2132922

Symptom: If a risk name or directory path contains a comma, the exported .csv file is corrupt.

Solution: Risk names and directory paths are now enclosed in double quotes.

SNAC Enforcer can't register with SEPM

Fix ID: 2137544

Symptom: When the SEPM server CPU usage is high, the SNAC Enforcer fails to register with SEPM.

Solution: The algorithm used for SNAC Enforcer registration was improved.

DevViewer copy function does not work

Fix ID: 2137606

Symptom: When using the DevViewer tool from the unsupported folder of the Symantec Endpoint Protection DVD, the copy command does not function properly and the string is not copied to the clipboard.

Solution: The DevViewer tool copy function was corrected.

Continuous LiveUpdate results in a random server running LiveUpdate

Fix ID: 2138882

Symptom: When there are multiple SEPM servers in a single site and Continuous LiveUpdate is enabled, a random server runs LiveUpdate.

Solution: It is by design that a random server runs LiveUpdate when there are multiple servers in a single site. As a workaround, a new configuration option has been added to con.properties:

scm.server.liveupdate.disabled=<value>

If <value> is "1", "y", "true", or "yes," then LiveUpdate on that server is disabled. A customer can employ this workaround on multiple servers to ensure that LiveUpdate runs on the desired server.

Restricted users see instructions to click the Fix button in the Symantec Endpoint Protection client UI when there is no Fix button

Fix ID: 2138998

Symptom: A feature of Symantec Endpoint Protection is disabled, or definitions are out of date. The Symantec Endpoint Protection client UI prompts the user to click the Fix button. However, for a restricted Windows user, the Fix button is hidden.

Solution: If the user is restricted, the Fix button is not shown because the user does not have the necessary file and registry permissions to make changes to Symantec Endpoint Protection. Symantec Endpoint Protection no longer asks the user to click the Fix button if the Fix button is hidden.

Symantec Endpoint Protection Manager query for clients with out-of-date virus definitions returns Macintosh clients that have current definitions

Fix ID: 2140795

Symptom: Virus Definition Distribution quick report for clients with out-of-date virus definitions returns Macintosh clients that have current defs. Windows client results are correct.

Solution: The underlying SQL query was modified to resolve this issue.

Commands initiated from SEPM fail to run when executed against a group that contains User-mode clients

Fix ID: 2141332

Symptom: A command from SEPM is initiated to a group that contains User-mode clients. The command fails to run.

Solution: A primary key issue was corrected to resolve this issue.

The SEPM Home page reports that All systems are unprotected from W32.Imsolk.B@mm

Fix ID: 2141975

Symptom: The SEPM Home page reports that All systems are unprotected from W32.Imsolk.B@mm.

Solution: A string format issue in the virus definition revision caused SEPM to report that clients were unprotected. The string format issue was corrected.

The export of a client package via the SEPM Web console fails with the error: AjaxSwing error Internal Error

Fix ID: 2145546

Symptom: Exporting a client install package via the SEPM Web console fails with the error: AjaxSwing error Internal Error: Check log file for details and the stack trace... The SEPM Java console is not affected by this issue.

Solution: The SEPM Web console was modified to resolve this issue.

The Group drop-down menu in logs and reports includes groups that no longer exist

Fix ID: 2146940

Symptom: The Group drop-down menu in logs and reports includes groups that no longer exist.

Solution: SEPM was modified to correctly delete OU groups and sub-OU groups. Deleted groups no longer appear in the drop-down list.

Email notification body conflicts with the attached report

Fix ID: 2147037

Symptom: An email notification contains an attached report (.mht) with different computer totals than indicated in the email body.

Solution: Java and PHP queries were synchronized so that the notification body now matches the attachment.

Rtvscan.exe process terminates unexpectedly with exception code 40000015

Fix ID: 2147234

Symptom: Rtvscan.exe process terminates unexpectedly with exception code 40000015.

Solution: Rtvscan was modified to prevent the crash.

Quarantine Server returns missing content length error when files are submitted

Fix ID: 2148241

Symptom: The Quarantine console shows the status of submitted samples as Error, with the reason Missing Content-Length.

