# Fix Notes for Symantec Endpoint Protection 12.1.2

## Component Versions

| | |
|---|---|
| **AutoProtect** | 14.2.0.7 |
| **AutoProtect Driver** | 14.2.0.6 |
| **AV Engine** | 20121.2.1.2 |
| **AV Engine Driver** | 20121.2.1.2 |
| **BASH Defs** | 7.1.1.5 |
| **BASH Defs Driver** | 7.1.1.5 |
| **BASH Framework** | 7.0.0.226 |
| **CIDS Defs** | 11.1.1.5 |
| **CIDS Defs Driver** | 11.1.1.5 |
| **CIDS Framework** | 11.1.0.73 |
| **Common Client** | 12.1.1.5 |
| **DecABI** | 2.3.0.22 |
| **DefUtil** | 4.6.1.11 |
| **DuLuCallback** | 1.5.0.69 |
| **ECOM** | 121.2.0.79 |
| **ERASER** | 112.2.0.13 |
| **ERASER Driver** | 112.2.0.13 |
| **Iron** | 3.1.0.12 |
| **Iron Driver** | 3.1.0.11 |
| **LiveUpdate (server)** | 3.3.100.15 |
| **LiveUpdate Express (client)** | 2.2.0.102 |
| **MicroDefs** | 3.6.0.79 |
| **SymDS** | 2.1.0.9 |
| **SymDS Driver** | 2.1.0.9 |
| **SymEFA** | 4.1.1.10 |
| **SymEFA Driver** | 4.1.1.9 |
| **SymELAM** | 1.0.0.111 |
| **SymELAM Driver** | 1.0.0.111 |
| **SymEvent** | 12.9.3.2 |
| **SymEvent Driver** | 12.9.3.1 |
| **SymNetDrv** | 13.1.0.8 |
| **SymNetDrv Driver** | 13.1.0.7 |
| **SymVT** | 5.1.0.9 |

## Top Impacting Issues Resolved in this Release

### Old definitions require a reboot in order to be removed

**Fix ID:** 2692127

**Symptom:** Old definitions appear to require a reboot in order to be removed. This is usually due to a scan running at the time of the update.

**Solution:** Updated the Common Client component to resolve a condition where the scanner held the virus definitions open, which prevented an update.

### Policy updates are not saved to the embedded database or distributed to clients.

**Fix ID:** 2819061

**Symptom:** Policy updates are not being saved to the embedded database, and changed policy profiles are not distributed to clients. PackageTask appears to be stopped or hung.

**Solution:** Changed the database configuration to allow idle connections to be disconnected. This allows system resources to be recycled.

### Symantec Endpoint Protection and Lotus Notes both crash with Lotus Notes plug-in installed (enabled or disabled)

**Fix ID:** 2665371

**Symptom:** The Lotus Notes Email Auto-Protect plug-in crashes, which cause Symantec Endpoint Protection and Lotus Notes to crash. These crashes occur even if you disable the plug-in.

**Solution:** Added code to better clean up after previous installs, and to update the notes.ini file before nlnvp.dll is launched.

### Install fails with message "StartService() failed for service 'BHDrvx64' with error 0x00000057."

**Fix ID:** 2638836

**Symptom:** Installation of the Symantec Endpoint Protection client fails or rolls back. The SIS_INST.LOG contains the following message "[StartService] StartService() failed for service 'BHDrvx64' with error 0x00000057."

**Solution:** Modified a driver to prevent a SONAR initialization error during installation.

### Windows Backup Server fails to back up after the installation of Symantec Endpoint Protection 12.1

**Fix ID:** 2745055

**Symptom:** Windows Backup Server fails to back up after the installation of Symantec Endpoint Protection 12.1.

**Solution:** Changed the process for detecting delete operations by Windows Backup Server on Symantec Endpoint Protection data files.

## Machines with large amounts of memory trigger Server Health

**Fix ID:** 2765283 / 2772948

**Symptom:** Machines with large amounts of memory (8GB physical RAM or +) exhibit high mapped file memory usage for the sem5.db (embedded DB) file, and generate low memory health notifications.

**Solution:** Changed the default caching parameters for starting the database service, and added a way to keep the original parameters if needed.

## Single risk events are sent multiple times an hour

**Fix ID:** 2788568 / 2850335 / 2805245

**Symptom:** Single risk events are sent multiple times an hour when they should not be.

**Solution:** Changed the way multiple notifications are triggered.

## App-V virtualized applications cannot load with Proactive Threat Protection installed

**Fix ID:** 2689005

**Symptom:** App-V virtualized applications cannot load with Proactive Threat Protection installed.

**Solution:** Changed Application Control and User Mode Hooking to allow NTDLL image validation.

## Incorrect date or state for Intrusion Prevention signatures

**Fix ID:** 2525136

**Symptom:** After the Symantec Endpoint Protection client updates Intrusion Prevention signatures, the client interface displays the wrong content version or the wrong state for Intrusion Prevention.

**Solution:** Faster internal notification of updated content and status.

## Cannot get the definition detail for some client entries

**Fix ID:** 2693845

**Symptom:** Cannot get the definition detail for some client entries after upgrading from Symantec Endpoint Protection 11.x to 12.1.

**Solution:** Added a flag to return all data rows.

## Excessive non-paged memory used by Symantec Endpoint Protection client

**Fix ID:** 2733231

**Symptom:** The Symnets.sys driver (pool tag SND1) slowly consumes a large amount of non-paged pool memory, eventually leading to a system crash.

**Solution:** Updated the SymTDI driver to resolve a non-paged pool memory leak.

## Home tab shows virus definition information "not available" after replication

**Fix ID:** 2825751

**Symptom:** Home tab shows virus definition information "not available" after replication. An update resolves the incorrect information, but only until the next replication.

**Solution:** Modified Symantec Endpoint Protection Manager to obtain the correct sequence number from the database.

## Windows 7 clients (32- and 64-bit) enables the Windows Firewall when you upgrade directly from Symantec Endpoint Protection 11 RU6 MP3

**Fix ID:** 2722224

**Symptom:** Windows 7 clients (32- and 64-bit) enables the Windows Firewall when Symantec Endpoint Protection Manager upgrades directly from version 11 RU6 MP3 to 12.1 RU1.

**Solution:** Changed the code so the migration process properly maintains the Windows Firewall settings.

## Possible Blue Screen of Death (BSOD) on Vista OS

**Fix ID:** 2489813

**Symptom:** Possible Blue Screen of Death (BSOD) on Vista OS occurs after upgrading from Symantec Endpoint Protection 11.x.

**Solution:** Correctly unload the Symantec Endpoint Protection 11.x service SymTDI, and keep track of each service installed to prevent accidental disabling of a legitimate service.

## Symantec Endpoint Protection Manager Limited Administrator experiences performance issues when they access either the Java or Web remote console

**Fix ID:** 2717943

**Symptom:** Symantec Endpoint Protection Manager Limited Administrator experiences performance issues when they access either the Java or Web remote console.

