

Fix Notes for Symantec Endpoint Protection

12.1.3

Top Impacting Issues Resolved in this Release

After applying Microsoft update KB2781197 to a Windows 8 computer, the Symantec Endpoint Protection client installer fails

Fix ID: 3123310

Symptom: The following lines are from the SEP_INST.log generated from a failed installation attempt:

```
(SERVER) MSI (s) (04:18) [08:56:49:093]: Executing op:
CustomActionSchedule(Action=ShowServiceProgress,ActionType=3073,Source=BinaryDa
ta,Target=ShowServiceProgress,CustomActionData={3771A34D-2132-48EA-A486-
D62ECDF9D553};SOFTWARE\Symantec\Symantec Endpoint Protection;Executing install
script via service;)

(SERVER) MSI (s) (04:5C) [08:56:49:250]: Invoking remote custom action. DLL:
C:\WINDOWS\Installer\MSI6B0.tmp, Entrypoint: ShowServiceProgress

(UNKNOWN) ScriptGen: ShowServiceProgress() MSIRUNMODE_SCHEDULED

(UNKNOWN) ScriptGen: ShowServiceProgress() calling
WaitForSingleObject(scriptStarted) ...

(UNKNOWN) ScriptGen: ShowServiceProgress() WaitForSingleObject(scriptStarted)
returned WAIT_OBJECT_0

(UNKNOWN) ScriptGen: ShowServiceProgress() script execution failed.

(UNKNOWN) ScriptGen: ShowServiceProgress() reset script failure event.

(UNKNOWN) ScriptGen: ShowServiceProgress() is returning an error (so close to
the end!)

(UNKNOWN) CustomAction ShowServiceProgress returned actual error code 1603
(note this may not be 100% accurate if translation happened inside sandbox)
```

Solution: For installations on Windows 8, removed the option to enable/disable Windows Defender after install, as this is no longer supported. Windows Security Center (WSC) will automatically disable Windows Defender when Symantec Endpoint Protection registers with WSC.

"Query Failed" when exporting Symantec Endpoint Protection logs after upgrade to version 12.1.2 (12.1 RU2)

Fix ID: 3020735 / 3033993

Symptom: You can generate a report that includes log data of more than 24 hours old, but you cannot export that report to CSV.

Solution: Changed the way invalid data values are handled.

Network performance slows on Windows XP with Symantec Endpoint Protection 12.1 RU2 MP1 installed

Fix ID: 3180923

Symptom: Computers experience network performance problems when the Network Threat Protection (NTP) firewall component of the Symantec Endpoint Protection 12.1.2.1 (12.1 RU2 MP1) client is installed and enabled. Symptoms include:

- Copying files from a network location over Windows File Sharing takes significantly more time.
- Programs that are started from a network share take significantly longer to load.
- Ping responses take longer to return.

Solution: Modified the firewall to call the proper notification routine for Windows XP.

License seats are not counted properly in the Symantec Endpoint Protection Manager when using User Mode clients

Fix ID: 3034131

Symptom: When using User Mode clients, the number of licenses required is the number of computers where the Symantec Endpoint Protection client is deployed, as described in TECH163955. However in RU2, "seats used" are incorrectly counted as the number of users that have logged on per machine, which may lead to warnings that Symantec Endpoint Protection has been over-deployed.

Solution: Updated the licensing logic to count by agent only, not per user logged into the client computer.

Lotus Notes hangs after upgrading to Symantec Endpoint Protection 12.1.2 (12.1 RU2)

Fix ID: 3069578

Symptom: After an upgrade to Symantec Endpoint Protection 12.1.2 with the Lotus Notes plug-in enabled, Lotus Notes 8.5.3 hangs during or after the splash screen.

Solution: Updated the Lotus Notes Auto-Protect plug-in to check for a null pointer.

Replication fails with a Java error "GC overhead limit exceeded"

Fix ID: 2920217/3055586

Symptom: After upgrading to Symantec Endpoint Protection Manager 12.1.2 (12.1 RU2), replication is failing with the exception message "OutOfMemoryError: GC overhead limit exceeded."

Solution: Modified the replication function to avoid a scenario where object references could be recursively checked.

Symantec Endpoint Protection client fails to report reboot status to Symantec Endpoint Protection Manager after upgrade to 12.1.2 (12.1 RU2)

Fix ID: 2871345/3069464

Symptom: The Symantec Endpoint Protection Manager console shows "Restarted Required" as "No" for clients which have not restarted after the upgrade to 12.1 RU2. The deployment status in the Symantec Endpoint Protection Manager console displays the message, "To provide complete protection Symantec Endpoint Protection requires this computer to restart." The Symantec Endpoint Protection user interface on the client also shows that a restart is needed.

Solution: Modified the upgrade process to send the latest opstate data to the Symantec Endpoint Protection Manager server.

High disk space is being consumed by C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\Importpackage

Fix ID: 2914951/3118490

Symptom: Hard disk on the Symantec Endpoint Protection Manager server is running low on space due to files building up in C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\Importpackage.

Solution: Added an additional attempt to forcefully remove the files in the import folder if the first delete fails.

Computer status log is empty when Windows Server 2008 is chosen as the operating system filter

Fix ID: 3048159/3099396

Symptom: The computer status log is empty when Windows Server 2008 is chosen as an advanced filter for the operating system.

Solution: Fixed an issue with the operating system identifiers.

httpd.exe process terminates unexpectedly with a stack overflow

Fix ID: 3177738

Symptom: The Apache service (httpd.exe) terminates unexpectedly and the Symantec Endpoint Protection Manager becomes unresponsive.

Solution: The server will reject application learning data from the client if the compressed file size is above 480 kilobytes. The threshold for data rejection is configurable via a new registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPMMaxClientAppLogSize (DWORD)

The value is the log data size in kilobytes. Log data above this threshold will be rejected. The threshold may be raised or lowered as needed by the administrator.

Groups with large numbers of clients load slowly when a non-System Administrator logs on to Symantec Endpoint Protection Manager using a remote console and authenticate with a standard Windows account

Fix ID: 2760909

Symptom: Groups with large numbers of clients load slowly when an Administrator over a specific domain, or a limited administrator with permission to a specific client group, log on to Symantec Endpoint Protection Manager using a remote console and authenticate with a standard Windows account.

