Fix Notes for Symantec Endpoint Protection 12.1 Release Update 1, Maintenance Patch 1 (RU1-MP1)

Component Versions

AutoProtect	12.3.4.3
AutoProtect Driver	12.3.4.2
AV Engine	20111.2.0.82
AV Engine Driver	20111.2.0.82
BASH Defs	6.6.2.6
BASH Defs Driver	6.6.2.6
BASH Framework	6.2.100.27
CIDS Defs	10.1.1.8
CIDS Defs Driver	10.1.1.8
CIDS Framework	9.8.3.6
Common Client	10.2.1.2
DecABI	2.1.2.12
DefUtil	4.4.2.5
DuLuCallback	1.3.1.10
ECOM	111.2.0.72
ERASER	111.2.2.9
ERASER Driver	111.2.2.9
Iron	1.7.0.9
Iron Driver	1.7.0.8
LiveUpdate (server)	3.3.2.2
LiveUpdate Express (client)	2.0.3.6
MicroDefs	3.2.0.24
SymDS	1.2.1.6
SymDS Driver	1.2.1.5
SymEFA	2.2.2.4
SymEFA Driver	2.2.2.4
SymEvent	12.9.2.21
SymEvent Driver	12.9.2.20
SymNetDrv	11.1.4.4
SymNetDrv Driver	11.1.4.3

Product Changes in this Release

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

Trusted internet domain exceptions do not support FTP

Fix ID: 2632015

Symptom: A trusted internet domain exception only supports HTTP. It does not support FTP.

Solution: Trusted internet domain exceptions now support both HTTP and FTP. The administrator may specify an IP address or a hostname. HTTPS is not supported.

LiveUpdate does not use user-defined proxy if a system-level proxy is configured

Fix ID: 2562148

Symptom: When both a user-defined proxy and a system-level proxy are configured, LiveUpdate will only use the system-level proxy.

Solution: The client was modified to use the user-defined proxy first, if specified, for LiveUpdate. If no user-defined proxy is specified, the client will use the system-level proxy. If neither proxy is found, the client will attempt a direct connection to LiveUpdate.

Cannot delete older client package from SEPM

Fix ID: 2575763

Symptom: Older client packages cannot be deleted from SEPM. This issue occurs when the older client package language is different from the newest package.

Solution: SEPM was modified to allow the administrator to delete the old package, even if it is the latest version for a particular language. SEPM will display a warning prompt in this case.

Top Impacting Issues Resolved in this Release

Application is slow to load or times out after SEP 12.1 is installed

Fix ID: 2493969

Symptom: Customer or third-party applications experience performance degradation when installed with SEP 12.1.

Solution: A configuration parameter in the SEP client (SymTDI.sys driver) was modified to improve network application performance.

Small Business Edition SEPM database transaction log does not truncate

Fix ID: 2660649

Symptom: The database transaction log on the SEPM Small Business Edition (SBE) server does not truncate. This may consume all of the available space on the server's hard drive.

Solution: The server was modified to prevent a build-up of the database transaction log.

Tamper Protection exceptions are not honored on 64-bit computers

Fix ID: 2580578

Symptom: Tamper Protection exceptions are not honored on 64-bit computers. An excluded process will trigger tamper protection.

Solution: The SEP client was sending a delta of the exclusion list to the BASH component on 64-bit computers. The client was modified to send the complete list to resolve this issue.

"Ending program… please wait" on ccSvcHst.exe during shutdown

Fix ID: 2607378

Symptom: Symantec Endpoint Protection client machines (workstations) are unable to shutdown gracefully. The message "Ending program... please wait" displays on ccSvcHst.exe but will not continue shutting down until "End Now" is selected.

Solution: The email session helper plugin (SavEmailSesHlp.dll) was modified to prevent a hang on shutdown.

Export of client package from SEPM never finishes

Fix ID: 2627397

Symptom: Export of a client package from SEPM does not complete on non-English Windows, when SEPM is configured to use the embedded database.

Solution: SEPM was modified to use a different database method to obtain binary stream data.

Cannot send scheduled email if the Outlook plugin is installed

Fix ID: 2552760

Symptom: Scheduled emails in Outlook 2010 remain in the Outbox when the Outlook Auto-Protect plugin is installed.

Solution: The Outlook Auto-Protect plugin was modified to prevent a condition where messages in the Outbox are blocked from sending.

Unable to create an application exception in SEPM

Fix ID: 2560976

Symptom: Unable to create an application exception in SEPM and the application exception window does not appear. The scm-server.log file may display the following exception:

> *SEVERE: Invalid query statement in:*
>
> *com.sygate.scm.server.consolemanager.requesthandler.GetObjectHandler*
>
> *java.sql.SQLException: Subquery returned more than 1 value. This is not permitted when the subquery follows =, !=, <, <= , >, >= or when the subquery is used as an expression.*

Solution: A SQL query was modified to allow the window to open properly.