**Solution:** Changed the group query method.

## The links to Symantec Security Response from the Home tab do not correctly redirect with a proxy

**Fix ID:** 2722657

**Symptom:** The links to Symantec Security Response from the Home tab do not correctly redirect within a proxy environment.

**Solution:** Now allows correct redirection of the link.

## Replication fails with "Invalid Hex String:0x00000000” and "LOGIN FAILED" errors.

**Fix ID:** 2811424 / 2722248 / 2911663

**Symptom:** Replication fails with "Invalid Hex String:0x00000000” and "LOGIN FAILED" errors.

**Solution:** Removed the invalid prefix from the hex string.

## SQL cluster node BSOD during failover

**Fix ID:** 2853447

**Symptom:** A SQL cluster node crashes with "Bug Check 0x9E: USER_MODE_HEALTH_MONITOR" during a failover.

**Solution:** Modified the SymEFA driver to cancel the operation and allow the volume to be detached during a cluster node failover.

## Applications are slow to launch over the network

**Fix ID:** 2756476

**Symptom:** Applications are slow to launch over the network after Symantec Endpoint Protection client is installed. Disabling the SymTDI driver resolves the issue.

**Solution:** Updated the SymTDI driver to improve performance of large networked files.

## ThinApp portable applications are slow to start from network share

**Fix ID:** 2645151

**Symptom:** Applications that are packaged as VMware ThinApp portable applications are slow to launch when the application is launched via a network share.

**Solution:** Modified the Auto-Protect driver to honor exonerated network files when the network scan on execute option is enabled.

## A filter to limit the results on the Deployment Report incorrectly returns all results

**Fix ID:** 2676753

**Symptom:** A filter for the Deployment Report intended to limit results to a specific time range incorrectly returns all deployed clients.

**Solution:** Changed the variable by which the report defined deployment times.

## ArcServer Backup fails to back up Hyper-V virtual workstations

**Fix ID:** 2729418

**Symptom:** ArcServer Backup fails to back up Hyper-V virtual workstations with Symantec Endpoint Protection 11.x installed.

**Solution:** Updated Auto-Protect to address this issue.

## When using a filter, the daily and weekly status reports include all Symantec Endpoint Protection clients

**Fix ID:** 2734454

**Symptom:** The daily and weekly status reports include all Symantec Endpoint Protection clients, even if you select only specific client groups.

**Solution:** Added the client group filter when generating daily and weekly status reports.

## Plugging in an NTFS-formatted USB disk causes Explorer.exe to stop responding

**Fix ID:** 2736323

**Symptom:** Plugging in an NTFS-formatted USB disk causes Explorer.exe to stop responding.

**Solution:** Updated the Auto-Protect driver (srtsp.sys) to resolve a deadlock involving other filter drivers.

## Each replication rebuilds all policy files even if there are no changes, and clients download them repeatedly

**Fix ID:** 2745696

**Symptom:** Under certain circumstances, each replication rebuilds all policy files even if there are no changes. Since the policy serial number changes, clients download the policy profile repeatedly.

**Solution:** Changed replication logic to prevent this specific replication event from occurring.

### The current IPS Definitions displays as "Not Available"

**Fix ID:** 2758416

**Symptom:** In the Symantec Endpoint Protection Manager client properties, the current IPS Definitions displays as "Not Available."

**Solution:** Fixed a database query responsible for the incorrect information.

### ArrayIndexOutOfBoundsException and data store errors appear, so the remaining client data logs are not parsed

**Fix ID:** 2815571 / 2849197 / 2860247

**Symptom:** "ArrayIndexOutOfBoundsException" and data store errors appear. As a result, the remaining client data logs are not parsed.

**Solution:** Changed the way long log entries are processed.

### Event ID 577 appears in the Security Log

**Fix ID:** 2822356

**Symptom:** Event ID 577 appears in the Windows Security Log when Symantec Endpoint Protection is installed

**Solution:** Modified the Common Client component to check for necessary privileges on Windows XP and Windows Server 2003.

### Attachments take a long time to open with the Outlook Email Auto-Protect enabled

**Fix ID:** 2865495 / 2851779

**Symptom:** In Outlook 2010, attachments take a long time to open with the Outlook Email Auto-Protect plug-in enabled.

**Solution:** Improved the method for saving the temporary file for scanning.

## All Resolved Issues

### Symantec Endpoint Protection Manager Limited Administrator with access rights to run commands cannot run commands for read-only groups

**Fix ID:** 2707321

**Symptom:** Symantec Endpoint Protection Manager Limited Administrator with access rights to run commands cannot run commands for read-only groups.

**Solution:** Changed the code so that Limited Administrators can now run commands on read-only groups.

## SNAC Enforcer cannot write log data to syslog

**Fix ID:** 2679480

**Symptom:** There is no Enforcer support for syslog.

**Solution:** SNAC Enforcer adds support for logging to a syslog server. You can configure this through Symantec Endpoint Protection Manager in the Enforcer settings > Log Settings tab.

## LiveUpdate Engine does not allow NTLM proxy authentication

**Fix ID:** 2608676

**Symptom:** LiveUpdate Engine does not allow NTLM proxy authentication.

**Solution:** Added support for NTLM proxy in LiveUpdate Engine. This option can be configured in the LiveUpdate settings policy. Select Server Settings, then Configure Proxy Options. The "NT LAN Manager Authentication" option appears at the bottom of the authentication settings.

## Computer crashes with Bug Check 0xD1: DRIVER_IRQL_NOT_LESS_OR_EQUAL

**Fix ID:** 2763669 / 2779756 / 2820996

**Symptom:** The computer crashes with Bug Check 0xD1: DRIVER_IRQL_NOT_LESS_OR_EQUAL referencing SYMTDI.SYS.

**Solution:** Modified the SYMTDI driver to prevent this crash.

## During peak hours, Apache crashes and the Symantec Endpoint Protection Manager becomes unresponsive

**Fix ID:** 2885456

**Symptom:** The Apache process (httpd.exe) crashes during peak hours. The Symantec Endpoint Protection Manager becomes unresponsive.

**Solution:** Fixed the synchronization issues that cause Apache to crash.

## Symantec Endpoint Protection Manager 12.1 RU1 replication times out and fails after four hours

**Fix ID:** 2654549

**Symptom:** Replication times out after four hours, with a repeated warning In ReplicationRemote-0.log: "BaseMetadataCollection>> saveToFile: file exists!!"

**Solution:** Fixed the code that generated the message.

## Unable to disable Network Threat Protection using a command

**Fix ID:** 2753106

**Symptom:** Unable to disable Network Threat Protection using a command from Symantec Endpoint Protection Manager. Instead, you get a command status message of "rejected."

**Solution:** The command from Symantec Endpoint Protection Manager now disregards any client-side locks on Network Threat Protection.

## Client bypasses the newly promoted Group Update Provider despite policy that states it should never bypass the Group Update Provider

**Fix ID:** 2757957

**Symptom:** Clients bypass newly promoted Group Update Provider and contact Symantec Endpoint Protection Manager directly for content, even though policy states it should never bypass the Group Update Provider.