Solution: Improved the checks for administrator checks and reduced duplicate queries to improve performance.

Clients that have not connected for more than 30 days still appear in the Symantec Endpoint Protection Manager

Fix ID: 2993984

Symptom: Clients that have not connected for more than the specified period of time (default value is 30 days) still appear in the Symantec Endpoint Protection Manager, even though you specify to delete these clients.

Solution: Changed the criteria on which the database sweeping performs the check to delete disconnected clients.

With User Account Control (UAC) on, "Disable Symantec Endpoint Protection" option is grayed out for domain administrators

Fix ID: 2610970

Symptom: With User Account Control on, "Disable Symantec Endpoint Protection" option is grayed out for domain administrators when they right-click on the Symantec Endpoint Protection tray icon.

Solution: Changed to now use a different security token associated with the user in order to determine whether they have the appropriate rights to enable or disable Auto-Protect.

Location switching performance slows after installing Symantec Endpoint Protection 12.1.1

Fix ID: 2794640

Symptom: Location switching in Symantec Endpoint Protection 12.1.1 (12.1 RU1) is noticeably slower than Symantec Endpoint Protection 11.0.7.1 (11.0 RU7 MP2).

Solution: Refined the timing checks to improve location switching speed.

BugCheck 19 (BAD_POOL_HEADER), 50 (PAGE_FAULT_IN_NONPAGED_AREA), or D1 (DRIVER_IRQL_NOT_LESS_OR_EQUAL) references various drivers

Fix ID: 2860505

Symptom: The Symantec Endpoint Protection client experiences various blue screens, including BugCheck 19 (BAD_POOL_HEADER), 50 (PAGE_FAULT_IN_NONPAGED_AREA), or D1 (DRIVER_IRQL_NOT_LESS_OR_EQUAL).

Solution: Updated the SymNetDrv component to avoid a buffer overflow.

Server logs show many SQL exception messages about SecurityAlertNotifyTask

Fix ID: 2913613

Symptom: The message "java.sql.SQLException: Connection is closed," which references SecurityAlertNotifyTask, appears repeatedly in the scm.server.log on Symantec Endpoint Protection Manager.

Solution: Now checks whether connection is already closed before attempting to close it.

CACHEINSTALL=0 parameter to msixexec.exe still places files into the "Cached Installs" folder

Fix ID: 2926512

Symptom: When the installer cache is disabled (using the CACHEINSTALL=0 parameter to msixexec.exe), part of the installer is still cached in the folder C:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\<version>\Data\Cached Installs.

Solution: Changed a condition on a custom action during the install to skip the step that links files in the install cache folder.

Replicated AV/AS policies revert to the previous settings

Fix ID: 2971564

Symptom: With replication enabled, Virus and Spyware Protection policy changes revert back to the previous settings after a short period of time.

Solution: Updated the policy verification procedure during replication to ensure all changes are saved properly.

Symantec Endpoint Protection Manager deployment status incorrectly displays that an uninstallation is successful

Fix ID: 2982705

Symptom: Symantec Endpoint Protection Manager deployment status displays that an uninstallation is successful even after Symantec Endpoint Protection client uninstallation rolls back.

Solution: Added the logic to correctly obtain the path to the symlink.xml policy file in a rollback scenario.

Symantec Endpoint Protection Internet Email Auto-Protect blocks email notifications generated by other applications

Fix ID: 2885909/3133482

Symptom: Email notifications generated by applications such as Norton Ghost and SkySeaClient fail to send after you enable Internet Email (POP3/SMTP) Auto-Protect.

Solution: Implemented changes to prevent timeouts, remove lock requirements and retry sending attempts to successfully allow these messages through.

Symantec Endpoint Protection's Sysplant/Sysfer prevents Microsoft Visual Studio 2010 Premium's performance profiling tool from running

Fix ID: 2807560

Symptom: Microsoft Visual Studio 2010 Premium's performance profiling tool fails to start with Sysplant enabled. When you disable Sysplant, this tool works as expected.

Solution: Added the ability within Application Control to exclude the child processes of a parent process. For this scenario, you add the parent process, dllhost.exe, to the exception list. However, since this exception applies for all child processes of dllhost.exe, you should evaluate the risk before implementation.

Repeated and random BugCheck 8E crashes on multiple computers

Fix ID: 2912189

Symptom: Random crashes occur on multiple machines. The BugCheck analysis indicates BugCheck 8E and that it is probably caused by sysplant.sys.

Solution: Changed the way Sysplant handles an invalid file pointer.

Auto-Protect generates an error when an ActiveX component tries to write to HTML resources

Fix ID: 2950336

Symptom: Some ASP programs use ActiveX, and when ActiveX tries to write to some HTML resources, Auto-Protect generates an error and prevents it.

Solution: Removed the race condition issue that disallowed an update to the DLL resource.

Symantec Endpoint Protection Manager does not correctly schedule the start time for the Comprehensive Risk Report

Fix ID: 2703519

Symptom: You receive the scheduled report for the Comprehensive Risk Report by email, but there seems to be a one-minute delay in the start time every day.

Solution: Now the schedule always runs based on the scheduled report time, rather than based on the time that the previous scheduled report ended.

Symantec Endpoint Protection Manager console shows IPS signature failures on clients where IPS is not installed

Fix ID: 2873641

Symptom: Symantec Endpoint Protection Manager is reporting signature failures or out-of-date IPS definitions on machines where IPS is no longer installed.

Solution: The IPS version or content revision will not be shown if the feature has been uninstalled from the client.

Migrating from Symantec Endpoint Protection 11.0 to SEP 12.1 on a 32 bit computer does not remove all older Symantec drivers

Fix ID: 2946066

Symptom: After upgrading a Symantec Endpoint Protection 11.0.x client to SEP 12.1.1 (12.1 RU1) on a Windows 7 32-bit computer, an older SymTDL.sys driver remains on the computer. The driver is listed as "Stopped" in the Windows device manger. The issue does not occur on a Windows 7 64-bit computer.

