IVANTI PATCH FOR SERVERS VERSION HISTORY

PATCH FOR SERVERS 9.3

9.3.4379.0

Released 4/24/2017

MAJOR NEW FEATURES

- Application Program Interface (API)

  The API feature is meant for advanced users who have a working knowledge of PowerShell and who want to perform tasks beyond those available through the Ivanti Patch for Windows® Servers user interface. You can use the API feature to:

  - Interact with different systems in your environment
  - Script a sequence of complex events that contain dependencies
  - Perform bulk operations or process list inputs from other systems
  - Programmatically stage patch deployments or initiate patch downloads
- Folder Paths in Navigation Pane

  Another new feature is the ability to create a hierarchical structure for your machine groups, patch scan templates and patch deployment templates. If you create many groups or templates, you should consider organizing them into logical folders. Doing so will enable you to quickly locate and manage your groups and templates.

- Staged Deployments

  There are now four discrete schedulable points in the patch scanning and deployment process. This gives you much greater control over the entire process. You might:

  - Perform a scan only
  - Perform a scan and then stage the missing patches on the target machine at a specific time without installing the patches
  - Perform a scan, stage the missing patches and then install the patches at a time of your choosing
- Scheduled Snapshot Maintenance

  This new feature enables you to schedule a one-time or recurring task that will remove old virtual machine snapshots from the server. Previously, the only way you could remove old snapshots was in real time during a deployment task.

- Ability to Use a Third-Party Certificate Authority (CA)

You have the option to use a trusted certificate authority (CA) from your own PKI infrastructure to issue a replacement root certificate for Ivanti Patch for Windows® Servers. This is not a necessity, but if you use a security tool that sees the default self-signed root certificate as a medium-level security risk, a process in now available for generating a replacement certificate.

MINOR FEATURES AND ENHANCEMENTS

- New Skins

  A new option is now available on the **Display Options** dialog that enables you to specify the color theme you want to use for the Ivanti Patch for Windows® Servers interface. In addition to choosing a color that suits your eye, you might also consider a skin that provides lots of contrast, particularly in low-bandwidth RDP environments.

- Scheduled Remote Tasks Manager

  There are several changes to the Scheduled Remote Tasks Manager.

  - It is now accessed by right-clicking on a machine in either Machine View or Scan View and then selecting **View scheduled tasks**.
  - Information about power tasks and patch deployment tasks is now presented in a format that is similar to the Scheduled Console Tasks Manager.
  - It will now display tasks that are scheduled on the remote machine using either the Ivanti Scheduler or the Microsoft Task Scheduler.

- New Column Filter Capabilities

  You can now apply filters to one or more column headers in the grid. You do this by hovering over a column header and then clicking the filter icon located in the upper-right corner.

- Manual Download Method

  A new **Download method** column indicates whether a patch can be downloaded automatically or if it must be downloaded manually.

- Deployment Configuration Information

  The **Deployment Configuration** dialog now shows information about the disk space requirements when deploying patches.

- Consolidated Program Options

  All program options are now consolidated in a single location. To view the options, select **Tools** > **Options**.

- Patch Group Filter

  Patch View contains a new patch group filter. The **Show patches (above) currently included in the selected Patch Group** checkbox enables you to choose whether patches contained in the selected patch group will be displayed in the Patch View list.

- Deployment Tracker UI Changes

  Deployment Tracker has been redesigned to provide more detail about the patch deployment tasks that are currently in progress. You can also now use Deployment Tracker to cancel a deployment.

- Export Download Package

  You can now export the download links for selected patches to a Comma Separated Values (CSV) file. This is especially useful for a console that is in a disconnected environment. The CSV file can be used by a connected machine to download the patches and the patches can then be copied into the disconnected console's patch directory.

- New IAVA Reports

  Two new IAVA reports are now available: Machine Compliance (IAVA) and Machine Non-Compliance (IAVA). These two reports contain additional information that is required by the U.S. Government when submitting report data.

- Global Thread Pools

  Thread Management has moved from the template level to a system-wide pool and is now defined on the **Tools > Options > Patch** dialog. By default the program will use 8 threads per CPU core, but you can adjust the value as you see fit. This single value specifies the total number of threads that can be used during a patch scan or deployment, an asset scan or a power status scan.

- Expanded Search Capabilities

  The product's search capabilities have been extended into more areas. You can now perform searches:

  - On the **Hosted Virtual Machines** tab of a machine group.
  - By right-clicking any machine group in the navigation pane and selecting **Search Machine Groups**. This enables you to locate specific machines and groups across all of your machine groups.
  - Using the new Search box in the middle pane in Scan View and Machine View.

DEPRECATED FEATURES

The following features have been removed from Ivanti Patch for Windows® Servers 9.3:

- Threat management (antivirus and Active Protection) is no longer offered with the product
- SQL Server 2005 is no longer supported as a database; the new minimum is SQL Server 2008
- The following platforms are no longer supported for use with agents:
  - Windows XP
  - Windows Server 2003
  - Windows Server 2008 R2 Gold

Windows XP, Windows Server 2003, and Windows Server 2008 R2 Gold are still supported for agentless scans.

RESOLVED ISSUES

- Resolved an issue where exporting a report with over 77,000 rows caused the program to crash.
- Resolved an issue where adding the Vendor Name column and then filtering caused the program to crash.
- Resolved an issue where an empty patch group would crash the console following an upgrade.
- Resolved an issue where an agent deployment would fail due to a large exitCode value.
- Resolved an issue where performing an agent scan every eight seconds caused problems.
- Resolved an issue where agents would stop reporting data if the lsbin file grew too large.
- Resolved an issue with reports whose names were longer than 100 characters.
- Resolved an issue with Asian characters in a user's profile during a scheduled scan.
- Resolved an issue where enabling the Scan Only Servers check box caused the program to crash when running an ITScript.
- Resolved an issue with batch jobs in the Scheduled Console Tasks Manager.
- Resolved an issue where scanning with a VM template crashed the program.
- Resolved an issue where custom patches did not appear in a deployment template's Custom Actions patch list file.
- Resolved an issue where database maintenance fails when attachment types 3, 4 and 5 existed.
- Resolved an issue where database maintenance would timeout when working with a 234 GB database.
- Resolved an issue where deleting the temporary staging folders caused the deployment to fail.
- Resolved an issue where the Deployment Notification report did not get sent when the deployment was a scheduled deployment.
- Resolved an issue where a Deployment Tracker query put too big a load on SQL server.
- Resolved an issue where deployments failed because of a problem stopping the SQL server instance.
- Resolved an issue where the Detailed Summary report did not get emailed when scanning a nested group.
- Resolved an issue where having a disabled Microsoft Scheduler service caused Ivanti Scheduler deployments to fail.
- Resolved an issue where passwords greater than 122 characters caused distribution server downloads and proxy authentication to fail during deployment.
- Resolved an issue where having duplicate ESX Hypervisor hosts caused the program to crash on startup.
- Resolved an issue where deleting a machine from Machine View caused a crash when the program was unable to contact and uninstall an agent on that machine.
- Resolved an issue where the deployment dialog would indicate that a reboot would occur even though the deployment template specified that no reboot would be performed.
- Resolved an issue where the Not Previously Scanned machine count was wrong in the Executive Summary.
- Resolved an issue where an Excel file would be exported with the wrong file extension.
- Resolved an issue where exporting a report with a .xlsx format would crash the program.
- Resolved an issue where disconnected users were unable to export download information for missing patches.