**Solution:** Client does not bypass the Group Update Provider if policy is set to "never bypass," even if the new Group Update Provider's guplist.xml is still empty.

## Cannot validate database when using Windows with NTLMv2

**Fix ID:** 2682376 / 2845764

**Symptom:** When you configure Windows to use NTLMv2, the database validation tool (dbvalidator) fails to complete.

**Solution:** Changed the code to check whether NTLMv2 is in use.

## Unable to send email with Internet Email Auto-Protect enabled

**Fix ID:** 2702851

**Symptom:** User or application cannot send email when the Internet Email Auto-Protect feature is enabled.

**Solution:** Updated the email proxy component of Common Client to address this issue.

## Computer crashes with Bug Check 0x8E: KERNEL_MODE_EXCEPTION_NOT_HANDLED

**Fix ID:** 2740714

**Symptom:** The computer crashes with Bug Check 0x8E: KERNEL_MODE_EXCEPTION_NOT_HANDLED referencing SRTSP.SYS

**Solution:** Modified the Auto-Protect driver to prevent a crash due to a compatibility issue between mounted volumes and Windows System Restore.

## SecurityMiningTask won't run and data is missing from the SEM_COMPLIANCE_CRITERIA table.

**Fix ID:** 2808901

**Symptom:** SecurityMiningTask won't run and data is missing from the SEM_COMPLIANCE_CRITERIA table.

**Solution:** Modified Symantec Endpoint Protection Manager to prevent a condition where multiple SecurityMiningTasks could create a deadlock.

## Microsoft Remote Access Service (RASMAN) fails to start after migrating to Symantec Endpoint Protection 12.1.x, then uninstalling it

**Fix ID:** 2740733

**Symptom:** Migrating from Symantec Antivirus 10.1 to Symantec Endpoint Protection 12.1.x, then uninstalling Symantec Endpoint Protection 12.1.x, causes Microsoft Remote Access Service (RASMAN) to fail to start.

**Solution:** Changed the condition for registry key backup action for the RASMAN service.

## Installation to thin client fails with reference to invalid memory

**Fix ID:** 2746057

**Symptom:** Installation to a thin client fails. The SymEvent log file contains the message:

The instruction at "0x0040a7c5" referenced memory at "0x00000000". The memory could not be "read".

**Solution:** Modified the SymEvent component to correct a crash on installation.

## Excessive SMB traffic with Symantec Endpoint Protection client installed

**Fix ID:** 2819666 / 2769637

**Symptom:** Excessive SMB traffic occurs between a Symantec Endpoint Protection client and a file server.

**Solution:** Skips and marks reputation queries as done if the file has a network path.

## Host Integrity verification erroneously results in quarantine

**Fix ID:** 2811107

**Symptom:** Clients pending Host Integrity verification are erroneously sent to the quarantine location.

**Solution:** Changed to distinguish a pending status from a failure.

## Unable to connect to Microsoft Exchange Server through WatchGuard SSL VPN

**Fix ID:** 2848103

**Symptom:** Unable to connect to Microsoft Exchange Server through WatchGuard SSL VPN. The connection is successful when the SYMNETS driver is disabled.

**Solution:** Modified the SYMNETS driver to prevent a condition where network data was incorrectly blocked.

## Network storm and outage due to AutoUpgrade

**Fix ID:** 2795300

**Symptom:** The AutoUpgrade feature in the enterprise version causes a network storm / outage when Randomize Days is set to 0. All clients begin downloading upgrades at the same time.

**Solution:** Added warning message to caution against setting the minimum randomize days value to 0, or to a value calculated to be too low for the number of clients set to automatically upgrade.

## Unable to select Symantec Endpoint Protection Manager dashboard dropdown menus when using Internet Explorer 9

**Fix ID:** 2665692 / 2727520

**Symptom:** Unable to select Symantec Endpoint Protection Manager dashboard dropdown menus when using Internet Explorer 9.

**Solution:** Added a header to recognize and display Symantec Endpoint Protection Manager in IE 9 mode.

## Conflict with Lotus Notes Email Auto-Protect causes application crash

**Fix ID:** 2715933

**Symptom:** Certain applications crash with the Lotus Notes Email Auto-Protect plug-in installed.

**Solution:** The Lotus Notes shutdown routine now runs after deregistering the extension manager.

## Unable to determine the last connected NAT IP of a virtual Symantec Endpoint Protection client

**Fix ID:** 2721540

**Symptom:** The last connected NAT IP of a virtual Symantec Endpoint Protection client is not available in the Symantec Endpoint Protection Manager console.

**Solution:** The last connected IP is saved in the Symantec Endpoint Protection Manager database. This data is available per client in the client properties (in the Network tab) and in the computer status logs.

## Schedule scan runs again after the last missed scheduled scan completes

**Fix ID:** 2681132

**Symptom:** The scheduled scan runs three minutes after the last missed scheduled scan completes.

**Solution:** Removed the code to update the LastStart value in the Schedule key, as this caused the LastStart to be the same as the LastCompleted time.

## Repeated detection of DWHxxxx.tmp as a threat

**Fix ID:** 2718341

**Symptom:** Repeated detection of DWHxxxx.tmp as a threat when a Defwatch scan runs on Quarantined items.

**Solution:** Increased Defwatch scan performance and moved the temporary extraction folder from %TEMP% to Application Data to avoid conflicts with Windows Search Indexer.

## Scheduled scan missed event does not run because of a policy update

**Fix ID:** 2732977

**Symptom:** Scheduled scan missed event does not run because of a policy update upon next heartbeat to the Symantec Endpoint Protection Manager.

**Solution:** Changed the way missed scan events are handled if a policy update occurs.

## Incorrect status display for Proactive Threat Protection in Symantec Endpoint Protection client interface

**Fix ID:** 2735831

**Symptom:** Disabling Auto-Protect then disabling Proactive Threat Protection causes an incorrect status display for Proactive Threat Protection under Status > Details. The incorrect status reads, "Disable all Proactive Threat Protection features" instead of "Enable Proactive Threat Protection."

**Solution:** Added an OR condition when Proactive Threat Protection is disabled, even if Auto-Protect status is off.

## Startup scan displays pop-up notification, even if pop-up notifications are disabled

**Fix ID:** 2810984

**Symptom:** Startup scan displays pop-up notification, even if pop-up notifications are disabled for Active Scans.D14

**Solution:** The Active Startup Scan and Active Scheduled Scan now properly add the registry value 'DisplayStatusDialogIfHighMediumDetected' during migration from 12.1 RTM to 12.1 RU1 or later.

## The SMC service terminates on Group Update Providers

**Fix ID:** 2722802

**Symptom:** For Symantec Endpoint Protection client computers acting as Group Update Providers, the SMC service terminates. If you manually restart the service, it terminates again in two hours.

**Solution:** Modified SMC to prevent a crash when the client is a Group Update Provider.

## When "Scan files on remote computers" is disabled, the child setting "Only when files are executed" is still enabled

**Fix ID:** 2777576

**Symptom:** When the Auto-Protect network drive scanning setting, “Scan files on remote computers," is disabled, the child setting "Only when files are executed" is greyed out but still enabled. This feature still scans files on remote computers.