Scheduled scan runs repeatedly in a multi-user environment

Fix ID: 2613428/2618423

Symptom: Multiple users have scans scheduled to run at or near the same time. As soon as one finishes, the next one starts.

Solution: This release introduces a new registry value which can be added by the administrator to disable all user scans:

> HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint
>
> Protection\AV\AdministratorOnly\General\EnableUserScans = 0

The administrator can add EnableUserScans as a DWORD. When the value is 0 all user scans are disabled. When the value does not exist or is non-zero, all user scans are enabled (default behavior). Administrator-defined scans are not affected by this registry value.

Windows Security Center (WSC) does not recognize that SEP is enabled after migration from SEP 11.0

Fix ID: 2649543/2507041

Symptom: After migrating from SEP 11.0 to 12.1, Windows Security Center reports "Turn on Symantec Endpoint Protection" when SEP is enabled.

Solution: The installer now passes the proper display name to Windows Security Center to allow the old product to unregister from WSC properly.

Symantec Endpoint Protection reports status to Windows Security Center in a format that is no longer supported

Fix ID: 2687476/2711787

Symptom: After installation of SEP 12.1 on Windows 7, Windows Security Center displays the following message:

> *Symantec Endpoint Protection is on but is reporting its status to Windows Security Center in a format which is no longer supported.*

Solution: The SEP client was modified to properly register with Windows Security Center.

Client online status is not reflected correctly after restoration of embedded database

Fix ID: 2620816/2612223/2659915/2710490

Symptom: After an embedded database is restored from backup, the client online status is not reflected properly in the SEPM console. The SEPM logs may also contain the messages:

> *1) Assertion failed: 200114*
>
> *2) Can't find values for row <ID> in index 'I_SEM_AGENT_COMPUTER_ID_PLUS'*
>
> *3) java.sql.SQLException: [Sybase][ODBC Driver][SQL Anywhere]Unable to find in index 'I_SEM_AGENT_COMPUTER_ID_PLUS' for table 'SEM_AGENT'*

Solution: The SEPM database restore function was updated to properly rebuild indices of databases that were created or migrated from SEP 11.0.

Citrix EdgeSight for Virtual Desktops application errors

Fix ID: 2608836/2637570/2647457

Symptom: Citrix EdgeSight for Virtual Desktops is installed with SEP and the Application and Device Control feature is enabled. Several applications may terminate unexpectedly after the computer is restarted:

“Rundll32.exe – Application error: The instruction at 0x75447740 Referenced Memory at 0x75447740. The memory could not be written.”

“Wermgr.exe – Application error: The instruction at 0x75447740 Referenced Memory at 0x75447740. The memory could not be written.”

“WerFault.exe – Application error: The instruction at 0x75447740 Referenced Memory at 0x75447740. The memory could not be written.”

“Userinit Logon Application has stopped working”

Solution: A method to get the volume name for a mount point was moved from the Application and Device Control DLL (sysfer.dll) into the driver (Sysplant.sys) to resolve this issue.

Web browsers terminate unexpectedly when Trusteer Rapport is installed with SEP

Fix ID: 2657350

Symptom: Trusteer Rapport is installed with SEP and the Application Device Control feature is enabled. Web browsers may terminate unexpectedly with the following errors:

Firefox (firefox.exe): 0x00003dbe

Internet Explorer (iexplore.exe): 0x0000a9f6

Google Chrome (chrome.exe) 0x000c6ce0

Solution: The application and device control driver (Sysplant.sys) was modified to prevent this crash.

Migration from SEP 11.0 to 12.1, or repairing a SEP 12.1 client, results in duplicate client entries if the client is a Hyper-V guest OS

Fix ID: 2477905

Symptom: Migrating a client from SEP 11.0 to 12.1 results in a duplicate client entry in the SEPM console if the client is a Hyper-V guest OS. This issue can also occur if a SEP 12.1 client is repaired via the add/remove control panel, if the client is a Hyper-V guest OS.

Solution: The SEP client installer was modified to prevent a condition where the hardware ID is re-generated, resulting in a duplicate client entry.

Multiple licenses installed do not increase the total license count

Fix ID: 2592244/2615674

Symptom: When multiple licenses are installed with the same license end date, the total seat count does not increase.

Solution: The license import logic was modified to resolve this issue.

Policy exported from SEP 11.0, then imported into SEP 12.1, cannot be edited or saved properly

Fix ID: 2601762/2559611

Symptom: An Antivirus policy, exported from SEP 11.0 and imported into SEP 12.1, cannot be edited or saved properly. Download Insight settings cannot be changed, locked, or saved.

Solution: The SEPM policy import logic was corrected to resolve this issue.

"The object cannot be found. 0x16010000" error is displayed when policy inheritance is disabled

Fix ID: 2650714/2693604

Symptom: The SEPM console displays the message "The object cannot be found. 0x16010000" when the option "Inherit policies and setting" is disabled. The DBValidator tool may also display the following messages:

> *Link is broken for [1] target ids:*
>
> *TargetId:[<GUID>] TargetType:[SemServerList]*
>
> *ObjectTypeName:[ObjReference] ParentObjectTypeName :[ExternalCommunication]*
>
> *Parent's TopLevelObject's GUID:[<GUID>]*

Solution: SEPM was modified to prevent a scenario where an object is not properly removed from a policy.