- Resolved an issue where the Report Gallery dialog was inadvertently closed after generating a report.
- Resolved an issue where using local account credentials that contained either a \ or a workgroup name caused a vCenter connection error and deployments to fail during copy.
- Resolved an issue where the Scan only filter in a machine group did not work correctly with hosted VMs.
- Resolved an issue where importing a file into a machine group caused a crash.
- Resolved an issue where the patch count was counting newly scanned machines twice.
- Resolved an issue where the progress bar showed green even if a patch failed.
- Resolved an issue discovering Windows 10 machines.
- Resolved an issue where exporting a large PDF report from the Machine Status Summary caused a crash.
- Resolved an issue where the information in the Machines Not Scanned tab and in the Executive Summary did not match.
- Resolved an issue with a timer that prevented a custom action from completing.
- Resolved an issue with performing a manual scan/auto deployment that caused the program to hang.
- Resolved an issue where more than one unrecognized product on a system prevented results from being imported.
- Resolved an issue modifying a distribution server with credentials shared by another user.
- Resolved an issue with saving an agent policy so that a check-in request was not required.
- Resolved an issue with opening a patch group that did not contain a name.
- Resolved an issue with memory leaks associated with opening agent policies.
- Resolved an issue with the maximum randomization interval time for patch tasks.
- Resolved an issue where the Patch Properties options were missing from the Patch Status Detail.
- Resolved an issue where Patch View search results showed no data.
- Resolved an issue with patch scan imports.
- Resolved an issue with invalid KB values in patch groups.
- Resolved an issue with misleading patch group error output.
- Resolved an issue with inconsistent field names between the UI and the API.
- Resolved an issue with agent recertification requests when using Protect Cloud.
- Resolved an issue with continuous time-outs with Protect Cloud.
- Resolved an issue with role-based security attempts to find users that would crash the program if the user count exceeded 1000 users.
- Resolved an issue with syncing distribution servers that caused program exceptions.
- Resolved an issue with a slow refresh files process that would at times crash the program.
- Resolved an issue where removing temp file did not delete patches after deployment.
- Resolved an issue where renaming a virtual machine from upper case to lower case caused an importer error.
- Resolved an issue where the selected item in the navigation pane changed after clicking View Results following a scan.
- Resolved an issue where role-based administration would allow an unspecified user access to the program.
- Resolved an issue running batch operation not running in the native platform architecture.
- Resolved an issue where after an upgrade, scan would not work from a patch scan template that was not previously opened and then saved.
- Resolved an issue where the scanner would return an error when opening a breadcrumb.
- Resolved an issue with excluding a device from an OU would not exclude the machine during a scan.
- Resolved an issue where scheduled jobs would fail to schedule between 6pm and 12am when using the Microsoft Scheduler.

- Resolved an issue where a scheduled Machine Status by Patch Count report used all scans rather than just the current scan.
- Resolved an issue where the scheduler folder did not appear in the C:\ProPatches directory.
- Resolved an issue where all custom actions would not be performed after a scheduled deployment to a virtual machine.
- Resolved an issue where the search filter caused a crash.
- Resolved an issue where duplicate trace results and invalid trace results were being bundled.
- Resolved an issue where a failover from the Ivanti Scheduler to the Microsoft Scheduler did not work.
- Resolved an issue where the Shift/Ctrl key multi-select behavior was incorrect in the Reports and Advanced options.
- Resolved an issue where a software asset scan would generate a malformed XML when a “registry type is not supported error occurred.
- Resolved an issue where connecting to a hypervisor with a duplicate virtual machine would cause the program to error.
- Resolved an issue where custom actions trace lines were not included in the trace logs.
- Resolved an issue where the Test existence/credentials command incorrectly showed success.
- Resolved an issue where the safe reboot dialog incorrectly showed the Extend time button.
- Resolved an issue upgrading the console OS to Windows 10.
- Resolved an issue where you were unable to add virtual machines to a machine group from the Virtual Inventory list.
- Resolved an issue where uninstalling the asset engine restarted the target machine without warning.
- Resolved an issue where refreshing content caused an error.
- Resolved an issue where the engines would determine the wrong OS service pack level.
- Resolved an issue where users assigned to individual machines would incorrectly get information about all machines in email and in reports.
- Resolved an issue where virtual machine IP addresses that contained a space at the end would cause the console to crash.

PROTECT 9.2

9.2.5119.0 UPDATE 3

Released 7/7/2016
Resolved Issues

- Resolved an issue where disabling the Microsoft Scheduler Service causes Shavlik Scheduler deployments (STDeploy) to fail.
- Resolved an issue where the maximum value for the Randomize scheduled time option was limited to 240 minutes. The new maximum is 1 minute less than the interval defined. For a daily patch task this can be randomized to a new maximum of 23 hours and 59 minutes.
- Resolved an issue where the Report Gallery closes after generating the report.
- Resolved an issue where hosted virtual deployments would only run the first custom action in the deployment template.
- Resolved an issue where a scan could return an Error 13 if deployment breadcrumb information is missing.
- Provided additional logging around custom actions during deployment.