Solution: A redirection issue in WinHTTP was resolved to prevent this issue.

Excessive number of COH32.exe processes

Fix ID: 2152553

Symptom: Task Manager shows a large number of running or stuck COH32.exe processes.

Solution: Rtvscan was modified to prevent the launching of duplicate COH32.exe processes.

Some events may be omitted from SEPM external logging

Fix ID: 2152670

Symptom: Some events may be omitted in external logging from the SEPM. For example, only the first of a series of different risk detection events in a short time span may be listed in syslog or dump files, even though all events can be seen in the risk logs when viewed in the SEPM.

Solution: SQL queries were modified to prevent data loss.

ClientRemote.exe process terminates unexpectedly with the special exception code c000000d

Fix ID: 2158061

Symptom: ClientRemote.exe process terminates unexpectedly with the special exception code c000000d.

Solution: A string format issue in ClientRemote.exe was corrected to prevent this crash.

The Virus Definitions Distribution report shows incorrect results for Macintosh clients

Fix ID: 2161348

Symptom: The Virus Definitions Distribution report may show more Macintosh clients than exist in the environment.

Solution: The report was incorrectly showing some Windows clients as Macintosh clients. The SQL query was updated to resolve this issue.

Scan start and end date/time are identical if scan continues beyond midnight local time

Fix ID: 2162894

Symptom: When a manual or scheduled scan continues beyond midnight local time, the start time is written to one log file and the end time is written to a second log file. The scan history shows the same date for "Started On" and "Completed" if the log retention settings are such that the log has been purged from the computer.

Solution: The Completed scan time is now shown as empty if it cannot be determined from the log files on the disk.

The remote console auto-populates the incorrect IP address in login console

Fix ID: 2163694

Symptom: On a computer with multiple network cards, the remote console may auto-populate with an incorrect, non-routable IP address.

Solution: The remote console now auto-populates with the IP address as determined by the browser session.

Client totals in Protection Content Versions report do not match the sum of individual counts

Fix ID: 2164519

Symptom: Client totals in the Protection Content Versions report do not match the sum of the individual client counts.

Solution: The bar chart and table were corrected so that the client totals add up correctly.

Administrator-defined scheduled scan settings are not migrated properly from SAVCE 10.1 to SEP 11.0

Fix ID: 2165113

Symptom: Administrator-defined scheduled scan settings for Macro viruses and Non-macro viruses are not properly migrated from SAVCE 10.1 to SEP 11.0

Solution: The SEPM console will use the default values for display if no setting can be determined for MacroVirusAction, NonMacroVirusAction or SecurityRisksAction. When policies are applied, the default values are also used if they do not exist. In addition SEPM will print message to the log: SEVERE - The AV Policy: <name> is corrupt, Please check and update.

Unknown Exception errors in Scm-server.log and PackagePublisherTask.log due to a corrupt AV/AS policy

Fix ID: 2188666

Symptom: The Scm-server.log and PackagePublisherTask.log file contain Unknown Exception errors due to a corrupt AV/AS policy.

Solution: The SEPM console will use the default values for display if no setting can be determined for MacroVirusAction, NonMacroVirusAction or SecurityRisksAction. When policies are applied, the default values are also used if they do not exist. In addition SEPM will print message to the log: SEVERE - The AV Policy: <name> is corrupt, Please check and update.

SEPM console hangs when you select Detected Processes in the TruScan Proactive Threat Scan Exceptions menu

Fix ID: 2166540

Symptom: In the SEPM console, go to Policies | Centralized Exception | <policy> | Edit | Centralized Exceptions | Add | Windows Exceptions | TruScan Proactive Threat Scan Exceptions | Detected Processes. The SEPM console hangs when you select Detected Processes if there a large number of client groups.

Solution: A SQL query was optimized for better performance when there are a large number of client groups.

A Client view export from SEPM only contains the first 1,000 entries

Fix ID: 2168449

Symptom: In the SEPM Client view, when a search query results in more than 1,000 clients, the export in .CSV format contains only the first 1,000 entries.

Solution: The query was modified to return all records in the exported .CSV file.