The SEPM "Clients" tab fails to open after migration from 12.1 to 12.1 RU1 on Polish OS/SEPM only

Fix ID: 2647498

Symptom: After upgrading from SEPM 12.1 to 12.1 RU1, the clients tab fails to open. The progress bar is displayed indefinitely. This issue only occurs with the Polish SEPM on a Polish operating system.

Solution: The SEPM console was modified to properly trim a localized string.

Deleted groups are displayed in the group selection for SEPM reports

Fix ID: 2585785

Symptom: Report filters in SEPM show groups that have been deleted.

Solution: SEPM was modified to restrict the group drop-down list to display existing groups only

All Resolved Issues

Virus definitions do not update after migration from SEP 11.0 to 12.1

Fix ID: 2694126/2602277

Symptom: After upgrading from SEP 11.0 to 12.1, SEPM and clients will not update 32-bit virus definitions. The definitions remain the same as before the migration. The scm-server.log may display the message:

> *SEVERE: java.sql.BatchUpdateException: Violation of PRIMARY KEY constraint 'PK_VIRUS'. Cannot insert duplicate key in object 'dbo.VIRUS'.*

Solution: SEPM was modified to resolve an issue where virus names are “escaped" differently between SEP 11.0 and 12.1. On migration, all VIRUSNAME history data is now reformatted to use proper escape sequences for SEP 12.1.

Notifications and alerts are sent to all SEPM administrators

Fix ID: 2675484

Symptom: Notifications and alerts will ignore the email address specified in the configuration. The email is sent to all SEPM administrators.

Solution: SEPM was modified to send each notification separately instead of batching them together.

"Query failed" during compliance report generation

Fix ID: 2072775

Symptom: The message "query failed" appears when generating any of the compliance reports: “Client by Compliance Failure Summary”, “Compliance Failure Details,” or “Non-compliant clients by Location.”

Solution: The SEM_COMPLIANCE_CRITERIA table was split into two tables to increase performance of these queries.

"Symantec Endpoint Protection detected Risks while you were logged out," but there is nothing in the risk log

Fix ID: 2529730

Symptom: A user configures a scheduled scan, and then logs off. The scan runs while the user is logged off. When the user logs in, the message "Symantec Endpoint Protection detected risks while you were logged out" is displayed. The risk log does not contain any new risks.

Solution: When a user-defined scan runs when a user is logged off, that scan runs with local system privileges. Risks may be detected that the user would not normally have access to view. SEP was modified to only show the alert message to users with administrator privileges.

SEPM migration from 11.0 to 12.1 fails with a SQL exception

Fix ID: 2681839

Symptom: SEPM upgrade from 11.0 to 12.1 fails with a SQL exception. The upgrade.log contains the message:

> *java.sql.SQLException: The CREATE UNIQUE INDEX statement terminated because a duplicate key was found for the object name 'dbo.INVENTORYREPORT' and the index name 'PK_INVENTORYREPORT'.*

Solution: SEPM was modified to use a case-insensitive comparison to find duplicate filter names for users/administrators.

.SLG files accumulate in the DB folder when using the embedded database

Fix ID: 2597184

Symptom: *.SLG files accumulate in the SEPM\DB folder when using the embedded database. The files are never deleted.

Solution: A Sybase DB parameter was modified to reduce the build-up of .SLG files.

Failover Gateway Enforcers switch to the active state instead of standby

Fix ID: 2596240

Symptom: Two Gateway Enforcers are in a failover configuration when using STP and OSPF. Both Enforcers enter active mode when started. The backup Enforcer may momentarily enter standby mode before switching to active mode.

Solution: Enforcer will now block multicast (OSPF) packets for a failover period to prevent packet storms. Enforcer will also block STP for 10 seconds to prevent a loop detection which could cause the failover Enforcer to enter the active state.

After migrating SEPM from 11.0 to 12.1, Enforcers are unable to register with the server

Fix ID: 2557651

Symptom: Enforcers are unable to register with the SEPM server after migrating SEPM from 11.0 to 12.1. The SEPM log may contain the following error:

> *SEVERE: in: com.sygate.scm.server.task.EnforcerCompilerTask*
>
> *java.lang.ClassCastException:*
>
> *com.sygate.scm.common.configobject.schema.SemServerList cannot be cast*

Solution: SEPM was modified to handle corrupted data when compiling the profiles for Enforcer groups.

javaw.exe CPU usage spikes when using the SEPM console

Fix ID: 2580216

Symptom: The CPU usage of javaw.exe increases when repeatedly loading the "Installed Package" tab.

Solution: The SEPM console was modified to reduce the CPU usage when the page is loaded multiple times.