- Resolved an issue where a scan with Auto-deploy could hang if you deploy to the same machine twice in a row. Specifically, this occurred if a test deployment was run followed by a real deployment.
- Resolved an issue in role-based administration where an unspecified user could gain full access to Protect. This bypassed the role-based feature set, but did not allow a user who was less than a full administrator to access Protect.
- Resolved an issue where jobs scheduled to execute between 6pm-12am would fail to schedule when using the Microsoft Scheduler.
- Resolved an issue where the Shavlik Protect console would crash if a VMware VM had an IP with a space at the end.
- Resolved an issue where clicking on “View results” in the Operations Monitor would change the navigator pane to show the “Results” window.
- Resolved an issue where connecting to an ESXi Hypervisor with duplicate VMs would cause an SQL exception error in Shavlik Protect when opening the console.
- Resolved an issue where, after upgrading an endpoint to Windows 10, a deployment would fail due to part of the Task Scheduler folder structure being removed if the folders were empty.
- Resolved an issue where deployment child processes timed out after 30 minutes.
- Added support for customers in disconnected environments, allowing them to export to a CSV file the list of patches that need to be downloaded. The CSV file can be moved to an internet-connected machine and the patches can be downloaded from that machine.
- Added the ability to change an agent policy without sending a check-in request to listening agents.
- Resolved an issue where a Protect manifest update that is missing a data delta in the hierarchy could cause an exception in a distribution server synchronization.
- Resolved an issue where the Deployment Notification Report is not sent if a deployment is scheduled rather than set to Deploy Now.

9.2.5046.0 UPDATE 2

Released 2/4/2016Resolved Issues

- Resolved an issue where a German console deploying to an English target would hit an exception when scheduling reboot.
- Resolved an issue where an incomplete agent result would be imported if processed with a batch of complete results.
- Resolved an issue where a vCenter Server that is configured with duplicate Service Content settings keys would cause the Protect UI to crash.
- Resolved an issue where a custom patch with a file defined for detection, but no version number defined in detection logic, would cause the scan to return an error 900.
- Resolved an issue where making a copy of a deployment template with custom actions defined would crash the console.
- Resolved an issue where using the Patch Drive Path feature with a root drive and (no sub folder) would fail to create the deployment sandbox.
- Resolved an issue where deployment to a target with C$ and a C_drive share with read-only permissions would try to copy to C_drive share and fail due to permissions.
- Resolved an issue where generating a report and filtering by a specific patch group would result in a crash.
- Resolved an upgrade issue where a certain combination of upgrade steps would result in a bad SQL query, causing certain reports to fail to generate.

- Resolved an issue where a custom action running an executable could pop up an interactive dialog on systems with “interactive session” enabled.
- Resolved an issue from Protect 9.1 and earlier where a deployment to a system that runs out of disk space gave a generic “failed” error instead of the more descriptive “not enough disk space” message.
- Resolved an issue where Predictive Patch Download would error out if any of the defined downloads do not have a URL.
- Resolved an UI discrepancy that made a deployment appear it would perform a reboot even though the deployment template was set to “no reboot.”

9.2.4988.0 UPDATE 1

Released 11/5/2015Resolved Issues

- Resolved an issue for customers who upgraded from the 9.2 beta to later versions where performing a file refresh would fail.
- Resolved an issue where upgrading from the 9.2 beta to a later version could cause a database error due to duplicate CVE data references.
- Resolved an issue where two scans running simultaneously and using different variations of the Scan Only filter could filter out all machines.
- Resolved an issue where certain environment configurations could cause content deltas to not download, resulting in a crash on startup.
- Resolved an issue where all variations of a selected patch did not download from View > Patches unless it was included in a scan result.
- Resolved an issue where, after upgrading to Protect 9.2, initial data imports failed or timed out.
- Resolved an issue where the intended behavior of patch scan templates that referenced patch groups was not always preserved after upgrading to Protect 9.2.

9.2.4918.0

Released 10/8/2015Major New Features

- Patch Assessment and Deployment Engines
  - The engines used for patch assessment, packaging and execution of updates have been upgraded. The new engines include a number of performance, content and reliability enhancements that enable many of the new features in this release.
- Patch Content
  - The patch assessment and deployment data that Shavlik Protect consumes has been repackaged and improved in many ways.
- Patch Scan Template Filtering
  - More metadata has been added to the patch content. In addition, the Filtering tab on the Patch Scan Template dialog has been updated to allow for more precision when scanning.
- Patch View / Patch Group
  - Patch View has been completely redesigned and updated. It leverages the new content format, enabling you to view patch information in a more concise way. In addition, patch groups are now created and managed from within Patch View. This allows you to research patches and create patch groups in a more unified manner.

- Scheduled Tasks
  - Scheduled tasks on the console now use the Microsoft Task Scheduler. A new dialog, available via the Manage > Scheduled Console Tasks menu, enables you to view and manage these tasks.
- Reports
  - A new End-of-Life by Product report is now available. In addition, a new Schedule Report dialog, available via the Tools > Schedule Report menu, enables you to automatically generate a report at some time in the future.
- Predictive Patch
  - This new option enables Shavlik Protect to automatically download patches that are likely to be deployed in the near future. Downloading patches in advance of their anticipated deployment will help speed the deployment process.

Minor Features and Enhancements

- Patch Tuesday + X (days) Scheduling
  - When scheduling console scans, you now have the ability to delay a recurring scan by a number of days to coincide with a regular event. For example, you might schedule a monthly patch scan to occur the day after Patch Tuesday by using the new Add delay (days) option.
- End of Life Notification
  - Going forward, if the version of Shavlik Protect that you are using is nearing its end of life (EOL) date, a notification will be displayed when you start Shavlik Protect.
- New Prerequisites
  - Windows 10 (Pro or Enterprise Editions) is now supported on client machines
- User Interface Changes
  - Patch View has been completely redesigned.
  - Patch groups are now created and managed from within Patch View.
- In Machine View:
  - The top pane contains three new columns: Virtual Server, VM Name, and Path
  - The Virtual Assets tab has been removed from the middle pane
  - In the bottom pane, the Machines Missing and Machines Installed tabs have been combined into one new tab named Affected Machines.
- On the patch deployment template:
  - Office Install Points and Original Media support has been removed
  - The Backup files for uninstall and Quiet Mode options have been removed; they are now always enabled
  - The Distribution Servers tab has been redesigned to help identify the order in which download sources will be used
- On the patch scan template:
  - The Filtering tab has been completely redesigned
    - User criticality has been removed
    - The Software Distribution tab only shows products that have not been superseded
  - In an agent policy, all tasks are now able to be created without a recurring schedule. This allows you to define tasks that will run only

via the agent user interface or by remote task initiation from the console.
        - In a machine group, the Test Existence and the Test Credentials options have been combined and are implemented by performing a power status scan.
        - In Scan View, the Scan Summary sub-pane is no longer collapsible
        - Scheduled tasks are now separated into two separate dialogs: Manage > Scheduled Remote Tasks and Manage > Scheduled Console Tasks
    - In Tools > Options:
        - Display: Contains a new check box named Show service packs in View > Patches
        - Notifications & Warnings: Contains a new check box named Warn before opening 7 or more bulletins and removed the Warn before scheduling operations when the Default Credentials do not match the current user check box
        - Patch Languages: This tab has been removed.
        - Scans: Contains a new check box named Always enforce machine group exclusions
        - Deployment: Removed the Deployment Tracker address option. The address is now defined using the Console Alias Editor.
        - Logging: Contains a new check box named Diagnostic patch scanning