Completed scan window cannot be closed due to a missing Close button

Fix ID: 2171285

Symptom: If multiple manual or scheduled scans start in series, the scan windows cannot be closed because the Close button never appears.

Solution: The scan window user interface was modified to show the Close button when the scan completes.

Duplicate entries in SEPM external logging

Fix ID: 2171952

Symptom: SEPM database maintenance generates duplicate entries in SEPM external logging (syslog or dump file records). For example, Virus found or Security risk found events that have already been logged appear again in the external logging at a later date, with a time stamp corresponding to the default midnight maintenance.

Solution: The SQL query for external logging was modified to prevent deleted records from appearing.

The Packet Log detail shows incorrect port information for TCP and UDP

Fix ID: 2173173

Symptom: In the Packet Log viewer, port number, sequence number, and ack number may show negative values. The checksum may be shown in the incorrect host byte order.

Solution: The Packet Log viewer was modified to use unsigned formatting for port, sequence, and ack numbers. Network byte order is now used for the checksum. In addition, the font has been changed to fixed width for better readability.

Location Awareness template for Safenet Softremote incorrectly identifies the connection as Juniper Netscreen VPN

Fix ID: 2174607

Symptom: A location awareness policy contains two locations: one for Juniper NetScreen VPN and one for Safenet Softremote. Clients running Safenet Softremote incorrectly switch to the Juniper Netscreen location.

Solution: Juniper NetScreen VPN and SafeNet SoftRemote VPN are now merged into a single location template.

SEPM console check boxes can be selected by clicking outside the bounds of the check box

Fix ID: 2179119

Symptom: In the SEPM remote console, some check boxes, for example SEPM | Clients | Group | Properties | Block New Clients) can be selected without clicking directly on the check box.

Solution: The remote console UI was modified to distinguish between clicks on the description vs. the check box.

Symantec Endpoint Protection client downloads a full.zip file instead of the delta

Fix ID: 2179554

Symptom: If the SEPM server heavily loaded, a client requesting a delta will not get a reply from the server in a timely manner. The client retries again and obtains a "full.zip" file instead of the delta.

Solution: SEPM now correctly handles subsequent requests from clients and allows the first one to complete before serving another request.

A notification is displayed for blocked device, even if the Notify users when devices are blocked option is disabled

Fix ID: 2183345

Symptom: The application and device control policy has disabled the option Notify users when devices are blocked. When the client user accesses a blocked device, Symantec Endpoint Protection may display a notification.

Solution: The check box label was modified to read as follows: Notify users when devices are blocked or unblocked.

A limited administrator cannot change AV policies

Fix ID: 2183562

Symptom: Administrators with limited rights who can manage a certain group cannot manage AV/AS policies.

Solution: The remote console was modified so that second or third level windows inherit the privileges from the parent window.

Migrating from SAVCE 10.1 to Symantec Endpoint Protection 11.0 does not reboot the client as expected

Fix ID: 2185290

Symptom: A Symantec Endpoint Protection client installation package is marked for silent restart after installation. The package is deployed to the SAVCE 10.1 client, but the client does not restart as expected at the end of the migration.

Solution: A Windows function call was not returning properly and did not pass the reboot status to the installer. The code was modified to pass the correct status to allow the reboot to occur.

A group name may appear more than once in the Group filter field when you create a report

Fix ID: 2185329

Symptom: A group name may appear more than once in the Group filter field when you create a report.

Solution: The SEPM console was modified to correct any redundant group names in the filter creation window.

SEPM LiveUpdate server settings policy allows you to add to the internal LiveUpdate server list even though the list is inactive

Fix ID: 2188576

Symptom: SEPM LiveUpdate server settings policy allows you to add to the internal LiveUpdate server list even though the list is inactive.

Solution: User interface elements in the third-party LiveUpdate server panel are now controlled by LiveUpdate server status to prevent this issue.

Legacy SAVCE servers cannot send logs to SEPM

Fix ID: 2188759

Symptom: Legacy SAVCE servers may intermittently stop sending logs to the SEPM server. The legacy.sab file on the SEPM server does not maintain the proper configuration.