Solution: Fixed a file handle issue during a migration scenario.

The Symantec Endpoint Protection Manager displays Port Scan detections and incorrect data for Windows 7 computers

Fix ID: 2949106

Symptom: False-positive Port Scan detections and incorrect identifying information display in the security log for Windows 7 computers.

Solution: To eliminate the false positives, the Port Scan detection now disregards any packets containing an IP address that does not belong to the client. These packets are sometimes created under certain conditions.

Attachments in Outlook 2010 take longer to open with Symantec Endpoint Protection installed

Fix ID: 3086057

Symptom: Attachments in Outlook 2010 are slower to open with Symantec Endpoint Protection 12.1 installed and the Outlook Auto-Protect feature enabled. Attachments in Outlook 2007 are not affected.

Solution: Optimized the Outlook Auto-Protect plug-in to avoid processing successive callbacks.

Database entries for Symantec Endpoint Protection 11.0.x content are not cleaned up when an 11.0.x client upgrades to version 12.1.x

Fix ID: 2932494

Symptom: After a Symantec Endpoint Protection 11.0.x client upgrades to version 12.1.x, the report of LiveUpdate content is not accurate.

Solution: The database maintenance task now correctly removes references to legacy monikers for upgraded clients.

All Resolved Issues

Firewall set to Block all until Symantec Endpoint Protection starts prevents GPO execution

Fix ID: 2880401

Symptom: You have configured the firewall to "Block all traffic until the firewall starts and after the firewall stops." However, the firewall blocks DHCP and GPO traffic, even though you have enabled the "Allow initial DHCP and NETBIOS traffic" setting.

Solution: The firewall now allows initial DHCP and NetBIOS traffic until the SMC service starts.

Symantec Endpoint Protection clients connect and disconnect with Symantec Endpoint Protection Manager intermittently

Fix ID: 3057712

Symptom: Proxy order of usage does not process as expected.

Solution: Changes to the proxy list mean that the proxy is no longer locked until the service is restarted. The proxy is unlocked when a server changes or goes offline.

Symantec Endpoint Protection does not automatically create Microsoft Exchange exclusions after moving the Queue folder

Fix ID: 3113496

Symptom: Symantec Endpoint Protection does not automatically create Microsoft Exchange exclusions after moving the Queue folder from one drive to another drive. This was previously expected behavior; Symantec Endpoint Protection did not create automatic exclusions in these circumstances.

Solution: Added an extra check to scan for the EdgeTransport.exe.config file, in order to get the Queue directory location and exclude it.

ccSvcHst causes CPU spikes on a Microsoft Exchange server

Fix ID: 3128260

Symptom: The ccSvcHst process causes CPU spikes on a Microsoft Exchange server after installation of the Symantec Endpoint Protection client.

Solution: Updated and expanded the algorithm used to generate automatic exclusions during the installation of Symantec Endpoint Protection.

Symantec Endpoint Protection Manager site becomes unresponsive on an intermittent basis

Fix ID: 3131253

Symptom: Symantec Endpoint Protection Manager site becomes unresponsive to console logins on an intermittent basis. This issue can affect access to the entire computer and may require a restart.

Solution: To prevent the lock of database tables, the Symantec Endpoint Protection Manager now only writes an event about successful client registration to the database after the transaction commit of the registration.

Client repeatedly requests content from the Group Update Provider or Symantec Endpoint Protection Manager

Fix ID: 3160786

Symptom: A client attempts to download a delta from Group Update Provider or Symantec Endpoint Protection Manager. The update fails and the client requests a full.zip file. This request also fails, and the client continues to request a full.zip in a "loop." Rebooting the computer or restarting the SMC service resolves the issue.

Solution: Modified SMC to add proper error handling when reading and writing files from the network.

Windows Action Center incorrectly reports that Symantec Endpoint Protection virus protection is off

Fix ID: 2646137

Symptom: Windows Action Center incorrectly reports Symantec Endpoint Protection virus protection is off. Microsoft Network Access Protection may quarantine client computers as a result.

Solution: When Windows Action Center cannot retrieve Auto-Protect's status, it reports that virus protection is off. A forced update from Symantec Endpoint Protection to Windows Action Center now occurs when the Auto-Protect status goes from Disabled to Enabled, or from 'not able to get status' to Enabled.

Symantec Endpoint Protection Manager performance is slower after upgrade to 12.1.1 (12.1 RU1 MP1) or later

Fix ID: 2882607

Symptom: After upgrade to Symantec Endpoint Protection Manager 12.1 RU1 MP1, performance of the Symantec Endpoint Protection Manager server is degraded. Delaying the security mining task (scm.timer.securitymining.delay) resolves the issue.

Solution: The data-mining task is no longer triggered immediately after restarting the Symantec Endpoint Protection Manager server. The Symantec Endpoint Protection Manager administrator can restore the original behavior by adding scm.datamining.runwhenrestarted=1 in the conf.properties file, which is located in the Symantec Endpoint Protection Manager installation directory under \tomcat\etc. Note: The data-mining task will always run after the first successful replication when an additional replication partner is added.

User can stop an administrator-defined scan by pressing the ENTER key

Fix ID: 2886274

Symptom: When an administrator-defined scan displays the scan dialog during scans, the user can stop the scan by clicking on the scan dialog and then pressing the Enter key, even though policy disallows the user to pause, snooze or stop a scan.

Solution: Updated the scan window to ignore the Windows close message if the administrator-defined scan locks the pause, snooze or stop scan options.

Linux clients are not included in the computer status details

Fix ID: 2900287

Symptom: Computer status logs are missing data about Symantec AntiVirus for Linux (SAVFL) clients. The exported logs do not contain Linux or Symantec AntiVirus (SAV) 10.x client information.

Solution: Modified the computer status query to include entries for Linux and Symantec AntiVirus 10.x clients.

Unexpected error in Symantec Endpoint Protection Manager: "Session already invalidated"

Fix ID: 2915051

Symptom: The scm-server log shows exception messages such as:

```
java.lang.IllegalStateException:  
getAttribute: Session already invalidated.
```

You may also receive notifications by email if you have configured such notifications.