Deprecated Features

- The following platforms are no longer supported for use on target machines:
    - Windows 2000
    - Windows 2000 Server
    - Windows 2000 Advanced Server
    - Windows 2000 Datacenter Server
    - Windows 2000 Small Business Server
- Virtual asset summaries are no longer available from within Machine View. All virtual asset information is now available using the Virtual Inventory feature.
- Removed the Virtual Machine Hardware Detail, Virtual Machine Memory Usage, and Virtual Machine Disk Usage reports.
- TIF, TXT, and RTF report export formats are no longer supported. Reports can still be exported to PDF, XLS, TSV, CSV, and XML formats.

Features That are Targeted for Removal After Shavlik Protect 9.2

- Threat Management
    - Shavlik is announcing that Protect 9.2 will be the last version to support threat management (antivirus and Active Protection). Users who purchase Shavlik Protect 9.2 on or before December 31, 2015, will have access to the threat management features and will continue to receive updated threat definition files until December 31, 2016. Users who purchase Shavlik Protect 9.2 after December 31, 2015 will not have access to the threat management features.
- Support for Agents on Legacy Windows Platforms
    - Agents will not be supported on Windows XP, Windows Server 2003, or Windows Server 2008 R2 Gold operating systems after December

31, 2016. This is due to a movement in the industry to migrate from the use of SHA-1 certificates to SHA-2 certificates. Shavlik is participating in this movement and by the end of 2016 will begin requiring the use of SHA-2 certificates for communication between Shavlik Protect agents and the Shavlik Protect console. The three operating systems listed above do not support SHA-2 certificates, so when the shift from SHA-1 to SHA-2 becomes permanent, they will no longer be valid agent platforms. Windows XP, Windows Server 2003, and Windows Server 2008 R2 Gold will continue to be supported for agentless scans.

Resolved Issues

- Resolved an issue where selecting multiple distribution server synchronization tasks would not allow ad hoc execution using the “Run Now” option.
- Resolved an export issue in Patch View where export to CSV exported all patches instead of just those that were visible.
- Resolved an issue where downloading patches through Patch View would not prompt with a size alert unless the total size of patches to be downloaded exceeded 1GB.
- Resolved an issue in role-based administration where the AD search could cause a crash if there were invalid characters in the user name.
- Resolved an upgrade issue where a database created in a much earlier version of Shavlik Protect could have a -1 value or missing foreign key relationship, which could cause the upgrade to fail.
- Resolved an issue where Deployment Notification report would not send if one of the systems was an offline VM.
- Resolved an issue were a custom patch would not display in Patch View if it was not properly associated with a bulletin.
- Resolved an issue in custom patch where DWORD value could be saved with an empty string, which would result in a failed assessment due to invalid data.
- Resolved an issue where a scan would fail to schedule if the name of operation was too long.
- Resolved an issue where Machine View patch counts could be off because of a UI duplication issue.
- Resolved a discrepancy in an error message where it called a failure to scan when a machine failed deployment due to an invalid network path.
- Resolved an issue on database setup where if “Has alternate credentials” is checked an invalid authentication option would be available in the dropdown list.
- Resolved an issue where an agent installed on Windows 8.1 N x64 (English-United Kingdom) would pass the wrong LangID resulting in failed patch downloads due to _ENU being appended to the file download.
- Resolved a console hang in Scan View when a large number of systems are selected and the user tries to deselect several devices.
- Resolved a distribution server synchronization issue where the PowerShellModules folder did not inherit permissions, causing the synchronization to fail with an access denied error.
- Resolved an issue in Threat View where some threat scans did not display information when selected.
- Resolved an issue in OU resolution where a domain server name would not prepend if DC= is lower or mixed case.
- Resolved an issue where machine exclusions were not being honored if using OU and nested groups.

- Resolved a race condition which could result in ad hoc report email to fail due to a “file not found” error.
- Resolved an issue in scheduled reoccurring jobs where a time change on the system would not be taken into account until the next occurrence.
- Resolved an issue where making a change to the Console Alias list would result in the console agent threat engine to stop and not automatically restart.
- Resolved an issue where an agent would fail to check in if a service pack group combo box contained empty spaces.
- Resolved an issue where a VM that contained an IP of 0.0.0.0 or 255.255.255.255 would cause the Shavlik Protect console to crash.
- Resolved an issue where Shavlik Scheduler failed in an IP-only environment because the scheduler install was using NetBIOS name.
- Added additional tracing and allowed Protect Cloud download timeout to be configured.
- Resolved an issue were Product End-of-Life date would not update if content changed.
- Resolved an issue where Detailed Summary report would not send when scanning a nested group.
- Resolved an issue where attempting to add VMware ESXi hypervisors with the same host name, but different object references, would fail due to “An item with the same key has already been added”.
- Resolved an issue where agent results from data rollup would not show up in Executive Summary report.
- Resolved an issue in Machine Status by Patch Count (IAVA) report where pie graph did not match individual machine counts.
- Resolved a consistency issue in Machine Hardware Detail Report where the View Current Status check box logic was reversed.
- Resolved an issue where Shut Down SQL Server deployment option would not work with named instances of SQL Server.
- Resolved an issue in the Executive Summary report where Machines Not Scanned information was confusing due to duplicates.
- Resolved an issue in the Executive Summary report where the Machine Group and Scan Template Name columns could overlap.
- Resolved an issue in Condensed Patch Listing report where two systems with the same name, but different domains, would consolidate under one machine and a merged view of the patches detected.

PROTECT 9.1

9.1.4511.0

Released 3/31/2015(Note: This build includes fixes from 9.1.4334.0, Protect 9.1 Patch 1, Protect 9.1 Patch 2, and Protect 9.1 Patch 3.)Bug Fixes

- Updated Shavlik Protect report views to support the change in syntax for CVE IDs.
- Resolved an issue that prevented email from being sent if you configured email options at the individual Hosted VM level in a machine group.
- Resolved an issue that prevented agents from being refreshed during check-in if their certificates were within six months of expiration.