Solution: The legacy.sab file was being overwritten with an incorrect value when administrators logged into SEPM. SEPM was modified to persist the legacy.sab value correctly.

The Symantec Endpoint Protection client is unable to clean invalid content from the download folder

Fix ID: 2189176

Symptom: The Symantec Endpoint Protection client receives the message: not configured to update from SEPM. Temporary (.tmp) files remain in the directory %Program Files%\Symantec\Symantec Endpoint Protection\LiveUpdate and cannot be purged

Solution: The Symantec Endpoint Protection client was modified to correctly purge temporary content when it is no longer needed.

Notification delivery is inconsistent when configured with a damper period

Fix ID: 2189828

Symptom: Only one notification is received if threats are found at an interval greater than the damper period. For example, suppose the damper period is 20 minutes. If the same threat is reported every 25 minutes, only one notification is received.

Solution: The SQL query for notifications was modified to properly report notifications if a damper period is selected.

Exported risk logs in .CSV format does not show the IP address of the device with the risk

Fix ID: 2191485

Symptom: Exported risk logs in .CSV format does not show the IP address of the device with the risk

Solution: A column for "IP Address" was added to the exported risk log in .CSV format

The Symantec Endpoint Protection client risk log is inconsistent with the SEPM risk log for the same event

Fix ID: 2192871

Symptom: The Symantec Endpoint Protection client risk log indicates "restart required - quarantined" but SEPM risk log for the same event only shows "Virus found (Quarantined)".

Solution: A new STATUS column was added to the ALERTS table to track the status of the risk log (success vs. restart required). The SQL queries used for the risk log were modified to take this status into account to ensure the client and server risk logs are consistent.

smc.exe causes a high CPU load on Windows 2008 R2 Terminal Server

Fix ID: 2192985

Symptom: smc.exe causes a high CPU load on Windows 2008 R2 Terminal Server.

Solution: Smc.exe was optimized to reduce the frequency of enumerating terminal server sessions and processes.

SEPM log file contains the message: Datastore Error; For input string: "((1))"

Fix ID: 2194856

Symptom: The SEPM log for processing clients displays the following message:

Datastore Error; For input String: "((1))"

This results in the failure of SEPM to update client data.

Solution: A database API call was returning an unexpected value. SEPM was modified to correctly parse the value and avoid the exception.

The Rtvscan.exe process terminates unexpectedly with exception code 80000003

Fix ID: 2195830

Symptom: The Rtvscan.exe process terminates unexpectedly with exception code 80000003.

Solution: Additional error checking was added to Rtvscan.exe to prevent this crash.

Randomized scans run multiple times and are not consistent

Fix ID: 2196367

Symptom: On Windows 7, a weekly scheduled scan is configured with a randomization window. The scan may run multiple times within that window.

Solution: The randomized scan logic was optimized to prevent multiple scans from running in the same time window.

Wireless MAC address is not reported to SEPM server

Fix ID: 2197860

Symptom: When a wireless adapter is enabled, the adapter's MAC address is not reported to SEPM and does not appear in reports.

Solution: Out-of-date MAC entries in the LAN_DEVICE_DETECTED table are now cleaned properly. This was preventing the new MAC address from registering with SEPM.

TN3270 terminal emulation software causes the computer to hang when Symantec Endpoint Protection 11.0 is installed

Fix ID: 2197976

Symptom: When certain TN3270 terminal emulation software is installed, it may cause the computer to hang when Symantec Endpoint Protection 11.0 is installed

Solution: SSSensor.dll was modified to prevent a deadlock during packet examination.

SEPM home page Risk Per Hour charts show 100 events when only a single risk event is found

Fix ID: 2200505

Symptom: SEPM home page Risk Per Hour charts shows 100 events when only a single risk event is found.

Solution: The SEPM home page logic was modified to correct the Risk Per Hour chart.

Bugcheck D1 (DRIVER_IRQL_NOT_LESS_OR_EQUAL) references wpsdrvnt.sys

Fix ID: 2202918

Symptom: The computer crashes with BugCheck D1 (DRIVER_IRQL_NOT_LESS_OR_EQUAL (D1) when Symantec Endpoint Protection 11.0 is installed. The BSOD references wpsdrvnt.sys.