SEPM report filters do not allow for partial matches with the * wildcard character

Fix ID: 2624748/2617514/2653095

Symptom: SEPM report filters do not allow for partial matches with the * wildcard character. The wildcard character * was valid in SEP 11.0.

Solution: SEPM now converts * to %, so either * or % can be used as wildcard characters in report filters.

Client does not communicate with the Shared Insight Cache Server if it has two locations

Fix ID: 2660926

Symptom: When two locations are defined, each with different scan options (one with shared insight cache, and one without), no submission to the shared insight cache server is performed.

Solution: The XML schema document for the cache server setting was updated to include the location path.

Client migration from 11.0 to 12.1 fails and rolls back

Fix ID: 2616385

Symptom: Migration from SEP 11.0 to SEP 12.1 fails and rolls back. This error occurs after multiple migrations, for example SEP 11.0 MR4-MP2 to SEP 11.0 RU6-MP2 to SEP 12.1. The MSI log contains the message "SymResolveFeatures. Return value 3."

Solution: The installer was modified to prevent a condition where an exception was generated when determining the older product version.

User-scheduled scan or user-initiated scan does not start

Fix ID: 2637651/2602021

Symptom: A scan scheduled by the user, or a user-initiated scan (right-click and Scan for Viruses) does not start. The scheduled scan will fail silently. The user-initiated scan mail fail with the message "DoScan Error: Failed to initialize scanning engine."

Solution: The scanner was modified to prevent a condition where the length of a user security identifier (SID) could prevent the scan from starting.

SNAC client cannot pass 802.1x authentication when starting

Fix ID: 2589795

Symptom: The SNAC client may not pass 802.1x authentication when the computer is started. The issue is resolved by disconnecting and reconnecting the network cable, or re-authenticating from the system tray icon after system boot up.

Solution: The SNAC client was enhanced with additional logic on computer startup to provide more reliable authentication.

LiveUpdate fails to run when SEPM is configured to use a proxy with Windows Authentication

Fix ID: 2579503

Symptom: LiveUpdate fails to run when SEPM is configured to use a proxy with Windows Authentication. The SEPM administrator log displays the message "Return code = 2". The scm-server-0.log contains the following error:

> *LiveUpdateTask>> CreateProcessAsUser failed with error 2: The system cannot find the file specified.*

Solution: SEPM was modified to remove an extraneous double quote in the command line to run LiveUpdate.

Database size increases rapidly after migration from SEP 11.0 to 12.1

Fix ID: 2585215

Symptom: The database size continues to increase if the replication partner is removed but the remote sites are not removed.

Solution: SEPM was modified to sweep policies and other non-log data after one year if the data has been marked as DELETED. Log data will be swept using the oldest replication time by checking the local site and directly-related sites. A warning message was added when deleting a partner:

> *"If you plan to delete this partner permanently please also delete the partner on the remote site to avoid possible log accumulation."*

A warning message was also added when deleting a site:

> *"If you plan to delete this site permanently please also delete the site on the remote server to avoid possible log accumulation."*

Iexplore.exe or rundll32.exe terminate unexpectedly

Fix ID: 2652223/2652224

Symptom: Internet Explorer (iexplore.exe) or the process rundll32.exe may terminate unexpectedly in the sysfer.dll module.

Solution: Sysfer.dll was modified to prevent the crash.

False positive in Outlook Auto-Protect scan

Fix ID: 2600674

Symptom: Outlook Auto-Protect falsely identifies an attachment as a threat when the attachment is scanned.

Solution: Outlook Auto-Protect was modified to query the file's reputation to reduce false positives. Download Insight must be enabled for this to occur.

Enforcer UI crashes when saving Automatic Quarantine Configuration

Fix ID: 2611696

Symptom: The Enforcer UI crashes when saving the Automatic Quarantine Configuration. When the UI is reloaded, the change was not saved. This issue may also occur when editing Advanced Settings "Select scopes to be enforced."

Solution: The Enforcer UI was modified to prevent the crash. The data is now saved properly.

Bugcheck 9F (DRIVER_POWER_STATE_FAILURE) references SYMEFA64.SYS

Fix ID: 2636799

Symptom: The SEP client experiences a blue screen with bugcheck 9F (DRIVER_POWER_STATE_FAILURE). The blue screen references faulting driver SYMEFA64.SYS.

Solution: The SymEFA64.sys driver was modified to prevent this crash.

Bugcheck D1 (DRIVER_IRQL_NOT_LESS_OR_EQUAL) references SYMNETS.SYS

Fix ID: 2690798

Symptom: The SEP client experiences a blue screen with bugcheck D1 (DRIVER_IRQL_NOT_LESS_OR_EQUAL). The blue screen references faulting driver SYMNETS.SYS.

Solution: The SymNetS.sys driver was modified to prevent this crash.

Client in user mode does not register with the correct client group until the UI is opened

Fix ID: 2559559

Symptom: When the client is configured for a user mode policy, the client does not change to the correct client group when the user first logs in. The client changes to the correct client group when the SEP UI is opened.