**Solution:** When you disable the parent setting, all child settings automatically disable.

## Check Point VPN Adapter not detected as a VPN adapter by the firewall

**Fix ID:** 2810794

**Symptom:** The Check Point VPN Adapter is not detected as a VPN adapter by the Symantec Endpoint Protection firewall.

**Solution:** If an adapter is online whose description contains the name "Check Point Virtual Network Adapter," the firewall recognizes that Check Point Client VPN is connected.

## NTFS corruption when bringing a Virtual Hard Disk online

**Fix ID:** 2570905

**Symptom:** NTFS corruption occurs with Symantec Endpoint Protection installed when bringing a Virtual Hard Disk online in Windows Server 2008 R2.

**Solution:** Changes to Auto-Protect address this issue.

## The computer freezes when clicking on an EICAR file

**Fix ID:** 2748135

**Symptom:** The computer freezes when clicking on an EICAR file.

**Solution:** When Auto-Protect processes a suspected threat, it cancels actions to open a file and dismisses actions to close a file.

## Firewall policy stops blocking after 24 hours, starts blocking again if you restart the SMC service

**Fix ID:** 2680390

**Symptom:** After 24 hours, the firewall no longer blocks previously blocked websites. If you restart the SMC service, they are blocked again.

**Solution:** Changed the way the firewall handles DNS cache overflows.

## Application and Device Control causes Compass 4.25 to fail

**Fix ID:** 2641442

**Symptom:** Application and Device Control in Symantec Endpoint Protection 12.1 RU1 causes Compass 4.25 to fail.

**Solution:** Changed how Application and Device Control handles 16-bit Windows applications.

## Symantec Endpoint Protection Small Business Edition 12.1 RU1 unable to add complete Exchange exclusions

**Fix ID:** 2723712

**Symptom:** Symantec Endpoint Protection Small Business Edition 12.1 RU1 client on Windows Small Business Server 2011 cannot add complete Microsoft Exchange exclusions.

**Solution:** Changed the query for Microsoft Exchange to more accurately detect the installation and add exclusions.

## Computer crashes with Bug Check 0x7F: UNEXPECTED_KERNEL_MODE_TRAP

**Fix ID:** 2776662

**Symptom:** The computer crashes with Bug Check 0x7F: UNEXPECTED_KERNEL_MODE_TRAP due to Double Fault.

**Solution:** This version of Symantec Endpoint Protection reintroduces the KStackMinFree registry value. You can adjust this value to set the minimum kernel stack needed for scanning. Customers should contact Symantec Technical Support for instructions on how to properly configure the value.

## Installation packages do not sort properly when you choose sort by "Created Time"

**Fix ID:** 2690913

**Symptom:** Sorting items by date results in incorrect order.

**Solution:** Convert formatted dates to raw date format before they are sorted.

## Compliance report entries that contain international characters are garbled

**Fix ID:** 2730728

**Symptom:** Compliance report entries that contain international characters are garbled.

**Solution:** Converted logs to UTF16 formatting.

## Symantec Endpoint Protection Manager is not creating deltas in timely manner

**Fix ID:** 2742344

**Symptom:** Symantec Endpoint Protection Manager gets so many repeated requests for the same content deltas, it cannot create those deltas.

**Solution:** Added a table to Secars to hold a list of pending requests; then only new requests are sent to Symantec Endpoint Protection Manager.

## Replication fails due to an improperly handled comma in report filter name

**Fix ID:** 2690962 / 2856990

**Symptom:** Replication fails due to an improperly handled comma in report filter name.

**Solution:** Changed the code so the whole filter name is processed as one.

## Out-of-date virus definition notifications are incorrect

**Fix ID:** 2863845

**Symptom:** Out-of-date virus definition notifications are incorrect.

**Solution:** Notifications now show the correct information.

## A false SNMP trap triggers against the CPU status

**Fix ID:** 2777494

**Symptom:** A false SNMP trap triggers against the CPU status.

**Solution:** Changed the code to use a 64-bit integer in the CPU info to avoid this false SNMP trap.

## Default "Configure Refresh Interval" combined with default "Symantec Endpoint Protection Status" procedure results in Kaseya server instability

**Fix ID:** 2812805

**Symptom:** The Kaseya Symantec Endpoint Protection Plug-in Deployment Settings are set by default to refresh every five minutes. This setting causes the default procedure "Symantec Endpoint Protection Status" to be run every five minutes. This may generate a large volume of queries and result in deadlocks or a Kaseya server crash.

**Solution:** The starting time for the scripts now spreads across a 30 minute interval to ensure scripts are not running at the same time. Two scripts can run every second for up to 30 minutes. For example:

10 machines would be spread over 5 seconds, with 2 machines per second.

120 machines would be spread over 1 minute, with 2 machines per second.

3600 machines would be spread over 30 minutes, with 2 machines per second.

7200 machines would be spread over 30 minutes, with 4 machines per second.

## "Detect servers and endpoints" cannot be restricted by Machine Group or ID

**Fix ID:** 2812810

**Symptom:** Clicking on the "Detect..." button finds server and endpoints among all of the machines in Kaseya, even if the user has a filter set in the Machine Filter bar.

**Solution:** Changed the queries to be Machine Filter-aware.

## IE "stop running this script" failure on Symantec Endpoint Protection Kaseya Plug-in Audit Log

**Fix ID:** 2881618

**Symptom:** Unable to open the Symantec Endpoint Protection Audit Log. Internet Explorer prompts you to click whether or not you wish to stop running the script. Both choice results in failure and you cannot access the log.

**Solution:** Modified the Symantec Endpoint Protection Audit Log to prevent this issue.

## Symantec Endpoint Protection Kaseya Plug-in Audit Log rows displayed filter does not work

**Fix ID:** 2885652

**Symptom:** The Symantec Endpoint Protection Kaseya Plug-in v1.5 does not filter the Audit Log by the maximum row count per page.

**Solution:** Modified the Symantec Endpoint Protection Audit log to honor the maximum row count filter.

## Application and Device Control policy does not honor allowed processes or folders on 64-bit Windows 7

**Fix ID:** 2751878

**Symptom:** The list of allowed processes/folders is not honored on 64-bit Windows 7.

**Solution:** Modified Application and Device Control to resolve this issue.

## Unable to launch cmd.exe after installing Symantec Endpoint Protection 12.1 RU1 MP1 client

**Fix ID:** 2852273

**Symptom:** Unable to launch cmd.exe after installing Symantec Endpoint Protection 12.1 RU1 MP1 on a 64-bit Windows client due to compatibility issue with Skysea software.