Solution: Additional error checking was added to wpsdrvnt.sys to prevent this crash.

AgentLogCollector-0.log contains an error regarding code page 65001 (UTF-8)

Fix ID: 2204547

Symptom: The following errors are displayed in the AgentLogCollector-0.log when SEPM is configured for a SQL 2008 server:

2010-10-14 18:58:21.893 FINE: SQLException: Failed to load data: SQLState =

S1000, NativeError = 0

Error = [Microsoft][SQL Server Native Client 10.0]This version of SQL Server

Native Client does not support UTF-8 encoding (code page 65001)

Using batch handler

Solution: SEPM was modified so that bcp.exe is never run in Batch Mode. In Bcp Mode, SEPM runs bcp.exe first and falls back to Batch Mode if any errors are encountered.

Broadcom network adapter configuration is modified unexpectedly when Symantec Endpoint Protection 11.0 is installed

Fix ID: 2213075

Symptom: The Broadcom network adapter Duplex configuration is unexpectedly changed when Symantec Endpoint Protection 11.0 is installed.

Solution: Symantec Endpoint Protection was modified with enhanced NDIS6 support in this release to resolve the issue.

SEPM remote console Home/Monitor/Report pages load very slowly or time out

Fix ID: 2216089, 2223013

Symptom: The three first pages (Home/Monitor/Report) in the SEPM remote console are very slow to load (5 minutes or more) and may time out.

Solution: A new stored procedure, and an index were added to optimize the Home/Monitor/Reports pages.

The Symantec Endpoint Protection client user interface displays green status for malfunctioning firewall

Fix ID: 2216186

Symptom: The Symantec Endpoint Protection client management system logs show the error "Firewall driver failed to open network adapter" and the firewall does not block connections as expected by policy. The client user interface shows the firewall is ON and functioning properly.

Solution: When the Teefer driver cannot be opened, SMC now correctly broadcasts red status to the user interface.

When SEPM machine locale is set to Thai, reports generated (risk, scan reports) from SEPM show the date 1/1/1970

Fix ID: 2216942

Symptom: When the SEPM machine locale is set to Thai, the reports that are generated (risk, scan reports) from SEPM show the date 1/1/1970.

Solution: The Symantec Endpoint Protection client was modified to save data with the Gregorian calendar format. SEPM was modified to detect and properly display any legacy logs in Buddhist calendar format.

The Comprehensive Risk Report shows discovered dates as 12/31/1969 in certain time zones

Fix ID: 2220016

Symptom: The Comprehensive Risk Report may show some dates as 12/31/1969 in some time zones.

Solution: SEPM was corrected to show the proper date, or to show Unknown if the date cannot be determined.

PTP scan results in a large amount of traffic to Samba file server

Fix ID: 2221915, 2235099

Symptom: The PTP scan in Symantec Endpoint Protection 11.0 enumerates the Start Menu .lnk files. If these link files resolve to a network share, the links are followed. A large number of Symantec Endpoint Protection clients running PTP scans simultaneously may result in a large amount of traffic to the network share.

Solution: The COH component was optimized to reduce the need to access the network share during PTP scans.

SEPM Web console OK button stops functioning after certain operations

Fix ID: 2223851

Symptom: The SEPM Web console OK button stops functioning after the LiveUpdate timeout interval is modified.

Solution: The Web console was corrected to resolve this issue.

Application and Device Control behaves differently in the Symantec On-Demand Protection virtual desktop

Fix ID: 2224081

Symptom: An Application and Device Control policy is configured to allow running wordpad.exe when it is launched under the Symantec On-Demand Protection virtual desktop environment. The policy behaves as expected in Windows XP, but not in Windows 7.

Solution: Operating System Protection (OSP) inheritance was modified on Vista and above operating systems to resolve this issue.

The SEPM console displays GMT time instead of local time on the Monitors/Reports pages after upgrading from Symantec Endpoint Protection 11.0 RU6a to RU6-MP2

Fix ID: 2227371

Symptom: After upgrading SEPM from Symantec Endpoint Protection 11.0 RU6a to RU6-MP2, the console always displays time as GMT instead of local time on the Monitors and Reports pages.