Solution: The SEP session plugin (SEPSessionPlugin.dll) was modified to trigger the group change earlier in the login sequence.

SEPM email notifications are sent repeatedly for old events

Fix ID: 2681891

Symptom: Multiple outbreak email notifications are sent during the damper period. Notifications may contain events that are older (30 days) than the triggered event.

Solution: SQL queries were modified to filter out old events and prevent notifications during the damper period.

Error 0x80010000 when searching for clients in the Client Deployment Wizard

Fix ID: 2560486/2668747

Symptom: When searching for computers by IP address range in the Client Deployment wizard, SEPM generates an unexpected error (0x80010000) and the search is stopped. This only occurs if an Unmanaged Detector has found an unknown device which has an IP address within the same range.

Solution: A runtime exception in the SEPM console was resolved to prevent this issue.

ccSvcHst.exe terminates unexpectedly in LueEim.dll

Fix ID: 2523086

Symptom: ccSvcHst.exe terminates unexpectedly in module LueEim.dll at offset 0xd0da.

Solution: The LueEim.dll module was corrected to prevent this crash.

"Error 1920. Service W3SVC (W3SVC) failed to start" during SEPM upgrade from 12.1 to 12.1 RU1

Fix ID: 2631815

Symptom: When upgrading SEPM from 12.1 to 12.1 RU1, the following error appears:

> *"Error 1920. Service W3SVC (W3SVC) failed to start. Verify that you have sufficient privileges to start system services."*

Solution: The SEPM installer was modified to remove the IISExtensionRecycle component if there no IIS (W3SVC) installed on the local machine.

Replication fails with "String index out of range: -1" message

Fix ID: 2533631

Symptom: Replication fails with "String index out of range: -1" on a LiveUpdate policy.

Solution: LiveUpdate servers with empty names are now removed from the policy before replication.

SMC.exe terminates unexpectedly in TSE.dll

Fix ID: 2526701

Symptom: SMC.exe terminates unexpectedly in module TSE.dll at offset 0x2654d.

Solution: The TSE.dll module was corrected to prevent this crash.

Endpoint status shows "out-of-date" when clients are installed with basic AV feature only

Fix ID: 2590266

Symptom: Clients are installed with the basic AV feature only. In the SEPM console and reports, the IPS Signature, SONAR, and Download Protection content are displayed as "out of date." These features are not installed.

Solution: The SEPM console was modified to display out-of-date content only if the features are installed.

Application and Device Control email alerts are sent when Send Email Alerts is disabled

Fix ID: 2586923

Symptom: The "SendEmail Alerts" option is not checked for an Application and Device Control rule. When the rule is triggered, the email alert is still sent.

Solution: Application and Device Control was modified to honor the "Send Email Alert" configuration per rule. If "Send Email Alert" is disabled, the event will not be included in the email notification. If the option "Send Email Alert" is disabled for all application control events, no email will be sent. Application control events can be seen in the notification report if they are excluded from the email content.

Moving a client does not update the SEM_AGENT table in a replication environment

Fix ID: 2652148

Symptom: One or more clients are moved in SEPM. After replication occurs, the clients do not appear in the correct group(s).

Solution: SEPM was modified to update the USN and TIME_STAMP together when the SEM_AGENT is modified to move a client between groups.

LDAP import fails with InvalidNameException

Fix ID: 2586832

Symptom: When importing an OU from LDAP, the import fails. This issue occurs when the user or computer begins or ends with a space. The ADSITask.log displays the message:

> *WARNING: javax.naming.InvalidNameException: <data> [LDAP: error code 34 - 0000208F: LdapErr: DSID-XXXXXXXX,comment: Error processing name, data 0*

Solution: Users or computers that begin or end with a space are not valid AD objects. During import, SEPM will now ignore the record and log an exception for the administrator to review. The remaining (good) records will be imported.

"Disable Symantec Endpoint Protection" option is not available to Domain Administrators when UAC is enabled

Fix ID: 2610970

Symptom: With UAC enabled, the "Disable Symantec Endpoint Protection" option is grayed out from the SEP tray icon for Domain Administrators.

Solution: The SEP client was modified to properly detect domain administrators and enable the option.

SEPM scan log does not display the "scan complete" status for resumed scans

Fix ID: 2628146

Symptom: Scans can be configured to "scan for up to X hours." When such a scan stops, then resumes, a new Scan ID is generated. When the logs are forwarded to SEPM, SEPM cannot correlate the scan stop and start due to the differing Scan ID.

Solution: The SEP client now uses the same Scan ID for resumed scans. SEPM will correlate the stop and start events into a single scan. NOTE: SEPM will list the scan duration as the entire time between scan start and scan complete, including the time the scan was suspended.

Normal user cannot disable the firewall

Fix ID: 2563429

Symptom: A normal/limited user is unable to enable or disable Network Threat Protection on the SEP client. The option to enable/disable NTP is checked in the SEPM policy.