Solution: Introduced a check to verify whether the session is invalidated. If it is invalidated, then the Symantec Endpoint Protection Manager sends the session timeout response directly.

IPS Definitions, Download Protection Definitions, and SONAR Definitions are incorrectly sortable in the Protection Technology view of the Symantec Endpoint Protection Manager

Fix ID: 2931188

Symptom: The sort function incorrectly works for the three columns IPS Definitions, Download Protection Definitions, and SONAR Definitions. The sort results are inaccurate.

Solution: Disabled the sort function for these three columns.

Reports for total scanned files for a resumed scan do not display correctly in the Client Logs screen

Fix ID: 2934430

Symptom: Reports for total scanned files for a resumed scan do not display correctly in the Client Logs screen in the Symantec Endpoint Protection client user interface. Raw data logs show different numbers that appear to be more updated.

Solution: Added extra steps to the Multi-Threaded Log Reader to ensure the logs are read in the correct order.

Startup scan doesn't run for a new user created after running sysprep.exe

Fix ID: 2947211

Symptom: If you create a new user after running sysprep.exe, the startup scan does not run for that user.

Solution: Sysprep clones all the keys under HKEY_CURRENT_USER for the current user to the new user. As a solution, before you run sysprep and the ClientSideClonePrepTool, delete the following registry key so that it does not get cloned: HKEY_CURRENT_USER\Software\Symantec\Symantec Endpoint Protection\SMC\RunOnceSessionPlugin

Windows Firewall is not fully functional after the Symantec Endpoint Protection firewall is disabled or the policy is withdrawn

Fix ID: 2949824

Symptom: Even after you disable the Symantec Endpoint Protection firewall, or withdraw the firewall policy, the Windows Firewall is not fully functional.

Solution: Changed the default so that when you disable or withdraw the policy for the Symantec Endpoint Protection firewall, Symantec Endpoint Protection does not take over Windows Firewall.

If Symantec Endpoint Protection is enabled, NetBackup RealTime disconnects when a remote desktop user logs off

Fix ID: 2970053

Symptom: With Symantec Endpoint Protection enabled, the NetBackup RealTime DRL LUNs disconnect when a remote desktop user logs off.

Solution: Changed the method used to detect drive types when the user logs into the computer.

Configuring the installation path using the Windows variable %systemroot% prevents Symantec Endpoint Protection 12.1 client installation

Fix ID: 2972965

Symptom: Client installation fails if your installation settings include the variable %systemroot% in the path for installation logging. Paths that use environment variables, such as %systemroot%\SEP_INST.LOG, cannot be parsed by setup.exe.

Solution: Changed the way Setup.exe processes the variables to allow for expansion during installation.

Invalid timestamp values cause the inability to export logs

Fix ID: 3038292

Symptom: Invalid values for timestamps prevent the export of computer status logs. Invalid values include negative numbers, like -11644473600000.

Solution: Changed the way invalid data values are handled.

Inconsistent information for virus and risk activity between reports

Fix ID: 3043727

Symptom: The information that displays in the Virus and Risks Activity Summary on the Symantec Endpoint Protection Manager Home page differs from the information generated through the Monitors and Reports tab.

Solution: Updated the database queries for consistency between reports.

Virus definitions don't update

Fix ID: 3075004

Symptom: The virus definitions do not update, but this issue is not apparently tied to a specific update. A restart sometimes resolves this issue.

Solution: Changed a pre-cleanup process to prevent potential deadlocks.

Database connection log contains database connection warnings

Fix ID: 3075314

Symptom: The db-connection.log contains the warning:

```
WARNING: ClientTransportInfoTask: (db conn) Return Connection Error->  
can't find connection (hashcode=X) in the map, total count=0
```

Solution: Fixed an issue in the database connection logic to resolve this warning.

BugCheck 8E (KERNEL_MODE_EXCEPTION_NOT_HANDLED) references SRTSP.sys

Fix ID: 3080628

Symptom: The Symantec Endpoint Protection client experiences a blue screen with BugCheck 8E (KERNEL_MODE_EXCEPTION_NOT_HANDLED). The blue screen references faulting driver SRTSP.sys.

Solution: Modified the File System Auto-Protect driver to prevent a BugCheck when a process is terminating on Windows Server 2003.

The SMC service crashes when using Avenail VPN to connect to the network and Symantec Network Access Control

Fix ID: 3084019

Symptom: The SMC service crashes when using Avenail VPN to connect to the network if Peer-to-Peer (P2P) Authentication is enabled in the firewall rules for Symantec Network Access Control.

Solution: Changed the method of accessing TCP information.

BugCheck 1 (APC_INDEX_MISMATCH) references fltmgr.sys

Fix ID: 3084393

Symptom: The Symantec Endpoint Protection client experiences a blue screen with BugCheck 1 (KERNEL_MODE_EXCEPTION_NOT_HANDLED). The blue screen references faulting driver fltmgr.sys (fltmgr!FltpProcessGenericWorkItem+0).

Solution: Resolved a variable initialization issue in the SymEFA.sys driver to prevent this BugCheck

Excessive duplicate Group Update Provider (GUP) entries in LiveUpdate policy

Fix ID: 3088546

Symptom: There are too many duplicate Group Update Providers (GUPs) in the LiveUpdate policy.

Solution: Changes to prevent duplication, particularly when two administrators edit the same GUP list at the same time from two different consoles. This action creates a condition that can double the number of existing GUPs in the policy.

Mapped network drive exceptions for A:, B:, and C: are not honored

Fix ID: 3094293

Symptom: Mapped network drive exceptions for A:, B:, and C: are not honored when you uncheck the option "Only when files are executed" for Auto-Protect.

Solution: Modified the Auto-Protect feature to properly check for network mappings on drive letters A: through C:.

BugCheck 8E (KERNEL_MODE_EXCEPTION_NOT_HANDLED) references SRTSP.sys

Fix ID: 3131618

Symptom: The Symantec Endpoint Protection client experiences a blue screen with BugCheck 8E (KERNEL_MODE_EXCEPTION_NOT_HANDLED). The blue screen references faulting driver SRTSP.sys.