Solution: The time zone calculation logic in SEPM was corrected to resolve this issue.

IIS fails to start Secars.dll and cannot process clients

Fix ID: 2227598

Symptom: Secars is unable to receive the Tomcat client cache information (action=35) and fails to start.

Solution: IIS 7.0 changed the default limit for maximum allowed content length to 30 megabytes. If the Tomcat client cache exceeds this value, Secars fails to start. During SEPM installation/migration, the IIS 7.0 max allowed content length is changed to 500 megabytes.

SEPM administrators who log out of the Web console are not shown as logged out

Fix ID: 2229298

Symptom: The status report for online SEPM administrators is not accurate when administrators log on and off using the Web console. Administrators are shown as logged in when they are not.

Solution: The Web console was modified to ensure that the logout function executes properly. In addition, the logic to determine the online/offline status was enhanced.

The Reports to Include option for a Scheduled Comprehensive Risk Report is reset to the default when the filter is save as Default in Korean

Fix ID: 2230808

Symptom: The Reports to Include setting for a Scheduled Comprehensive Risk Report is reset to the default when the filter is save as Default in Korean.

Solution: A PreparedStatement is now used to query the filter by filter name.

Smc.exe process terminates unexpectedly with exception code e06d7363

Fix ID: 2232964

Symptom: When SMC is stopped with the command smc -stop, the smc.exe process may terminate unexpectedly with exception code e06d7363.

Solution: The Group Update Provider (GUP) feature in smc.exe was modified to prevent this crash.

SEPM fails to replicate some data in the SCANS table

Fix ID: 2236222

Symptom: SQL queries executed on the SCANS table on two replicated databases may show discrepancies. In some cases a client's last scan time is not identical, or one site contains client scan records that are missing on the other site.

Solution: Replication was enhanced with caching to ensure that the client scan data is replicated properly.

SEPM experiences multiple failures: failed replication, creation of 0-byte packages, and slow remote console access

Fix ID: 2237558, 2292931, 2240393

Symptom: SEPM experiences multiple failures: failed replication, creation of 0-byte packages, and slow remote console access.

Solution: A deadlock in a SQL query was resolved to prevent these issues.

Restoring SEPM database results in high CPU usage by SemSvc.exe

Fix ID: 2239986

Symptom: During a database restore, SemSvc.exe causes high CPU usage and does not recover.

Solution: An invalid client package in the database failed to import. During database restore, SemSvc.exe would attempt to import the package repeatedly. SemSvc.exe was modified to skip invalid client packages.

CygWin fatal error "couldn't allocate heap" when running Perl script with Application and Device Control enabled

Fix ID: 2241805

Symptom: The client has an active and enabled Application and Device Control policy. A Perl script running inside CygWin may fail with fatal error: couldn't allocate heap.

Solution: The Application and Device Control driver, sysplant.sys, was modified to use a different memory allocation method to prevent this error.

The Symantec Endpoint Protection system log displays Windows 7 clients as "Windows Vista"

Fix ID: 2241934

Symptom: A Symantec Endpoint Protection system log may incorrectly display the operating system as "Windows Vista" for a Windows 7 client.

Solution: The Symantec Endpoint Protection client now changes a Windows API call to properly determine the operating system version.

Embedded database version displayed on the SEPM console is not correct

Fix ID: 2244601

Symptom: The version of the embedded database is incorrect in the SEPM console (Admin | Servers | Local host database).

Solution: The embedded database version is now correctly updated in the schema during migration.

Updating the Install Data Collection setting causes an exception on the server

Fix ID: 2245924

Symptom: When updating the Install Data Collection setting in SEPM, the scm-server-0.log file may contain the error: SEVERE: PackageTask.publishPackages: Caught exception while unzipping client package!

Solution: After updating the IDC setting, the package task no longer includes 0-byte delta packages.

Application and Device Control policy causes a third-party application to consume 100% CPU

Fix ID: 2251285

Symptom: When Symantec Endpoint Protection is installed and an Application and Device Control policy is enabled, a third-party application consumes 100% CPU.