Solution: The SEP client was modified to allow limited/normal users to enable or disable NTP based on the policy setting. NOTE: Guest users cannot enable/disable NTP, regardless of the policy.

Cancelled email message results in a broken attachment

Fix ID: 2680030

Symptom: Internet Email Auto-Protect is enabled and a large attachment is sent. If the message is cancelled from the email client before it is completely sent, it results in a broken attachment for the recipient.

Solution: When a client aborted the connection during the DATA command, ccEmailProxy would incorrectly save the partial contents of the DATA command and relay it to the email server.

Last Time Status Change does not update for some clients

Fix ID: 2632371

Symptom: The SEPM console shows clients with an outdated "Last Time Status Changed" timestamp. The clients are online and functioning correctly.

Solution: A deadlock in SEPM was resolved to allow the agent status to be updated properly.

Computer Version report does not match number of installed clients

Fix ID: 2637838

Symptom: The Computer Version report shows fewer clients than are installed.

Solution: The SQL query for the Computer Version report was modified to display the correct number of installed clients.

Unable to select groups for notification conditions if there are a large number of groups

Fix ID: 2652119

Symptom: When creating a notification condition, the administrator cannot select a group in the drop down list when there are a large number of groups. Selecting any group resets the selection.

Solution: SEPM no longer wraps longer group names to the next line in the drop down list box.

Unable to activate license when regional options are set to Thai

Fix ID: 2516150

Symptom: When regional settings for the operating system are set to Thai, the system cannot apply a license file because it reports it as out of date. When applying an active license, the following error message is displayed:

> *Error: The license has reached its expiration date and is no longer valid. To purchase the license, contact your preferred reseller.*

Solution: The Thai calendar date is now properly converted to the license date for activation.

Unable to delete an administrator account that contains a space in the name

Fix ID: 2616794

Symptom: Unable to delete an administrator account with a space in the name if the administrator is the owner of a scheduled report. SEPM displays the message "Unexpected server error [0x10010000]."

Solution: The owner name is now encoded properly when passed to the URL request.

"An unexpected exception has occurred" logged in the server activity log after SEPM service starts

Fix ID: 2629570

Symptom: "An unexpected exception has occurred" is logged in the server activity log when the SEPM service starts if the computer has no internet connection. The SecurityDataTask runs after SEPM service startup but the computer has no internet connection so it cannot connect to securityresponse.symantec.com. SEPM 11.0 does not have this issue. The scm-server-log shows the following message:

```
SEVERE:  in:com.sygate.scm.server.task.SecurityDataTask

java.net.UnknownHostException: securityresponse.symantec.com
```

Solution: The administrator may disable the SecurityDataTask to avoid the error in the logs. The administrator must edit the conf.properties file and add the following line:

```
scm.server.securitydatatask.disabled=1
```

SEPM failed to publish the HI policy after migration from 11.0 to 12.1

Fix ID: 2638037

Symptom: After migration from SEPM 11.0 to 12.1, the HI policy cannot be published to all client groups. All client HI function is disabled.

Solution: SEPM was modified to prevent a primary key violation while processing HI policies.

"Latest Manager virus definitions" on Home Page is up-to-date even if definitions are outdated

Fix ID: 2622097

Symptom: In a replication environment, some sites have up-to-date content and some are outdated. The "Latest Manager virus definitions" from the up-to-date site is replicated to the other sites.

Solution: The "Latest Manager virus definitions" is no longer replicated if LiveUpdate content is not configured for replication.

SEPM fails to install on an existing database with Microsoft SQL Server 2000

Fix ID: 2528190

Symptom: Installing SEPM on an existing database with SQL Server 2000 fails. The install_log.err displays the following exception:

java.sql.SQLException: Cannot drop the view 'syssegments' because it is a system view

Solution: SEPM no longer attempts to drop the sysconstraints and syssegments tables during installation.

Cisco AnyConnect VPN displays the message "Status: Acquiring network address" when SMC is stopped with the command 'smc -stop'

Fix ID: 2612880

Symptom: When the SEP client is stopped with the 'smc -stop' command, the Cisco AnyConnect VPN Client Connection displays the pop-up message "Status: Acquiring network address."

Solution: The Device Control feature of the client was modified to prevent starting devices that were not disabled by SEP.

SEPM console "Total Endpoints" on Home page does not equal to "Seats Used" on the Licensing status page

Fix ID: 2537023

Symptom: The SEPM console home page number for "Total Endpoints" does not equal the Licensing status page number for "Seats Used"

Solution: A SQL query was corrected to ensure the two figures match.

AutoProtect actions are unlocked for a SEP 11.0 client managed by a SEPM 12.1 server

Fix ID: 2657285

Symptom: The administrator has locked the AutoProtect options by SEPM policy. On a SEP 11.0 client that is managed by a SEPM 12.1 server, the AutoProtect actions are unlocked. This is a cosmetic issue, as the actions are locked correctly.