Solution: Resolved a filename normalization issue in the File System Auto-Protect driver (SRTSP.sys).

Symantec Endpoint Protection Manager service fails to start

Fix ID: 3165435

Symptom: The Symantec Endpoint Protection Manager service fails to start with no warning or notification. The service may start successfully after multiple attempts.

Solution: Modified the Symantec Endpoint Protection Manager to detect a deadlock condition and retry until startup is successful.

Policies are not sorted properly in the Symantec Endpoint Protection Manager console

Fix ID: 2764681

Symptom: The Symantec Endpoint Protection Manager console displays a sort arrow in the header, but the columns cannot be sorted.

Solution: Resolved an issue when switching between pages in the Symantec Endpoint Protection Manager console. Columns are sorted correctly after switching between pages.

Monitors and logs do not show the same information as reports

Fix ID: 2836444

Symptom: When comparing the output from emailed risk reports to logs from Monitors, Logs, and Risk Log, the number of computers and detections do not match.

Solution: Updated reporting queries to provide consistency between various reports, logs, and notifications.

Symantec Endpoint Protection 12.1.x installation fails if Safend Data Protection Agent is installed

Fix ID: 2841607

Symptom: Installation of Symantec Endpoint Protection 12.1.x fails if Safend Data Protection Agent is installed. The SIS_INST.log file contains the following message:

```
[StartService] StartService() failed for service 'BHDrv86' with error 0x00000003.
```

Solution: Resolved an error condition with the installation of SONAR definitions.

For Compliance reports, saved filters from Quick Reports are not available for use in Scheduled Reports

Fix ID: 2844603

Symptom: A filter you created for Compliance reports under Quick Reports does not display under “Use a saved filter when adding a Scheduled Report.”

Solution: Changed so that saved filters created in Quick Reports display under Scheduled Reports. This matches the behavior of other types of reports.

Limited Administrators cannot maximize a read-only firewall policy window or increase the column size under Firewall Rules

Fix ID: 2920877

Symptom: Limited administrators cannot maximize a read-only firewall policy window or increase the column size under Firewall Rules.

Solution: Changed code to allow limited administrators to make these interface adjustments.

Incorrect estimation of the minimum package size when exporting a client installation package

Fix ID: 2947564

Symptom: In the Export Client Package dialog, the estimated minimum package size displayed is less than or greater than the size of the actual setup.exe created.

Solution: Changed the way Symantec Endpoint Protection Manager estimates the size of the client installation package.

External logging filename extension is changed from .tmp to .log

Fix ID: 2962101

Symptom: The file extension .tmp changes to .log when you visit the External Logging user interface, even if you do not make a change.

Solution: Changed the Symantec Endpoint Protection Manager console to maintain the external logging filename extension.

NetBackup jobs are slower when Application and Device Control is enabled

Fix ID: 2845896

Symptom: With Application and Device Control (ADC) enabled, NetBackup jobs take anywhere from two to six times longer.

Solution: Added device map information for Windows Server 2008 R2 and Windows 8 to improve performance.

Limited administrator cannot view the enforcer client log

Fix ID: 2677526

Symptom: Limited administrators and administrators cannot view the enforcer client log in the Symantec Endpoint Protection Manager monitors. The system administrator can view the enforcer client log normally.

Solution: Removed a restriction on limited administrators that previously required the domain ID to match. This restriction is not applicable to enforcer.

Tamper Protection exceptions defined with the variable [PROGRAM_FILES] fail on 64-bit systems

Fix ID: 2739395

Symptom: Tamper Protection exceptions defined with the variable [PROGRAM_FILES] fail to work on 64-bit systems.

Solution: Changed code to exclude files correctly for Tamper Protection in both C:\Program Files (x86) and C:\Program Files.

Symantec Endpoint Protection alerts on WS.reputation.1 and Bloodhound.Sonar.9, but the Symantec Endpoint Protection Manager log only displays the application name

Fix ID: 2748848

Symptom: Symantec Endpoint Protection alerts on WS.reputation.1 and Bloodhound.Sonar.9, but the Symantec Endpoint Protection Manager log only displays the application name for the same detection.

Solution: Changed the report to show the risk name instead of application name.

TECH166238 "How to block a user's ability to disable Symantec Endpoint Protection" is not working correctly

Fix ID: 2775346

Symptom: The user can disable Symantec Endpoint Protection even after following the steps in document TECH166238. The location shown in the Symantec Endpoint Protection user interface, under **Help > Troubleshooting...** does not match the applied policy.

Solution: Resolved a race condition between the auto-location thread and the profile management system.

Unmanaged detectors exceptions not honored, 'phantom detector' not showing in Symantec Endpoint Protection Manager

Fix ID: 2788825

Symptom: Unmanaged detector reports are sent, even if all unmanaged detectors have been demoted. Querying the database confirms there are no clients flagged as unmanaged detectors in the Symantec Endpoint Protection Manager.

Solution: During an OU sync, if a client is removed, the corresponding entries in the LAN_DEVICE_EXCLUDED and LAN_DEVICE_DETECTED tables are removed. When a client registers and has a hash update in the SEM_CLIENT table, the corresponding entries in the LAN_DEVICE_DETECTED table are removed and entries in the LAN_DEVICE_EXCLUDED table are updated.

"AllowSkipEvent" setting is missing in Symantec Endpoint Protection 12.1

Fix ID: 2789185

Symptom: The "AllowSkipEvent" registry value for scheduled scans is not honored in Symantec Endpoint Protection 12.1.

Solution: Added the ability to use the "AllowSkipEvent" registry value. The AllowSkipEvent registry value is the number of times a scan is allowed to be skipped prior to automatically running the scan. The default is 1 if the value is not set or missing.

The property "scm.email.content.type" does not work for "New risk detected" notifications

Fix ID: 2833855

Symptom: "New risk detected" notification emails arrive in HTML format, even after you change the property "scm.email.content.type" to value "text/plain" as described in Symantec support document TECH189497.

Solution: Updated email notifications to honor the scm.email.content.type property for new risk detections.