**Solution:** Changed the way Application Control interacts with cmd.exe so that Skysea can recognize it.

## Connected applications disconnect after updating the Intrusion Prevention signatures

**Fix ID:** 2865665

**Symptom:** Connected applications disconnect after updating the Intrusion Prevention signatures.

**Solution:** Sets a flag to ensure that the appropriate packets are allowed during update process.

## Incorrect sorting of the column "Definitions Date"

**Fix ID:** 2632418

**Symptom:** Incorrect sorting of the column "Definitions Date" from Monitors > Logs > Computer Status.

**Solution:** Changed the field by which the column is sorted.

## Upgrading from 12.1 RTM to 12.1 RU1 removed custom client purge settings

**Fix ID:** 2637853

**Symptom:** An upgrade from 12.1 RTM to 12.1 RU1 removed custom client purge settings and reset them to defaults.

**Solution:** Saves client purge settings from site properties to domain properties during upgrade process.

## Unable to select different language client packages via the Client Deployment Wizard

**Fix ID:** 2641702

**Symptom:** Unable to select different language client packages via the Client Deployment Wizard.

**Solution:** Append a language tag when adding client packages to a group.

## Cannot load the Symantec Endpoint Protection Manager from the Symantec Protection Center 2.x once the logon banner is enabled

**Fix ID:** 2685653

**Symptom:** Cannot load the Symantec Endpoint Protection Manager from the Symantec Protection Center 2.x once the logon banner is enabled. Error: "Internal Error - Check log file for details and the stack trace."

**Solution:** Changed the order in which the frames load in the Symantec Protection Center.

## Management Server Wizard description for optional Enforcer appliances is not correct

**Fix ID:** 2689017

**Symptom:** There is an incorrect description in the fifth pane of Management Server Configuration Wizard. "This password will be required if you install optional Enforcer appliances" is not correct.

**Solution:** Reworded the Management Server Wizard description for clarity.

## LAN Enforcer RADIUS group policies are empty

**Fix ID:** 2741567

**Symptom:** The RADIUS Server Groups list may be incorrectly shown as empty unless there is also a switch policy. Once a switch policy is created, the missing RADIUS groups may appear again.

**Solution:** Modified Symantec Endpoint Protection Manager to correctly check if the switch policy is empty.

## Replication site cannot login with the error: "Unable to connect to the server specified."

**Fix ID:** 2879943 / 2683207

**Symptom:** After configuring a replication partner via the Management Server Configuration Wizard, the replication site cannot login with the error: "Unable to connect to the server specified." The admin password included a special character, %, which is a reserved character for URLs.

**Solution:** Changed so that the special character is translated E58before sending out the password for remote login.

## Non-English daily and weekly reports display the incorrect date and time.

**Fix ID:** 2912692 / 2883896

**Symptom:** Non-English daily and weekly reports display the incorrect date and time, such as "01/01/1970".

**Solution:** Added code to convert the retrieved date to the expected date of format "YYYY-mm-dd" in the SQL query.

## The Symantec Endpoint Protection Manager does not receive virus definition updates, even if a replication partner received the update

**Fix ID:** 2922555

**Symptom:** PackageTask fails to complete, preventing the update of the virus definitions on the Symantec Endpoint Protection Manager, even if a replication partner received the update.

**Solution:** Changed code to allow for successful completion of PackageTask.

## Replication hangs, which causes the Symantec Endpoint Protection Manager to hang

**Fix ID:** 2848668

**Symptom:** Replication hangs, which causes the Symantec Endpoint Protection Manager to hang.

**Solution:** Changed the way replication interacts with the mail utility.

## Security event log records an audit failure Event ID 560 when starting a Symantec Endpoint Protection service

**Fix ID:** 2672119

**Symptom:** Security event log records an audit failure Event ID 560 for object access for every attempt to start a Symantec Endpoint Protection service.

**Solution:** Changed the access right on the service start to avoid this audit failure.

## Setup.exe cannot expand an environmental variable during installation

**Fix ID:** 2675376

**Symptom:** Setup.exe cannot expand an environmental variable, such as %systemdrive%, during installation.

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

### The Action List report includes Symantec Endpoint Protection 11.x client data

**Fix ID:** 2753449

**Symptom:** The Action List report includes Symantec Endpoint Protection 11.x client data, which contradicts a statement in the report.

**Solution:** Removed the disclaimer in the Action List report.

### In scheduled reports, the "group by" field continues to display an incorrect value after choosing a different filter.

**Fix ID:** 2757279

**Symptom:** In scheduled reports, the "group by" field continues to display an incorrect value after choosing a different filter.

**Solution:** Corrected the values by which the reports are grouped.

### Enforcer Activity log settings do not produce the results you expect

**Fix ID:** 2776010

**Symptom:** Enforcer Activity log settings are unclear in the user interface, and do not produce the results you expect.

**Solution:** Updated the text on the “Log Settings” and the text on the Monitors tab under the Compliance log type.

### Notifications & Reports display too many devices

**Fix ID:** 2801881

**Symptom:** In Symantec Endpoint Protection 11.0 you could create notifications that only displayed blocked devices. In Symantec Endpoint Protection 12.1 the same notifications display all devices.

**Solution:** Improved notifications so that they no longer display disabled devices.

### Initial replication to SQL Server fails

**Fix ID:** 2850167

**Symptom:** The initial replication of a new site fails if the transaction log is larger than 8 GB.

**Solution:** Symantec Endpoint Protection Manager now shrinks the transaction log before replication.

## Unable to set scan report filter settings back to the default value

**Fix ID:** 2780518

**Symptom:** Unable to set scan report filter settings back to the default value of zero (0).

**Solution:** Allowed "0" for the scan filter.

## For Symantec AntiVirus for Linux client reports do not reflect current information

**Fix ID:** 2855262

**Symptom:** For Symantec AntiVirus for Linux client reports, the "Last Scan Time" is never updated, and always shows "Never" in the computer status logs.

**Solution:** Changed to update last scan time when processing security log from Symantec AntiVirus for Linux clients.

## The sort order is incorrect for Show LiveUpdate downloads

**Fix ID:** 2905112

**Symptom:** The sort order is incorrect under Admin > Servers > Local Site > Show LiveUpdate downloads.

**Solution:** Changed sort order to use date comparison.

## Symantec Endpoint Protection for Macintosh LiveUpdate progress dialog is blank

**Fix ID:** 2639169

**Symptom:** The Japanese Symantec Endpoint Protection for Mac 12.1 RU1 client shows a blank LiveUpdate progress dialog.

**Solution:** Modified LiveUpdate for Macintosh to correct this issue.

## Symantec Endpoint Protection for Macintosh clips some strings in the context menu

**Fix ID:** 2739747

**Symptom:** The Japanese Symantec Endpoint Protection for Mac client clips some strings in the context menu.

**Solution:** The clipped strings now display in full.

## The Outlook Auto-Protect plug-in logs silent detections

**Fix ID:** 2671594 / 2777532

**Symptom:** The Outlook Auto-Protect plug-in logs Bloodhound.Exploit.446 detections, which is a silent detection.

**Solution:** Apply existing checks for silent detections to non-compressed files.

## Syntax errors appear when you submit items to the Quarantine Server

**Fix ID:** 2747299

**Symptom:** Syntax errors pertaining to SDPck32i.dll appear when you submit items to the Quarantine Server.

**Solution:** Recompiled the Scan and Deliver binary.

## "Unable to open file" for various file paths when you run the Virtual Image Exception tool

**Fix ID:** 2897351

**Symptom:** Error messages appear for various file paths when you run the Virtual Image Exception tool: "PM ERROR: Unable to open file." The file paths do not actually exist.