- Resolved an issue that prevented the Shavlik Protect console certificate from being renewed if the certificate was within six months of expiration.
- Resolved an issue where a long computer name would not be included in the console certificate when the console is installed.

9.1.4472.0

Released 10/21/2014(Note: This build includes fixes from 9.1.4334.0, Protect 9.1 Patch 1, and Protect 9.1 Patch 2.)Bug Fixes

- Updated content feed to allow for new format change for CVE.
- Resolved an issue where deployment email notifications were not being sent if the Hours until post deployment e-mails are sent option was set to 0 and the deployment fails on any system in the deployment.
- Resolved an issue where ST.ServiceHost.exe.config is not overwritten on upgrade from a previous version if the configuration file was manually modified, resulting in an 'email service is currently unavailable' error.

9.1.4446.0

Released 08/21/2014(Note: This build includes fixes from 9.1.4334.0 and Protect 9.1 Patch 1)Bug Fixes

- Resolved an issue where a scan of an online hosted virtual machine would fail to scan with an error 201 if NetBIOS could not be resolved. Hosted scan flow will now fail over to IP if NetBIOS fails
- Resolved an issue where machine resolution by OU could return no machines due to an error when querying LDAP (System.DirectoryServices.DirectoryServicesCOMException (0x80072030): There is no such object on the server).
- Resolved an issue where scanning by OU would try to resolve by FQDN, but would not fail over to NetBIOS if FQDN failed.
- Resolved a console crash that occurred when opening Tools > Operations > Distribution Servers when the console service has been manually configured as a specific credential instead of Local System.
- Resolved a performance issue where the email service could return an unavailable error due exceeding the default timeout.
- Resolved an error in Event History for ITScript results that exceeded the max field length when displaying results.
- Resolved an issue where a scan result would not delete due to a constraint on an impartial deployment status that could not be deleted.
- Resolved an issue in Patch Status Detail report where machine counts could be incorrectly calculated.
- Resolved a performance issue where machine resolution could take significantly longer due to machines being resolved more than once instead of being identified as a duplicate and skipped.
- Resolved an issue where STSchedEx would attempt to listen on an additional legacy port that is no longer being used. Will only attempt to open 5120 (default) and not open 5120 and 5121.
- Resolved an issue where, after changing from the local console language to another language, you may not be able to switch back to the native console language.

- Resolved an issue where a null credential associated with a hypervisor causes the Protect UI to crash when refreshing the hypervisor.
- Resolved an issue where scanning a machine with the remote registry disabled would receive an error 270 instead of error 501.
- Resolved an issue where deleting scans on a system with low resources fails, resulting in the rollback transaction being called twice.
- Resolved an issue where installing PowerCLI 5.5 Release 2 causes a crash when enumerating a hypervisor or vCenter server due to a change in an interface in VIM.
- Resolved an issue where deployment would not display the proper error message when the target machine did not have enough disk space.
- Resolved an issue where the console could crash due to too many SQL transactions occurring, resulting in "SQL unavailable" or "Maximum pooled connects to SQL Server exceeded" errors.
- Resolved an issue where refresh files would not download HF7b.xml and PD5.xml due to timeout on slow connections.

9.1.4334.0

Released 4/17/2014Major New Features

- Localized Console Experience
  - Shavlik Protect is now localized for the following languages: Chinese (Standard), Chinese (Traditional), French, German, Italian, Japanese, Korean, Portuguese (Brazil), Russian, and Spanish.
- Localized SafeReboot
  - The SafeReboot dialog has been localized to support the same language set as above. The language of the client machine's operating system will determine which language is displayed. The SafeReboot dialog will default to English if the operating system language is not supported.
- Online Help
  - Localized versions of the Help system are now available on the Web. The help text will be localized according to the language specified on the Display Options dialog. An Internet connection is required in order to access localized help text from the console. For environments that do not have direct Internet access, an English-only version of the Help system is still shipped with the product and is available locally on the console.
- IPv6 Support
  - Shavlik Protect now supports IPv6. IPv4 is still the preferred IP scheme that will be displayed in the UI, so for environments that happen to have IPv6 turned on but are not utilizing it yet, the IPv4 address will be the default address shown for machines.
- Report Views
  - In conjunction with this release, Shavlik is providing a Report Views Guide that describes how to use database views within SQL Server database queries to generate custom reports for Shavlik Protect. This also allows for third-party tools such as SQL Reporting Services, Crystal Reports, Splunk, and others to be used to create reports for Shavlik Protect.

Minor New Features and Enhancements

- Improved Machine Resolution in FQDN and IP-only Environments
    - For customers who have environments that require FQDN or IP to resolve machines, Shavlik has made significant improvements to our machine resolver so that Shavlik Protect will retain multiple resolution methods for each machine. FQDN, Hostname, and IP can all be attempted to ensure the machine is resolved correctly.
- Scan by Vendor Severity
    - The patch scan templates and the assessment engine have been updated to include filters that enable you to scan by vendor severity. You can now scan specifically for Critical, Important, Moderate, Low, or Unassigned security or non-security patches.
- Deployment Workflow Enhancements
    - The deployment workflow has been consolidated to reduce the many branches that existed in the deployment experience. When you perform a deployment now you will see the same level of detail as a scheduled deployment. The deployment results are also available for viewing after the deployment is complete.
- Machine-Level Status in Operations Monitor and in Deployment Tracker
    - A machine-level status has been added to the deployment flows. This gives you better visibility into the current state of your deployments.
- Deployment Return Codes
    - Deployment return codes are now available within Deployment Tracker and within the deployment reports. Making the return codes available within the Shavlik Protect UI eliminates the need to comb through target machine logs for the return codes.
- Active Directory (AD) Enhancements
    - Shavlik Protect is now able to discover any Active Directory Forests and Domains that are broadcasting themselves to the console machine's domain. In addition, you can now add additional Forests and Domains and save credentials for these items. This allows you to browse these items without having to reconnect each time.

Deprecated Features**Features That Have Been Removed in Shavlik Protect 9.1**

- The following platforms are no longer supported for use as a console:
    - Windows XP
    - Windows Server 2003
    - Windows Vista
    - Windows Server 2008 (prior to R2)
    - Windows 8 (Windows 8.1 is supported)
    - 32-bit architecture operating systems

In response to Microsoft's strategic direction and recent end-of-life announcements, Shavlik has removed support for the above platforms as a Shavlik Protect console. Shavlik Protect 9.0 is the last version to support these platforms as a Protect console. All of these platforms are still supported as agentless and agent-based targets.To help ease the migration to newer platforms, Shavlik has developed a migration tool that will help administrators to transition a console from one machine to another. Microsoft has announced an end-of-life for Windows XP in April 2014 and for Windows Server 2003 in April 2016. We are recommending that customers on these platforms migrate to newer operating systems as soon as possible. Shavlik will not be supporting Windows 8 as a console

due to an incompatibility issue with Powershell 4.0, which is a new prerequisite in Protect 9.1. Windows 8.1 support is being added with Protect 9.1.