Solution: SEPM was modified to use the same setting for parent group and sub group when the setting is not overridden.

External communication proxy server port for Windows does not get copied to Mac

Fix ID: 2558263/2614360

Symptom: In the external communication settings, the Windows port does not get copied to the Mac port when the option "Copy proxy settings used for Windows client" is enabled.

Solution: The option "Copy proxy settings used for Windows client" has been removed from the SEPM UI. The Mac port must be configured separately by the administrator.

"Manual scan" displayed instead of "Scheduled scan" in scan log

Fix ID: 2525801

Symptom: When a scheduled scan is started manually it is logged properly as "Manual scan." The next time the scheduled scan starts automatically (on schedule) it will be logged as a "Manual scan" instead of "Scheduled scan."

Solution: The client was modified to properly set the scan type in the registry when the scan starts.

Database maintenance scheduled tasks cannot be configured for 12:00pm

Fix ID: 2577570

Symptom: Database maintenance scheduled tasks cannot be configured for times between 12:00pm and 12:59pm. When saved, the times change to 00:00am to 00:59am.

Solution: The SEPM console was modified to properly accept 12-hour times for database maintenance tasks.

LiveUpdate fails to process content if 8.3 name creation is disabled on NTFS partitions

Fix ID: 2670315

Symptom: LiveUpdate on the SEPM server may fail to process content if 8.3 name creation is disabled on NTFS partitions. This issue does not affect SEP clients.

Solution: Windows LiveUpdate on the SEPM server was updated to allow content processing if 8.3 name creation is disabled.

Windows 7 Professional clients show operating system as "Unavailable" in SPC 2.0 endpoint reports

Fix ID: 2573996

Symptom: In SPC 2.0 endpoint reports, Windows 7 Professional clients show the operating system as "Unavailable." Windows 7 Enterprise clients report correctly as "Windows 7."

Solution: Windows 7 Professional was added to the operating system tables in SEPM to resolve this issue.

Folder/file exclusions in SEPM will not accept the ampersand (&) character

Fix ID: 2564781

Symptom: The ampersand (&) character is a valid file/folder-name character on both Windows and Macintosh. Folder/file exclusions in SEPM do not accept the ampersand (&) character.

Solution: SEPM was modified to allow the ampersand (&) character in file/folder exclusions.

Description field is missing from the Client tab default view

Fix ID: 2553588

Symptom: In the SEPM console client tab (default view) the Description field is missing. This field was present in SEP 11.0.

Solution: The Description field was added to the SEPM console clients tab (default view).

SEPM notification email messages are sent in HTML format

Fix ID: 2483756

Symptom: Email notifications sent by SEPM are in HTML format. In SEP 11.0 the notifications were sent in plain text format.

Solution: SEPM now supports sending email notifications in plain text format. The default format remains HTML. To send notifications in plain text format, the SEPM administrator must edit the conf.properties file on the server and add the following new line:

scm.email.content.type=text/plain

"Top Devices Blocked" report contains duplicate entries

Fix ID: 2630555

Symptom: The "Top Devices Blocked" report contains duplicate entries. The client may need to be rebooted for the report to display duplicates.

Solution: The report will no longer display duplicate entries. In SEP 12.1, the "Top Devices Blocked" report will show both blocked and allowed devices when in log-only mode. This behavior is unchanged.

Daylight Savings Time end date in a report results in inaccurate data

Fix ID: 2613156

Symptom: Specifying a Daylight Savings Time (DST) end date in a report results in start/end times that are offset by one hour. The specified reports, and all subsequent reports, are incorrect until the administrator logs off from SEPM.

Solution: A JavaScript function was modified to correctly support DST time.

Custom proxy settings remain in the UI after being deleted

Fix ID: 2594355

Symptom: In the SEP client UI, if the custom proxy settings are entered, then later removed, the settings remain in the UI.

Solution: The SEP client UI was modified to clear the custom proxy settings if they are no longer used.

Scheduled or on-demand reports do not calculate local time offset properly

Fix ID: 2634774

Symptom: Scheduled or on-demand reports do not calculate the local time offset properly when the start or end time exceeds 12:00am UTC. This affects reports that use the virus definition date as a risk factor.

Solution: For the purposes of reporting, SEPM was modified to use the virus definition date only to determine if definitions are out-of-date. Virus definition dates do not specify a time.

Defwatch quickscan is logged as "defwatch scan"

Fix ID: 2553839

Symptom: Two different scans occur after a new set of definitions arrive: 1) Defwatch quarantine scan - this scans the quarantine and 2) Defwatch quickscan - this is an active scan. The second scan is logged as "defwatch scan" instead of "defwatch quickscan."

Solution: Scan logging was modified to identify certain defwatch scan events (start, stop, abort, pause, and resume) as "defwatch quick scan" in the scan log. Items in the risk log, if detected, will be logged as "defwatch scan," independently of the scan type.

Compliance report "Failed" filter cannot be saved

Fix ID: 2589909

Symptom: The Compliance Report "Failed" filter cannot be saved. The report will show passed clients only.