**Solution:** Disables File System Redirection on 64-bit OS before enumerating file paths, and reverts File System Redirection to its original state when all files have been processed.

## Custom application settings for Network Threat Protection disappear when upgrading

**Fix ID:** 2678247

**Symptom:** Custom application settings for Network Threat Protection disappear when upgrading from Symantec Endpoint Protection 11.0 RU7 to Symantec Endpoint Protection 12.1 RU1.

**Solution:** Application settings are now migrated from Symantec Endpoint Protection 11.0.x to Symantec Endpoint Protection 12.1.2.

## The "Latest from Symantec" date is earlier than the "Latest on Manager" date

**Fix ID:** 2651631

**Symptom:** The "Latest from Symantec" definitions revision date on the Home tab of the Symantec Endpoint Protection Manager is earlier than the "Latest on Manager" definitions revision date.

**Solution:** Updated code to reflect the actual "Latest from Symantec" definitions revision date.

## Computer Status log displays incorrect data

**Fix ID:** 2653137

**Symptom:** Computer Status log displays incorrect data when filtered by Definition Date.

**Solution:** Changed the variable by which the data is filtered.

## Out-of-date Intrusion Prevention signature data incorrectly appears in the Endpoint Status chart.

**Fix ID:** 2763130

**Symptom:** If you uncheck the "Percentage of computers reporting out-of-date Intrusion Prevention signatures" in the Home page preferences, this change does not affect the Home page Endpoint Status chart.

**Solution:** Out-of-date checking of IPS definitions is disabled if "Percentage of computers reporting out-of-date Intrusion Prevention signatures" is unchecked.

## The Symantec Endpoint Protection Manager console immediately logs out due to multiple NICs

**Fix ID:** 2811561

**Symptom:** The Symantec Endpoint Protection Manager console immediately logs out after login on a server that has multiple NICs.

**Solution:** Symantec Endpoint Protection Manager performs matching between IP address and host name to resolve this issue.

## The system log contains blanks for the Symantec Endpoint Protection Japanese client

**Fix ID:** 2841583

**Symptom:** The system log contains blanks for the Symantec Endpoint Protection Japanese client.

**Solution:** The Japanese client now indicates when LiveUpdate cannot connect to the server.

## Data within the Symantec Endpoint Protection Japanese client logs get garbled when you click to sort the columns.

**Fix ID:** 2733575

**Symptom:** Data within the Symantec Endpoint Protection Japanese client logs get garbled when you click to sort the columns.

**Solution:** Changed how the data is sorted when clicking on the column header.

## Upgrade from Symantec Endpoint Protection 11.x deletes shared DLLs.

**Fix ID:** 2839333

**Symptom:** Upgrade from Symantec Endpoint 11.x to 12.1 on a 64-bit operating system deletes shared DLLs.

**Solution:** Changed lookup mechanism for SharedDLLs during the upgrade process.E92

## ccSvcHst crashes frequently and randomly

**Fix ID:** 2695895

**Symptom:** ccSvcHst crashes frequently and randomly.

**Solution:** Modified The AVHostPlugin.dll loaded by ccSvcHst.exe to prevent this crash.

## Stationery-based emails with an attachment disappear

**Fix ID:** 2760344

**Symptom:** Stationery-based emails with an attachment disappear after you send them when Lotus Notes Auto-Protect is installed.

**Solution:** Symantec Endpoint Protection no longer adds certain properties to stationery-based emails.

## ccSvcHst.exe crashes on shutdown

**Fix ID:** 2793958

**Symptom:** ccSvcHst.exe crashes on shutdown.

**Solution:** Changed code to allow for graceful shutdown.

## Symantec Endpoint Protection Internet Email Auto-Protect blocks email notifications from Norton Ghost

**Fix ID:** 2885909

**Symptom:** Symantec Endpoint Protection Internet Email Auto-Protect blocks email notifications from Norton Ghost.

**Solution:** Updated the email proxy component of Common Client to address this issue.

## The data within a computer status log report disappear

**Fix ID:** 2701203

**Symptom:** The data within a computer status log report disappear after an automatic refresh.

**Solution:** Removed extra slashes from group name before being saved in the database.

## "Last Scan" time does not match the "Scan Start" time

**Fix ID:** 2744246

**Symptom:** The "Last Scan" time does not match the "Scan Start" time.

**Solution:** Changed code so that the two dates match.

## AutoUpgrade notification message is empty

**Fix ID:** 2664598

**Symptom:** The notification message text box for the AutoUpgrade setting is empty. It should have the default text.

**Solution:** The default notification message is applied when clicking the "Use Default" button. The notification message is not saved if the notification is disabled.

## Audit log fails to export any data

**Fix ID:** 2673833 / 2637938

**Symptom:** Audit log fails to export any data except for column headers.

**Solution:** Changed the way date information is processed prior to writing to the log.

## Client details incorrectly indicate the status has never changed

**Fix ID:** 2681947

**Symptom:** Computer status report correctly shows the last time the status changed, but the client details indicate the status has never changed.

**Solution:** Changed the source of the client details.

## The LUDBfix tool does not work on the embedded database

**Fix ID:** 2699754

**Symptom:** The LUDBfix tool does not work on the embedded database to fix broken links.

**Solution:** Modified the LUDBfix tool to work on the embedded db.

## Client Inventory Details incorrectly report list definitions versions as "Not Available"

**Fix ID:** 2730270

**Symptom:** Client Inventory Details report list definitions versions as "Not Available" when selecting a specific definition date filter.

**Solution:** Changed the query to correctly return the client's content revisions. "Not Available" is only displayed if the content is not installed or not supported by the client, such as Mac.

## Risk Detection Counts Report shows no data

**Fix ID:** 2735365

**Symptom:** Risk Detection Counts Report shows no data when filtered by Group.

**Solution:** Replaced HTML entities in client group name. For example: "\" is converted into “\” (backslash).

## Unable to enable On Demand Client on the Enforcer

**Fix ID:** 2727493

**Symptom:** Unable to enable On Demand Client on the Enforcer in a French language Symantec Endpoint Protection Manager.

**Solution:** Use an alternate translation of the group name "My Company" to eliminate the international character.

## The weekly "Rebuild Indexes" task runs one day earlier than expected

**Fix ID:** 2784331

**Symptom:** The weekly "Rebuild Indexes" task runs one day earlier than expected.

**Solution:** Changed code to correctly calculate when the task should run, and to compute the next scheduled rebuild index task.

## Forward slashes are incorrectly displayed in the file path

**Fix ID:** 2863471

**Symptom:** Forward slashes are incorrectly displayed in the file path in the Symantec Endpoint Protection Manager's application log.

**Solution:** Replaced the forward slashes with backslashes.

## Unable to make policy changes and the clients cannot update

**Fix ID:** 2875586

**Symptom:** Unable to make policy changes and the clients cannot update due to LiveUpdate content broken links in the database.