Symantec Endpoint Protection Manager "Risk Detections Count" report does not work correctly with a group filter

Fix ID: 2837145

Symptom: When you use a group filter with a "Risk Detection Count" report, no records appear.

Solution: Forced the browser to generate a new pie chart when you apply a filter.

Accessing client groups in the Symantec Endpoint Protection Manager console are slower when logged in as a limited admin or standard admin

Fix ID: 2839215

Symptom: When you log into the Symantec Endpoint Protection Manager console as a limited administrator or a standard administrator, access to client groups is slower. There is no delay if you log in as a system administrator.

Solution: Optimized the Symantec Endpoint Protection Manager console to remove unnecessary or duplicate queries.

Inconsistent information reported for Action on the client risk log

Fix ID: 2844472

Symptom: The Symantec Endpoint Protection client risk log indicates "Restart Required - Cleaned," but Symantec Endpoint Protection Manager risk log for the same event only shows "Cleaned."

Solution: Added "Restart Required - Cleaned" to the filter Action dropdown list for the Symantec Endpoint Protection Manager.

Application ccSvcHst.exe crashes after the installation of Symantec Endpoint Protection 12.1.1.1 (RU1 MP1)

Fix ID: 2860679

Symptom: Application ccSvcHst.exe crashes after the installation of Symantec Endpoint Protection 12.1.1.1 (12.1 RU1 MP1) on Windows XP Service Pack 3. The application error involves msvcr90.dll.

Solution: Resolved an issue in the HTTP communication engine.

Notification email is not sent when "[Client Security Alert] - [Compliance]" is logged in the Symantec Endpoint Protection Manager console

Fix ID: 2866954

Symptom: When the Symantec Network Access Control Host Integrity check fails, an event is transferred the Symantec Endpoint Protection Manager and logged in the Notifications View. The administrator does not receive an email. Other notifications are working properly.

Solution: Updated the notification queries to ensure that they include host compliance events.

System Lockdown UI string "Applications not in the unapproved list are approved for execution" is confusing

Fix ID: 2874467

Symptom: The System Lockdown UI contains extraneous text "Applications in the approved application list are approved for execution" and "Applications not in the unapproved application list are approved for action."

Solution: Removed the extraneous text. These strings should only appear if blacklist mode is enabled, as described in Symantec support document HOWTO81099.

Client Deployment Wizard reports as successful even though it failed

Fix ID: 2878971

Symptom: Client Deployment Wizard reports as successful even though it failed; a closer look shows that Symantec Endpoint Protection manager purged the ..\inetpub\ClientPackages\pkgtemp folder while the Client Deployment Wizard was still open. This purge causes the Client Deployment Wizard to deploy an incomplete installation package.

Solution: A cleanup task now skips the pkgtemp folder and sweeps it the next time Client Deployment Wizard generates temporary files.

BugCheck D1 (DRIVER_IRQL_NOT_LESS_OR_EQUAL) references symnets.sys

Fix ID: 2914058

Symptom: The Symantec Endpoint Protection client experiences a blue screen with BugCheck D1 (DRIVER_IRQL_NOT_LESS_OR_EQUAL). The blue screen references faulting driver symnets.sys.

Solution: The driver now detects for improperly-formed DNS response structures.

Symantec Endpoint Protection Manager does not send single risk notifications for Forced Application detections logged by legacy TruScan engine

Fix ID: 2928236

Symptom: The Symantec Endpoint Protection Manager is configured to send single risk notifications. With Symantec Endpoint Protection Manager 12.1 managing Symantec Endpoint Protection 11.0 clients, forced application detections generated in the client's TruScan logs appear in the SONAR logs (as "Forced SONAR") and they do not generate single risk notifications. Notifications for other types of events are functioning as expected.

Solution: Updated the Symantec Endpoint Protection Manager to send notifications for potential risks reported by TruScan.

Lotus Notes Auto-Protect causes voice mail (.wav) files to duplicate

Fix ID: 2930770

Symptom: With Symantec Endpoint Protection 12.1.x installed and the Lotus Notes Email Auto-Protect plug-in enabled, voice mail .wav files duplicate when you play then close them. The duplicate .wav file display as an additional attachment in the original email.

Solution: Modified the Lotus Notes Auto-Protect plug-in to avoid caching data unnecessarily.

Application and Device Control Client Control log fails to log registry values, only logs registry keys

Fix ID: 2943355

Symptom: Application and Device Control does not identify registry read or write activity to registry values in the Client Control log. This log identifies only read or write activity to registry keys.

Solution: Application and Device Control now also logs all read and write activity to registry values in the Client Control log.

A compliance-related client security alert logs but Symantec Endpoint Protection Manager for Symantec Network Access Control does not send a notification email

Fix ID: 2948717

Symptom: A Symantec Network Access Control-enabled Symantec Endpoint Protection Manager does not send a notification email as configured. Logs show a compliance security alert, which should have triggered an email.

Solution: Email notifications now generate based on two separate tables in the database.

A DLL related to the Lotus Notes plug-in still loads with Lotus Notes, even after you remove the Lotus Notes Email Scanner

Fix ID: 2957838

Symptom: The Lotus Notes plug-in file NLNVP.dll still loads with Lotus Notes, and a reference to it appears in the file notes.ini, even though you have removed the Lotus Notes Email Scanner.

Solution: Added code to correctly delete NLNVP.DLL from the Lotus Notes folder and to modify notes.ini to remove the plug-in's entry.

Enabled devices are logged with a severity of a "Major"

Fix ID: 2980693

Symptom: Allowed or enabled device event types are logged with a severity of "Major" when they should be "Information."

Solution: This event type now displays with the severity level "Information."

BugCheck 50 (PAGE_FAULT_IN_NONPAGED_AREA) references teefer.sys

Fix ID: 2990492

Symptom: The Symantec Endpoint Protection client experiences a blue screen with BugCheck 50 (PAGE_FAULT_IN_NONPAGED_AREA). The blue screen references faulting driver teefer.sys.

Solution: Modified the Teefer driver to prevent this blue screen

Active scan starting causes current window to lose focus

Fix ID: 3016261

Symptom: The currently active window loses focus when an active scan starts in the background.