- The following VMware ESX Hypervisors are no longer supported:
  - ESX 4.0
  - ESX 4.1 (ESXi 4.1 Hypervisors are still supported)

Shavlik is removing support for hypervisor patching and offline VM, template, and snapshot features for these versions, as VMware is ending support for these platforms in 2014. Shavlik Protect 9.0 is the last version to support these versions.

- Export to TIF, TXT, and RTF formats

Shavlik has removed support for these formats as they are little used and provide little value to the majority of customers. Future versions of Shavlik Protect will still support export to PDF, XLS, TSV, CSV, and XML formats.**Features That are Targeted for Removal After Shavlik Protect 9.1**

- Windows Server 2000 support for agentless scan and remediation will be removed after 9.1

Shavlik is announcing that Protect 9.1 will be the last version to support Windows Server 2000 as an agentless target. Protect 9.1 will support this version of Windows until it reaches its end-of-life, which has not yet been announced.

- SQL Server 2005 support will be removed after Protect 9.1

Shavlik is announcing that Protect 9.1 will be the last version to support SQL Server 2005 (all editions). Customers should work towards moving to newer editions of SQL Server as soon as possible.

- User Criticality Filter will be removed after Protect 9.1

With the introduction of the Vendor Severity filter, the User Criticality Filter's primary function is now obsolete and will be removed in a later release. The feature has a high maintenance cost and low value for most customers.Bug Fixes

- Resolved an issue where duplicate agent results could conflict, causing import to fail.
- Resolved an issue where duplicate agent results cause a loop on import, blocking up the import queue.
- Resolved an issue where custom patch could allow a .bat file to be used which would cause agents to fail deployment. The .bat extension has been pulled from the custom patch file options.
- Resolved an issue where LDAP over SSL connections would attempt to use the Shavlik Certificate. The Shavlik Certificate on upgrade will be moved into a custom store.
- Resolved an issue where the 'Is Policy Current' value for Threat Protection Agents could incorrectly show as No when they really are up to date.
- Updated the Help System to include descriptions for agent icons that were not documented.
- Updated the Help System with an outbound port 443 requirement for the Protect Cloud Sync feature.

- Resolved an issue where a result could not be imported if the service pack of the product could not be determined.
- Resolved an issue where attempts to delete a partial scan result could result in a console crash.
- Resolved an issue where an agent result missing the EndTime attribute would fail to import.
- Resolved an issue where the Patch Status Detail Report could end up with PatchBulletinTitle on multiple lines due to a carriage return.
- Updated the community link for data conversion errors on upgrade to point to the proper community article.
- Resolved an issue where the Executive Summary Report could reflect the Effectively Installed Patches count incorrectly.
- Resolved an issue where scan results could fail to import do to a 'Arithmetic overflow error' on the primary key in the ScanItems table.
- Updated the Administration Guide to place the 'What's New?' section in the correct location in the document.
- Resolved an issue where using the Microsoft Scheduler could cause scans to add five minutes to the specified scheduled time.
- Resolved an upgrade issue where an unassociated event subscription could cause the database upgrade to fail from 8.0.2 to 9.0.1182.
- Resolved an import issue where Agent Deployment Results could cause the importer to loop backing up the import queue.
- Resolved an issue where the console could crash when you start many scans simultaneously on a resource constrained machine.
- Changed from using MD5 hash to SHA1 in asset value normalization to be compliant on a FIPS enabled machine.
- Resolved an issue where HFCLI.exe was not using the Protect License Key, causing certain licensed features of HFCLI to not work.
- Resolved an issue where using the Browse Active Directory feature would not allow you to select a forest.
- Resolved an issue where the console service could crash on foreign key exceptions.
- Resolved an issue where the console service could crash when encountering an unknown service pack item type.
- Resolved an issue where 2003 R2 SP2 systems could reboot unexpectedly when upgrading the agent from 8.0.2 to 9.0.1106.
- Resolved an issue where an unnecessary horizontal scroll bar would appear in the Machine View.
- Resolved an issue where the console service could crash when it is unable to decrypt credentials.

PROTECT 9.0

9.0.1316.0

Released 3/31/2015(Note: This build includes fixes from 9.0.1106.0, Protect 9.0 Patch 1, Protect 9.0 Patch 2, and Protect 9.0 Patch 3.)Bug Fixes

- Resolved an issue that prevented the Shavlik Protect console certificate from being renewed if the certificate was within six months of expiration.

- Resolved an issue that prevented agents from being refreshed during check-in if their certificates were within six months of expiration.

9.0.1304.0

Released 12/8/2014(Note: This build includes fixes from 9.0.1106.0, Protect 9.0 Patch 1, and Protect 9.0 Patch 2)Bug Fixes

- Updated the database schema and the content importer to support upcoming changes in the CVE-ID syntax. Prior to this patch, CVE-ID numbers using the new syntax would have prevented content from being updated and may have resulted in a console crash.

9.0.1182.0

Released 6/25/2013(Note: This build includes fixes from 9.0.1106.0 and Protect 9.0 Patch 1)New Features

- Manual activation of Shavlik Protect is now available through a self-help portal. When you choose manual activation mode, instructions are provided to walk you through the process.

Bug Fixes

- Resolved an issue where bad agent results were continuously imported rather than being discarded, resulting in the ST.ConsoleService.managed.log showing multiple “Stream header magic number is invalid” errors.
- Resolved an issue where multiple IP ranges that use the same distribution servers cause full cloud policy updates to fail with 400 (bad request).
- Resolved an issue where the advanced filter options for the Deployment Status By Machine report could cause Protect to crash.
- Resolved an issue where reports emailed from Tools > Create Report are a tmp file instead of PDF.
- Updated the Administration Guide to correct an issue where the default console service port was shown as 3131 instead of 3121.
- Resolved an issue where the machine inventory email does not get sent when applied to a machine group.
- Resolved an issue where agent registration and checkin uses FQDN not NetBIOS, causing the install to fail if FQDN could not be resolved.
- Resolved an issue where agent checkin without a policy uses FQDN not NetBIOS, causing the install to fail if FQDN could not be resolved.
- Resolved an issue where emailing a report from Scan View could cause Protect to crash.
- Resolved an issue where the Scan and Report Only and the Deploy and Report Only roles do not allow the user to create and assign their own credentials.
- Resolved an issue where the Scheduled Tasks Manager abnormally exits when right-clicking in the jobs window.
- Resolved an issue where scheduled jobs might not appear in the Scheduled Tasks Manager.
- Resolved an upgrade issue from 8.0.2 to 9.0.1106 where, after upgrade, some machine groups could not be opened.