**Solution:** Deletes the broken links automatically if there are no related records in the database.

## ArcServer Backup fails to back up Hyper-V virtual workstations

**Fix ID:** 2729418

**Symptom:** ArcServer Backup fails to back up Hyper-V virtual workstations with Symantec Endpoint Protection 11.x installed.

**Solution:** Updated Auto-Protect to address this issue.

## Inconsistent reports of infected files

**Fix ID:** 2771319

**Symptom:** The number of infected files reported by Auto-Protect is different than the number reported by the Symantec Endpoint Protection log.

**Solution:** Updated Auto-Protect file statistics to address this issue.

## Microsoft Dynamics intermittently fails to send email invoices

**Fix ID:** 2785611

**Symptom:** Microsoft Dynamics intermittently fails to send email invoices when Internet Email Auto-Protect is enabled or installed.

**Solution:** Updated the email proxy component of Common Client to address this issue.

## Groups fail to apply new feature set with Auto Upgrade

**Fix ID:** 2632218

**Symptom:** Groups fail to apply new feature set if Auto Upgrade has previously changed the feature set at least three times.

**Solution:** Changed the destination copy folder to the temporary folder.

## File copy fails with "Access Denied" message

**Fix ID:** 2782347

**Symptom:** Copying or moving a file when the destination file has the same name (will be overwritten) results in the message "Access Denied."

**Solution:** Modified the Auto-Protect driver to correct a file synchronization issue.

## Computer crashes with Bug Check 0xD1: DRIVER_IRQL_NOT_LESS_OR_EQUAL

**Fix ID:** 2553308

**Symptom:** The computer crashes with Bug Check 0xD1: DRIVER_IRQL_NOT_LESS_OR_EQUAL referencing IDSxpx86.sys.

**Solution:** Modified the Intrusion Prevention driver to prevent this crash.

## High CPU usage of ccSvcHst.exe process

**Fix ID:** 2707848

**Symptom:** The Symantec Endpoint Protection service (ccSvcHst.exe) consumes 100% of one CPU during a scan.

**Solution:** Modified the Decomposer component to prevent a condition where the scanner could become stuck on a malformed archive file.

## Cluster environment does not fail over

**Fix ID:** 2731793

**Symptom:** A cluster environment does not fail over when Symantec Endpoint Protection client is installed due to inability to unload drivers.

**Solution:** Modified a driver to properly detach from a volume when the volume dismounts.

## Performance of App-V applications is slow

**Fix ID:** 2825796

**Symptom:** Applications using Microsoft Application Virtualization (App-V) are slower to launch and slower to execute.

**Solution:** Modified a driver to allow the scanner to store cached data in memory for App-V virtualized applications.

## Computer crashes with Bug Check 0xD1: DRIVER_IRQL_NOT_LESS_OR_EQUAL

**Fix ID:** 2733440

**Symptom:** The computer crashes with Bug Check 0xD1: DRIVER_IRQL_NOT_LESS_OR_EQUAL referencing SYMNETS.SYS.

**Solution:** Modified the SYMNETS driver to correct this crash.

## Microsoft Direct Access network traffic is blocked

**Fix ID:** 2745094

**Symptom:** Traffic to Microsoft Direct Access (DA) servers is blocked when Symantec Endpoint Protection is installed and network threat protection is enabled. Traffic is still blocked with an "allow all" rule.

**Solution:** Modified the SYMNETS driver to allow Direct Access traffic.

## Unable to complete initial replication. Connection/socket is dropped before data.zip is done, with error "Connection reset by peer: socket write error."

**Fix ID:** 2869914

**Symptom:** Replication of a large database to a newly added site takes a long time, then exits with an error because the TCP socket connection closes. This may occur if you have configured a firewall or similar device to kill idle connections.

**Solution:** Allow a way to perform manual replication by copying the data.zip created on the remote site to the new site:

1. Edit conf.properties and add the following entry:

   scm.replication.inbox.drop=true

2. Copy data.zip into [Symantec Endpoint Protection Manager install directory]\data\replication\inbox\[remote site id]

3. Relaunch the configuration wizard to complete the replication and site setup.

This will only affect the initial replication when a new site is added. After replication, the "replication guid" entry should be removed from conf.properties.

## Replication of a large database to a newly added site fails despite keepalive packet configuration

**Fix ID:** 2881885

**Symptom:** Replication of a large database to a newly added site takes a long time, then exits with an error because the TCP socket connection closes. This occurs even if you have configured the Symantec Endpoint Protection Manager to send keepalive packets.

**Solution:** Truncated SEM_CONTENT table on the new site. In the short term, this means you cannot get accurate information from the new site about virus definition revisions on each client at first. Eventually, each client checks in to that site to populate this and other information, which is then replicated.

## Older .Net applications fail to launch with Application and Device Control enabled

**Fix ID:** 2805543

**Symptom:** Older .Net applications, such as scriptlogic.cbm.agent.exe, fail to launch with Application and Device Control enabled.

**Solution:** Resolved an issue where Application and Device control failed to properly detect 32-bit vs. 64-bit .Net applications due to a conflict with Citrix Offline plug-in.

## A Symantec Endpoint Protection Mac client with a teamed NIC cannot register

**Fix ID:** 2096474

**Symptom:** A Symantec Endpoint Protection Mac client with a teamed NIC cannot register with Symantec Endpoint Protection Manager.

**Solution:** Now treats a teamed virtual interface as a valid Ethernet interface, which allows the Mac client to register.

## Symantec Endpoint Protection Manager does not transfer logs to a Syslog server in a timely manner

**Fix ID:** 2700001 / 2877068

**Symptom:** Transfer of risk logs to the external Syslog server by the Symantec Endpoint Protection Manager occurs after a delay as long as two hours.

**Solution:** Ensured that all the risk logs can be sent out within fifteen minutes.

## Sub-OUs of deleted OUs still appear in dropdown menus

**Fix ID:** 2713695

**Symptom:** After deleting an imported organizational unit (OU) at the root level, sub-OU groups appear in the Group dropdown menus under Monitors > Reports.

**Solution:** Correctly identifies and deletes the identity map values of the sub-OU groups.

## Date information missing on the Home tab on the Chinese language Symantec Endpoint Protection Manager

**Fix ID:** 2722741

**Symptom:** Chinese language Symantec Endpoint Protection Manager console definition date displays incorrectly on the Home tab. It is missing the date information.

**Solution:** Excluded improperly translated Korean and Taiwanese double-byte character set.

## Error: "JDesktop Integration Components binary has stopped working"

**Fix ID:** 2724433

**Symptom:** Error appears after clicking on “View Notifications" on the Home Tab: "JDesktop Integration Components binary has stopped working."

**Solution:** Changed the way the Symantec Endpoint Protection Manager passes the parameters.

## Typographical error in UAC warning with Java remote console

**Fix ID:** 2743343

**Symptom:** There is a typographical error in the UAC warning when you use the Java remote console.

**Solution:** Changed the description from:

> "If the User Account Control in Control Panel is enable, then part of remote console content will not be accessible."

to:

> "If Windows User Account Control is enabled, some portions of the remote Symantec Endpoint Protection Manager Console may not be accessible."