Solution: Changed the behavior of the scan results window to show the scan results when it detects a risk, rather than creating a hidden Windows dialog window at the beginning of the scan.

BugCheck 7E (SYSTEM_THREAD_EXCEPTION_NOT_HANDLED) references teefer.sys.

Fix ID: 3034930

Symptom: The Symantec Endpoint Protection client experiences a blue screen with BugCheck 7E (SYSTEM_THREAD_EXCEPTION_NOT_HANDLED). The blue screen references faulting driver teefer.sys.

Solution: Fixed an issue in the Teefer driver to avoid a scenario where memory is freed immediately after it is allocated.

"The request is not supported" appears when browsing for a computer on the Browse Network tab

Fix ID: 3088227

Symptom: In the Japanese version of Symantec Endpoint Protection, the error message "The request is not supported" appears in the Client Deployment Wizard when you browse the network using Remote Push. The environment also uses Symantec Network Access Control.

Solution: Remote Push now skips the Symantec Network Access Control network provider when browsing for clients, since it is a virtual network.

Limited Administrators lack scrollbars and viewing capabilities in Java-based remote console

Fix ID: 2866747

Symptom: When limited administrators log in to the Symantec Endpoint Protection Manager using the Java-based remote console, the scrollbars are grayed out and viewing capabilities are limited. This behavior does not occur when they use the web-based console.

Solution: Updated the user interface filters to display these objects correctly.

Scheduled scan runs repeatedly in a multi-user environment

Fix ID: 2918859

Symptom: Multiple users on an unmanaged Symantec Endpoint Protection client appear to have scans scheduled to run at or near the same time. As soon as one finishes, the next one starts.

Solution: The unmanaged Symantec Endpoint Protection client no longer creates a default user scan for each user account.

Outlook Express cannot send or receive email after an upgrade to Symantec Endpoint Protection 12.1.x with Internet Email Auto-Protect enabled.

Fix ID: 3058731

Symptom: When you upgrade to Symantec Endpoint Protection and then enable Internet Email Auto-Protect, Outlook Express cannot connect to the mail server. This occurs if the network interface card NIC has several IP addresses which are not in the same subnet.

Solution: Internet Email Auto-Protect now checks against the routing table to make sure it matches the route selected.

Scan Log shows some scan events with same "Started On" and "Completed" date

Fix ID: 2829569

Symptom: A scan starts on one day and finishes the next day. The scan events appear in different log files because the log files roll over at midnight. The "Scan Log" will display this scan event with the same "Started On" and "Complete" dates. This issue occurs in a multi-processor environment.

Solution: Resolved a thread synchronization error which caused the client to read empty data from the log file.

Symantec Endpoint Protection client cannot apply policy settings from manager

Fix ID: 2995158

Symptom: Symantec Endpoint Protection client machines do not update with the latest policy version from the Symantec Endpoint Protection Manager. The clients shown as connected to the Symantec Endpoint Protection Manager and update other content. The Symantec Endpoint Protection client debug.log shows the following errors when attempting to apply the new policy downloaded from the manager:

```
=====EXCEPTION: SndException ==== Reason Code: 0, Reason:invalid rawip  
protocol number, it should be 0-255
```

```
=====EXCEPTION: SndException ==== Reason Code: 0, Reason:failed to import
from DM

=====EXCEPTION: SndException ==== Reason Code: 0, Reason:failed to import
ServiceGroup from DM

=====EXCEPTION: SndException ==== Reason Code: 0, Reason:fail to import
ServiceGroupZone from DM

=====EXCEPTION: SndException ==== Reason Code: 0, Reason:fail to import
global group from profile

import trident config for server profile failed
```

Solution: Resolved an issue with the IP/Ethernet protocol validation in the firewall policy that prevented the client from applying the policy.

Scheduled reporting runs based on the incorrect time zone

Fix ID: 2933213

Symptom: After a switch to Daylight Savings Time, scheduled reporting runs according to the GMT time zone when the system time zone is set to GMT+10 (Canberra, Melbourne, Sydney).

Solution: Corrected the logic for checking the Daylight Savings Time status for the southern hemisphere.

Risk log is not generated by Auto-Protect when the "Display the Auto-Protect results dialog" check box is unchecked

Fix ID: 3123316

Symptom: Auto-Protect properly detects threats but does not log them if you have disabled "Display the Auto-Protect results dialog on the infected computer" for Auto-Protect notifications in the Virus and Spyware Protection policy.

Solution: Modified the Auto-Protect feature to properly log threats in this scenario.

CCRBridge.exe application terminates unexpectedly

Fix ID: 3006641

Symptom: The CCRBridge.exe application terminates unexpectedly when the Application and Device Control driver (sysplant.sys) is installed.

Solution: Modified the Application and Device Control driver (sysplant.sys) import table address to dynamically allocate memory.

Symantec Endpoint Protection Manager does not log failed login attempts from administrators that do not exist

Fix ID: 2775699

Symptom: When a user that does not exist attempts to log into the Symantec Endpoint Protection Manager console, Symantec Endpoint Protection Manager does not log the failed login attempt.

Solution: Symantec Endpoint Protection Manager now logs all failed login attempts, even if the administrator does not exist.

Default logging doesn't provide enough information for SECARS troubleshooting

Fix ID: 2831728

Symptom: A lack of specific error codes related to SECARS with the logging level set to default hampers initial troubleshooting efforts. These error codes only appear when you enable more verbose logging.

Solution: Changed to increase visibility for important SECARS issues at the default logging level. The logs display this related information without changing the log level.

Download randomization does not work with location specific settings

Fix ID: 2988742

Symptom: The download randomization setting does not work correctly when you enable location-specific communication settings.

Solution: Updated the location-specific policy to include the download randomization setting.

The "Domain/Workgroup" field no longer appears in Symantec Endpoint Protection 12.1

Fix ID: 2961966

Symptom: The "Domain/Workgroup" field no longer appears under **Clients > View > Default View**.

Solution: Added the "Domain/Workgroup" field back under **Clients > View > Network Information**.