- Resolved an issue on ProtectCloud login where using dangerous HTML characters in the Protect Cloud password causes an exception.
- Resolved an issue where scheduled deployments to a hosted VM shows a scheduled time discrepancy between Deployment Tracker and the Scheduled Tasks Manager.

9.0.1106.0

Released 5/2/2013Major New Features

- Support for Cloud Agents
  - Shavlik Protect agents can be installed from the cloud and can function without ever connecting directly to the Shavlik Protect console
  - Agent policies are uploaded from the console to the cloud where they are available to be downloaded by the agents
  - Agent results are uploaded to the cloud and then downloaded to the Shavlik Protect console
- Virtual Inventory (ESXi Hypervisor Patching)This new feature is used to manage and track the vCenter Servers and the ESXi hypervisors that are used in your organization. You can use the Virtual Inventory feature to:
  - Add vCenter Servers and ESXi hypervisors to Shavlik Protect
  - View basic configuration information about the vCenter Servers and the ESXi hypervisors
  - Perform a scan of the managed and unmanaged ESXi hypervisors
  - View the security bulletins that have already been installed on the managed and unmanaged ESXi hypervisors
  - View the security bulletins that are missing on the managed and unmanaged ESXi hypervisors
  - Deploy any missing security bulletins to the ESXi hypervisors
  - Power on and off the virtual machines that reside on your managed and unmanaged ESXi hypervisors
  - Add the virtual machines and virtual machine templates to a new or existing machine group
- Installation and Prerequisite Changes
  - Support for 64-bit operating systems
  - New web version of the installation program that detects which architecture is supported by the console's operating system and will automatically download the correct 32-bit or 64-bit MSI file
  - Support for SQL Server 2012
  - Support for Windows 8 and Windows Server 2012
- Event History Event History provides a way to view the background operational events that occur with Shavlik Protect. Entries are generated for a large number of events, including:
  - Database maintenance
  - Distribution server synchronization
  - Scheduler events
  - Core engines/definitions downloads
  - Core engines/definitions synchronization
  - Threat data downloads
  - Threat data synchronization
  - Operation result imports (patch scans, threat scans, etc.)
  - ESXi Hypervisor patch deployments
  - Agent policy synchronization using Protect Cloud

Minor Features and Enhancements

- Patch Management Enhancements
  - Patch replacement resolution has been added to patch groups
  - Agentless target machines that download patches from distribution servers will now install the patches they download even if they cannot download all patches in the deployment
- Threat Management Enhancements
  - Quarantined items can be added as filename-based exceptions from the quarantine management UI
  - Detected threats can be added to the Allowed Threats list of select policies from the Threat Events View
- PowerShell Scripts
  - PowerShell scripts can now target ESXi hypervisors and use PowerCli commands
  - PowerShell modules are now supported
- Performance Improvements
  - Reports have been reworked and are significantly faster and more accurate
  - Rollup and import performance are improved by exporting and importing batches of results
  - Performance improvements have been made in the Policy Editor
  - Stronger cryptographic keys are now used to make the program more secure
  - Multi-console support has been improved
  - Scheduling of distribution server synchronization can now be done on a per-distribution server basis
- User Interface Changes
  - The Navigation pane has been modified to better utilize the available space
  - The menu bar is simplified and has only six items: Home, New, View, Manage, Tools, and Help
  - Product End-of-life (EOL) information has been added to the data and is displayed in several places in the interface
  - Notes can be associated with individual machines in machine groups
  - Machine names and IP addresses can now be edited
  - The Active Directory browser has been improved
  - Credentials Manager now shows where specific credentials are used
  - The About dialog clearly displays current and installed data file versions
  - The Agent Manager has been removed. All functionality is available from within Machine View.
  - Reworked the Active Directory / OU browser
  - Searching within the current view is simplified. You no longer need to select the column to search; all columns are searched.
  - Patch Type has been added to the middle section of Machine View and Scan View patch results
  - Manage Items now appears as a dialog rather than being displayed in the main window. This reduces memory usage and provides better performance.
  - Scheduled operations that were previously configured in Tools > Options have been moved to a new area under Tools > Operations

        - Management of distribution servers has been moved to Tools > Operations
        - An Error code column has been added to a number of grids and the error code has been removed from the error message
        - A Patch Breakdown column has been added to a number of grids. This provides a visual representation of the percentage of installed patches (green) vs. missing patches (red) and missing service packs (yellow).
    - IAVA Reporter

      If you purchase the Government Edition of Shavlik Protect you will receive a license key that enables you to use the Information Assurance Vulnerability Alert (IAVA) Reporter. The IAVA-specific files are automatically installed when Shavlik Protect is installed and are completely integrated in Shavlik Protect.

Bug fixes

- Resolved an issue in role based administration where Scan/Deploy & Report Only users had more access than expected.
- Resolved an issue where after upgrade from 7.8 to 8.0 scanning offline hosted VM and offline VMWare .vmx file would fail.
- Resolved an issue in the Machine Group Editor treelist where the background color should be all white.
- Resolved an issue in the Scan Summary box in scan view where it does not remember collapsed state (minimized state).
- Resolved an issue in the Deployment tracker where collapsed rows expand during auto refresh.
- Resolved an issue in documentation to show that we support SQL 2008 SP3.
- Resolved an issue in the Deployment Notification email shows incorrect date and should specify GMT.
- Resolved an issue where splitter bars in the Scan Summary do not remember their position when the application is closed.
- Resolved an issue in Machine View where column sorts only on the first column.
- Resolved an issue in Custom Patch Deployment when using bat file where the deployment fails to complete.
- Resolved an issue where the file size confirmation dialog for downloading patches does not display during a single patch deployment.
- Resolved an issue where right click context menus under machines not scanned tab were removed.
- Resolved an issue in the custom patch regkey editor where you cannot change from DWORD to String and put in a string value without getting an error.
- Resolved an issue where file and registry key details in the Patch Information view don't scale.
- Removed 'query remote log information' from deployment results screen due to compatibility issues across different operating systems.
- Resolved an issue in machine groups where 'Scan Only IIS Servers' filters out all machine with IIS installed on it instead of including only IIS servers.
- Resolved a race condition where you could click on a machine group multiple times opening many windows if you are on a slow system.
- Resolved an issue where removing all email recipients from a machine does not remove the email.