## The Security Status shows attention needed, but the details pane does not show a problem

**Fix ID:** 2769815

**Symptom:** The Home tab says "Security Status - Attention Needed" but clicking on View Details shows everything is good (green).

**Solution:** Added "License Problem" to the Security Status Detail page.

## Notifications incorrectly go to Limited Admins

**Fix ID:** 2815268

**Symptom:** Symantec Endpoint Protection Manager Limited Administrators receive notification emails from groups to which they have no access.

**Solution:** Verifies permission conditions when sending notification emails to Limited Administrators.

## The Symantec Management Client (SMC) service crashes

**Fix ID:** 2671737

**Symptom:** The Symantec Management Client (SMC) service crashes if the description field in an Application and Device Control rule contains asterisks.

**Solution:** Clears the description field before logging if the field contains asterisks.

## Only a limited number of Firewall rules are visible

**Fix ID:** 2727592

**Symptom:** There is a limitation to the number of firewall rules visible under "View Firewall Rules" on the Symantec Endpoint Protection client.

**Solution:** Removed the priority limitation so that all rules display correctly. Previously, the rule viewer would only show rules with a priority of less than 255.

## Application and Device Control policy fails to block "Apple Mobile Device USB Driver" on a physical machine

**Fix ID:** 2730712

**Symptom:** Application and Device Control policy fails to block Apple Mobile Device USB Driver on a physical machine.

**Solution:** Application and Device Control now correctly blocks this USB bus controller.

## The JAWS screen reader does not read the field titles in the Symantec Endpoint Protection Manager 12.1

**Fix ID:** 2658515

**Symptom:** JAWS, a screen reader for Windows, is not able to read text on login screen of Symantec Endpoint Protection Manager.

**Solution:** Updated the Symantec Endpoint Protection Manager login screen text fields to allow JAWS to read the text field names using AccessibleContext. Additional steps may be required to install JAB (Java Access Bridge) into the Symantec Endpoint Protection Manager version of JRE. Please contact Support and reference TECH177395 for details.

## The Network Threat Protection traffic log report displays Ethernet protocol events as EHERENET

**Fix ID:** 2672953

**Symptom:** The Network Threat Protection traffic log report within Symantec Endpoint Protection Manager displays the wrong name for the Ethernet protocol.

**Solution:** Updated to reflect the correct name.

## Symantec Endpoint Protection Manager incorrectly displays the rule condition in the Application Control log

**Fix ID:** 2702850

**Symptom:** Symantec Endpoint Protection Manager incorrectly displays the rule condition under "Rule Name" in the Application Control log.

**Solution:** Displays both rule name and rule condition under the "Rule Name" column.

## Dates in Symantec Endpoint Protection Manager show in the wrong format for "English (UK)"

**Fix ID:** 2762719

**Symptom:** Dates in Symantec Endpoint Protection Manager show in the "English (US)" format (MM-DD-YY) instead of the "English (UK)" format (DD-MM-YY).

**Solution:** Updated code to use the date format of the region indicated in the Windows control panel.

## Symantec Endpoint Protection client notification area (tray) icon does not appear if Hitachi HIBUN is also installed

**Fix ID:** 2621590

**Symptom:** Symantec Endpoint Protection client notification area (tray) icon does not appear if Hitachi HIBUN is also installed.

**Solution:** Resolved an issue in the SLIC licensing component that prevented it from loading when HIBUN was installed.

## Modification date of Notes document is changed while Notes Auto-Protect is enabled

**Fix ID:** 2641817

**Symptom:** When you open an attachment file, Notes Auto-Protect scans it, even though the Notes document has not been updated or the virus definition has not been updated since the last scan for the temporary file.

**Solution:** Improved the bookkeeping function when Notes Auto-Protect scans an attachment, so that the plug-in skips the file next time if it remains unchanged.

## File operations too slow with Symantec Endpoint Protection client and SOXBOX agent

**Fix ID:** 2662063

**Symptom:** Symantec Endpoint Protection client and SOXBOX agent installed together cause file operations to run too slowly.

**Solution:** SymEFA no longer enables an NTFS change journal for the SOXBOX agent's hidden NTFS volume.

## ccSvcHst.exe crashes on scanning a particular compressed file.

**Fix ID:** 2758005

**Symptom:** The ccSvcHst.exe crashes while scanning a particular .rar (archive) file.

**Solution:** Updated the Decomposer engine to address this issue.

## Encrypted, read-only devices become writable on Japanese systems

**Fix ID:** 2792591

**Symptom:** Safend-encrypted read-only USB drive becomes writable if you reformat it twice as NTFS on a Japanese system using Symantec Endpoint Protection.

**Solution:** Changed SymEFA allow it to properly close the volume handle.

## Auto-Protect setting "Delete newly created security risk if the action is 'Leave alone (log only)'" does not have a lock option.

**Fix ID:** 2653057

**Symptom:** The Auto-Protect setting "Delete newly created security risk if the action is 'Leave alone (log only)'" does not have a lock option.

**Solution:** Updated the Symantec Endpoint Protection client user interface to add a lock to this option.

## Certain passwords cause irregular behavior with password security features

**Fix ID:** 2693672

**Symptom:** Certain passwords cause irregular behavior with password security features on the Symantec Endpoint Protection client.

**Solution:** Changed the way password string is verified to avoid a NULL value.

## High SQL Server utilization and deadlocks on the Kaseya server

**Fix ID:** 2885687

**Symptom:** Users with large numbers of endpoints (>1500) are seeing deadlocks and extensive SQL Server utilization on the Kaseya server.

**Solution:** Modified the Kaseya plug-in to improve performance with a large number of clients.

## Replicated virus and spyware protection policies reverting back to the previous settings

**Fix ID:** 2961739

**Symptom:** When you enable replication, virus and spyware protection policy changes revert back to the previous settings after a short period of time.

**Solution:** Corrected the policy verification algorithm to properly merge both name and code elements.

## Dump files contain unknown strings from the ExternalLoggingTask

**Fix ID:** 2930359

**Symptom:** When you enable the security log in external logging, the agt_security.tmp file or agt_security.log records and HI check result or firewall check result. The logs contain erroneous

ExternalLoggingTask messages. For example: "!ExternalLoggingTask.localport! 0,!ExternalLoggingTask.remoteport! 0,!

ExternalLoggingTask.cidssignid! 0,!ExternalLoggingTask.strcidssignid! ,!

ExternalLoggingTask.cidssignsubid! 0,!ExternalLoggingTask.intrusionurl! ,!

ExternalLoggingTask.intrusionpayloadurl!"

**Solution:** Corrected the logging code to use standard property names and entries in the property files.

## The Symantec Endpoint Protection Manager web console freezes on a non-English operating system

**Fix ID:** 2949053

**Symptom:** When you open the web console on a non-English operating system computer, any pop up dialogs such as "Search Clients" or "Create Group" fail to open. You do not see the problem on the Java Remote Console.

**Solution:** Included a new AjaxSwing module that resolves this issue.