Resolved Issues from Previous Version

The following issues are integrated from Symantec Endpoint Protection version 11.0 Release Update 7 Maintenance Patch 3.

The time stamp changes on restored quarantined files

Fix ID: 2661232

Symptom: The original time stamp on a file changes after being restored from the quarantine.

Solution: Fixed an issue where file restoration from the quarantine modifies the time stamp and the attribute of the file.

Mismatch between reported clients in the Unmanaged Detector report

Fix ID: 2663136

Symptom: The total number of clients on an Unmanaged Detector report does not match the actual number of devices listed.

Solution: The Unmanaged Detector report now includes the total number of detected unknown devices and the unique number of unknown devices.

Notification not logged in notification view

Fix ID: 2712563

Symptom: "Single Risk Event" notification is not logged in the notification view in Symantec Endpoint Protection Manager when the event was triggered.

Solution: When a single risk event occurs, Symantec Endpoint Protection Manager now writes it to the database, where you can view it by clicking **Notifications > View notifications**.

Clients do not update definitions downloaded from Symantec Endpoint Protection Manager

Fix ID: 2715989

Symptom: After the clients come out of standby, the definitions do not update until after Symantec Endpoint Protection Manager restarts.

Solution: Fixed so that LiveUpdate restarts after the client computer recovers from standby.

Server logs show that the Virus and Spyware Protection policy was corrupt after migration from SAV 10.x

Fix ID: 2699388

Symptom: The log file states that the Antivirus and Spyware policy is corrupt when it is not.

Solution: Fixed the issue caused by some Virus and Spyware Protection policies that did not have the necessary Auto-Protect actions, which generated a log entry in Symantec Endpoint Protection Manager.

RADIUS settings not saved for the Enforcer

Fix ID: 2791090

Symptom: The management server does not save the Enforcer RADIUS settings.

Solution: Fixed by removing a broken or unused management server list. When you edit the Enforcer properties, the broken or unused management server list is now skipped.

Symantec Endpoint Protection Manager Scan log status is not updated

Fix ID: 2778391

Symptom: The Scan Log status doesn't update when you suspend and then complete an administrator-defined scheduled scan.

Solution: Fixed by adding the suspended event into a list of known events that the management server processes.

Some system files are not visible in the unmanaged client user interface

Fix ID: 2740080

Symptom: Unable to exclude VMMS.EXE and VMWP.EXE in W2K8R2 in an unmanaged SEP 11.0 RU7 MP1 client.

Solution: Fixed the issue by calling an API that allows the viewing of all system files.

.err files are not cleaned up

Fix ID: 2767546

Symptom: The Symantec Endpoint Protection Manager produces files with the .err extension but does not clean them up. This causes the Symantec Endpoint Protection Manager to miss the parsing of events.

Solution: Fixed the code to bypass the error. Symantec Endpoint Protection Manager continues to process the log and record the error line.

Unmanaged client appears in the Symantec Endpoint Protection Manager console

Fix ID: 2800124

Symptom: When you create and deploy a client installation package using the default group policy settings but turn off the Use Group Communication Settings setting, the installation results in an unmanaged client.

Solution: Fixed an issue to remove the location-level communication settings in the exported package.

Replication failed

Fix ID: 2810324

Symptom: The replication fails continuously. The data.zip file is generated and transferred, but replication is not successful.

Solution: Fixed this issue by cloning the default management server list in the Enforcer's policy.

Lotus Notes scan records are left on the client computer

Fix ID: 2834021

Symptom: The default behavior is for scan records for Lotus Notes to remain on the client computer. You had to change the default value on each computer manually to remove these records.

Solution: The default setting in the registry for Lotus Notes Auto-Protect is now "NotLeaveScanRecords=1."

Performance impact with Limited Admin rights

Fix ID: 2885818

Symptom: The Home page and the client groups take a long time to load in the Symantec Endpoint Protection Manager Java remote console when you are logged on with a limited administrator account.

Solution: Improved the limited administrator performance issues and reduced the number of times the administrator context is reloaded.

Folder exclusions for scans does not work

Fix ID: 2705877

Symptom: Exclusions for a folder in the format of \foldername works for Auto-Protect but fails for manual and scheduled scans.

Solution: Fixed by expanding the folder exclusions for all possible drives. Folder exclusions now work for manual scans.

The management server does not remove the database backup files

Fix ID: 2703417

Symptom: The "Remove the database backup files during uninstall" feature doesn't work if you have moved the server data folder.

Solution: Fixed by deleting the current data area in conf.properties when the data and backup folders are deleted.

Symantec AntiVirus for Linux logs are not replicated

Fix ID: 2804484, 2915591

Symptom: Symantec AntiVirus for Linux logs are not replicated to remote sites.

Solution: Fixed an issue during replication, which deleted legacy clients from some tables.

Component Versions

SEP/SEPM	12.1.3001.165
AutoProtect	14.4.0.6

AutoProtect Driver	14.4.0.5
AV Engine	20121.3.0.76
AV Engine Driver	20121.3.0.76
BASH Defs	7.6.1.4
BASH Defs Driver	7.6.1.4
BASH Framework	7.0.0.226
CIDS Defs	11.3.0.9
CIDS Defs Driver	11.1.1.5
CIDS Framework	11.1.0.73
Common Client	12.3.2.6
Common Client Driver	12.3.2.3
ConMan	1.0.2.4
DecABI	2.3.1.1
DefUtil	4.7.0.27
DuLuCallback	1.5.0.69
ECOM	121.3.0.78
ERASER	112.2.0.13
ERASER Driver	112.2.0.13
Iron	3.2.0.11
Iron Driver	3.2.0.11
LiveUpdate (server)	3.3.100.15
LiveUpdate (client)	2.2.1.7
MicroDefs	3.6.0.79
SymDS	2.2.0.19
SymDS Driver	2.2.0.19
SymEFA	4.2.0.53
SymEFA Driver	4.2.0.53
SymELAM	1.0.0.111
SymELAM Driver	1.0.0.111
SymEvent	12.9.3.2
SymEvent Driver	12.9.3.1
SymNetDrv	13.1.1.8
SymNetDrv Driver	13.1.1.7
SymVT	5.2.0.5