Solution: The SEPM console was modified to correctly save the compliance report filter.

Compliance report "Subnet" filter cannot be saved

Fix ID: 2591284

Symptom: The Compliance Report "Subnet" filter cannot be saved. SEPM displays the "group" report only.

Solution: The SEPM console was modified to correctly save the compliance report filter.

Virus and Spyware policy has misleading description for Log Event Aggregation

Fix ID: 2627792

Symptom: The Virus and Spyware policy “Log Event Aggregation” setting has the following description:

> *"Specify how often client computers send aggregate events to the server. Send aggregated events every __ minutes"*

This setting can be confused with the heartbeat.

Solution: The description for Log Event Aggregation has been updated to the following:

> *"Specifies how long the client aggregates similar events. After the time period expires, the client sends the aggregated events to the management server at the next heartbeat. Aggregate log events for __ minutes"*

Link to the SEPM web console cannot be opened

Fix ID: 2619570

Symptom: Email notifications sent by SEPM have a link to the SEPM web console. The link does not include a fully-qualified domain name.

Solution: SEPM now includes a link to the fully-qualified domain name (FQDN) if it can be determined. If the FQDN cannot be determined, the link will include the host name only.

Client with a large number of interfaces fails to communicate with the server

Fix ID: 2585839

Symptom: A client with a large number of network interface cards or loopback adapters fails to communicate with the SEPM server. The client fails to generate a hardware ID (HWID).

Solution: The client was corrected to account for a large number of network interface cards or loopback adapters.

Windows Backup Server failure after SEP 12.1 is installed

Fix ID: 2652280

Symptom: Windows Backup Server is configured to back up the "System State". When the backup needs to prune the destination drive the operation will fail with an access violation error. The Windows Backup logs may contain the following message:

> *“Error in deletion of [C:\System Volume Information\EfaData\] while pruning the target VHD: Error [0x80070020] The process cannot access the file because it is being used by another process.”*

Solution: The client was modified to exclude the EfaData folder. This exclusion only takes effect for new backups. Existing backups must be manually removed before the next backup will succeed.

Encrypted offline files cannot be accessed or may display incorrectly

Fix ID: 2668853

Symptom: After installing the SEP 12.1 client, encrypted Windows offline files cannot be accessed or the file contents do not display correctly. The problem does not occur when offline file encryption is disabled.

Solution: The AutoProtect kernel driver (srtsp.sys) was modified to perform unbuffererd I/O on encrypted files on Windows Vista and later operating systems.

SEPM cannot process LiveUpdate content, or replication of content fails, in a Japanese environment

Fix ID: 2673317/2621376

Symptom: SEPM can download LiveUpdate content, but fails to process it. SEPM may also fail to replicate content or policy data. This issue affects the Japanese localized product only. The SesmLU.log shows the following error message:

> *ERROR: sesmIPSdef32 SesmLu Failed to notify SESM servlet of new LiveUpdate package.at .\SesmLu.cpp[1319]*

Solution: A JDBC driver issue was resolved to allow SEPM to process binary stream data properly.

Admin user with read-only access cannot search clients

Fix ID: 2679121/2694803

Symptom: The search client function is not allowed for a limited administrator with read-only privileges.

Solution: The ability to search clients was re-enabled for limited administrators with read-only privileges.

Access to DFS shares is slower when Application and Device Control is enabled

Fix ID: 2685572

Symptom: Performance of DFS file shares on mapped drives is slower when Application and Device Control is enabled.

Solution: Application Control performance is improved by converting the DFS mapped drive to the underlying network path.

Windows 7 standard user is allowed to disable the firewall

Fix ID: 2740045

Symptom: A normal or standard user on Windows 7 is allowed to disable the SEP client firewall, even if disallowed by policy

Solution: The SEP client was modified to honor the firewall policy for all Windows 7 user types.

“Deployment target version” is localized in Spanish instead of Italian

Fix ID: 2696557

Symptom: In the Italian SEPM console, on the client properties “general” tab, the string for “deployment target version” is localized in Spanish instead of Italian.

Solution: The string was properly localized into Italian.

Translation error for Event ID 34 in German

Fix ID: 2699722

Symptom: "When the SEP Master Service is started, two Windows Events are logged in the Windows Application Log:

Event ID 34: ""The SepMasterService is Starting""

Followed by

Event ID 35: ""The SepMasterService has Started""

On a German operating system the event ID 34 string is logged incorrectly:

Event ID 34: ""Der Dienst 'SepMasterService' wurde deinstalliert."""

Solution: The German translation was modified to resolve this issue.

German translation for “Default Group” is incorrect

Fix ID: 2722148

Symptom: In the SEPM console, the translation for Default Group into German is "Std.gruppe." It should be translated as "Standardgruppe.”

Solution: The translation was corrected to “Standardgruppe.” During upgrade to RU1-MP1, the migration process will detect and convert the default group to the new translation.