Solution: The Sysfer DLL was modified to correctly handle shadow copy.

SEPM log warns of PRIMARY KEY violation

Fix ID: 2253184

Symptom: The SEPM log contains the error message: SEVERE: Unknown Exception java.sql.SQLException: Violation of PRIMARY KEY constraint 'PK_SEM_COMPUTER'. Cannot insert duplicate key in object 'dbo.SEM_COMPUTER'.

Solution: A SQL query was modified to prevent the primary key violation.

Replication fails due to deadlock during ReplicationTask

Fix ID: 2253188

Symptom: Replication fails due to deadlock during ReplicationTask while processing SEM_CONTENT_DEL table.

Solution: The batch size for table replication was increased to resolve this issue.

SEPM is slow to process .dat files

Fix ID: 2273344

Symptom: SEPM is slow to process .dat files, causing the .dat files to build up in the AgentInfo folder. The Secars log may include the message: The disk space allocated for inbox is full.

Solution: The performance of AgentInfo was increased by adding an index and using several prepared statements.

NTP displays the message Waiting for updates after migration

Fix ID: 2275269

Symptom: An AV-only installation of Symantec Endpoint Protection is upgraded to one with firewall/NTP using the ADDLOCAL="Firewall" option to msiexec. After migration, the NTP stripe in the Symantec Endpoint Protection UI displays the message: Waiting for updates.

Solution: Network Threat Protection content was not being properly applied during migration. The DefUtils component was updated to resolve this issue.

Local user profiles become corrupted on Windows Vista and Windows 7 computers

Fix ID: 2291558

Symptom: Users are unable to log on to their local Windows profiles.

Solution: The method that Rtvscan.exe uses to monitor the user's scheduled scan registry has been enhanced to resolve this issue.

BugCheck 8E (KERNEL_MODE_EXCEPTION_NOT_HANDLED) references Sysplant.sys

Fix ID: 2291863, 2275174

Symptom: The computer crashes with BugCheck 8E (KERNEL_MODE_EXCEPTION_NOT_HANDLED) when Symantec Endpoint Protection 11.0 is installed. The BSOD references sysplant.sys.

Solution: The Application and Device Control driver (sysplant.sys) was modified to obtain file path data from the PEB structure.

AntiVirus definitions become stuck on a single revision until SMC is restarted or the computer is rebooted

Fix ID: 2296147

Symptom: AV definitions become stuck on a single revision and are not affected by a LiveUpdate. The client updates definitions only if the SMC.exe service is restarted or the computer is rebooted.

Solution: SMC.exe was modified to prevent a condition where it fails to apply new content because another type of content is pending.

Replication performance is decreased after upgrading to Symantec Endpoint Protection 11.0 RU6-MP2

Fix ID: 2305346, 2297935, 2312010

Symptom: Replication performance is decreased after upgrading to Symantec Endpoint Protection 11.0 RU6-MP2. A SQL query of the SEM_CONTENT table shows many stale entries.

Solution: SQL queries were optimized and stale entries in the SEM_CONTENT table are now removed during the sweeping task.

Large numbers of VDI sessions become unresponsive

Fix ID: 2315197

Symptom: In a virtual desktop infrastructure environment, VDI sessions running Symantec Endpoint Protection 11.0 may become unresponsive or hang

Solution: The COH component was modified to prevent a condition where it cannot properly determine the owner of a process.

After migration from SAVCE 10.1 to Symantec Endpoint Protection 11.0, clients report AV Engine Off until SMC service is restarted

Fix ID: 2334318

Symptom: A client is migrated from SAVCE 10.1 to Symantec Endpoint Protection 11.0. After migration, the Symantec Endpoint Protection clients report AV Engine Off.

Solution: Rtvscan was incorrectly reporting the AV Engine status due to the service name change between SAVCE and Symantec Endpoint Protection. Symantec Endpoint Protection now queries the proper service name.

A new help window is opened for every use of F1

Fix ID: 2349564

Symptom: A new help window displays each time the F1 key is pressed.

Solution: Before launching Windows Help (hh.exe), Symantec Endpoint Protection now checks whether the help has already been launched.