- Resolved an issue where RDP fails to install on German 2K3E R2.
- Updated documentation to reflect what OS languages Shavlik Protect supports for system requirements.
- Resolved an issue where the manual RDP installation link is missing from the manual installation section of the install guide.
- Resolved an issue where Agents with pre-deploy reboot, do not wait for the reboot to start installing patches.
- Resolved an issue where consoles configured for data rollup display warning messages incorrectly due to differences in time between consoles.
- Resolved an issue on upgrade from 7.8 to 8.0 where you receive error 1714. The older version of Shavlik Protect Patch Engine cannot be removed. Contact your technical support group. System Error 1612.
- Resolved an issue where the %Pathtofixes% variable is not honored when installing scheduler from scheduled task manager.
- Resolved an issue on the chart screen if you select options always show this chart, the options at the bottom of the page are disabled until you do a refresh.
- Resolved a potential crash during deployment when deploying to large groups.
- Resolved an issue in the Deployment Notification email where "Scheduled Installation Time" would show as blank.
- Resolved an issue where the Shavlik Protect Console could crash when filtering in scan results.
- Resolved an issue when changing the scheduler port where the task scheduler honors the new value, but the Shavlik Protect GUI does not.
- Resolved an issue in the Scan Summary --> Patch Information section where "File version is less than expected: ..." is truncated.
- Resolved an issue where agent deployments using pre-deployment reboots could end up in a continuous reboot cycle if there are still missing patches.
- Resolved an issue where closing Shavlik Protect with an RDP window open and the RDP window no longer honors the cancel action.
- Resolved an issue where STAgent service could hang during start-up on XP and 2k3.
- Resolved an issue where Active Protection prevents opening embedded Outlook files (.msg) in a word document.
- Resolved a database upgrade issue where an ALTER TABLE statement conflicted with the FOREIGN KEY constraint "FK_LinkEmailRecScanTemplate_ScanTemplates".
- Resolved an issue in STSchedex.exe where shutdown could cause an application error.
- Resolved an issue with in asset scans that could cause software asset scans to fail importing due to an invalid URI error.
- Resolved an issue in Data Rollup where IP Address or hostname containing a space will cause the console service to error and prevent start-up.
- Resolved an issue where there could be discrepancies interpreting scan result between agent GUI and console GUI.
- Updated the description of Non-Security Patches in new scan template to reduce confusion.
- Resolved an issue where items are unable to deleted from Manage > Items due to overlapping scans results.
- Resolved an issue where offline activation for vCP with Configuration Management, configure product activation fails with "Offline activation stream is invalid".
- Resolved an issue where copying a machine group could cause the app to crash.
- Resolved an issue with activating multiple license key issues with console add-on keys.
- Resolved an issue where Daily AP Alert is still triggered even though threat protection feature is no longer licensed.

- Resolved an issue with the Condensed Patch Listing report where information appears in exported CSV that is not part of the report.
- Resolved an issue when deploying SQL Server 2000 patches could crash the console with System.ArgumentOutOfRangeException: Positive number required. Parameter name: culture.
- Resolved an issue where manually installing an agent using a lowercase passphrase could cause an "Invalid request" during registration.
- Updated command line help to provide an example on how to register an agent using STAgentManagement.exe.
- Resolved an issue in STThreat.exe where it could locking up a system when RunDetection: detection function 5094 crashed error occurs.

PROTECT 8.0

8.0.2.4027

Released 11/01/2012Bug Fixes

- Added support for the vCenter Protect installer to detect PowerShell 3 as a prerequisite for PowerShell.
- Resolved an issue where Java Runtime would uninstall the current version and then fail to install due to file(s) in use.
- Removed a dependency on two Microsoft components (oHotFix and Qchain) as they are reaching end of availability from Microsoft Corporation.
- Resolved an issue where an offline virtual machine on an ESXi Hypervisor would fail to scan with an Error 4000.
- Resolved an issue where deployments using Install at next reboot could execute immediately.
- Added installation support for Windows 8 and Windows Server 2012.
- Added support for installations using SQL Server 2012 databases.

8.0.3965.1

Released 9/10/2012New Features

- Integration with VMware Licensing
  - Support for multiple license keys, allowing for valid VMware vSphere and Accelerator Kit bundle licenses to activate along with VMware vCenter Protect licenses.
  - Retain support for the legacy (Shavlik) license keys and make key combinations additive.
  - Update to license services within VMware vCenter Protect, allowing active licenses to refresh without user intervention. Customers no longer have to manually refresh their active licenses when Support or data renewals occur, etc.

- Updated Product Activation
  - VMware vCenter Protect now has the ability to activate a trial within the product.
  - VMware vCenter Protect Free version is now activated through the same activation dialog as Trial or Product\Bundle keys.
- Renaming of the Product
  - VMware vCenter Protect Essentials is renamed to VMware vCenter Protect Standard
  - VMware vCenter Protect Essentials Plus is renamed to VMware vCenter Protect Advanced

Bug Fixes

- Resolved a rendering issue in the Patch View where you could select one of the affected patches and the Patch Details would not display correctly resulting in an application crash.

8.0.3787.0

Released 12/28/2011(NOTE: This build includes fixes from 8.0.3756.0 and Protect 8.0 Patch 1)Bug Fixes

- Enhanced ITScripts engine to provide more user-friendly error messages.
- Resolved an issue where scheduled value in Tracker and deployment status was showing date and time the job was scheduled on, and not the date and time the job would execute.
- Resolved an issue in the STAgent.exe where a race condition could cause a crash.
- Resolved an issue in the IAVA reporter where Patch Status Detail would crash if viewed by specific product and service pack combinations.
- Resolved an issue in the Help file where a link for ITScripts would redirect to custom patch instead.
- Resolved an issue where refreshing a license after viewing a power status scan result could result in a crash.
- Resolved an issue where Browse Active Directory feature in Machine Groups did not list child OUs.
- Updated Help file to correct steps for creating a manual install script for agent installation.
- Resolved an issue where upgrade from 7.x to 8.x results in agents running threat protection needing to be re-installed.
- Resolved an issue where STAgentUpdater could crash when creating SSL registration.
- Resolved an issue where the service could crash when retrieving system credentials due to size of credential store.
- Resolved a regression where the patch pane in Machine View defaulted to expanded instead of collapsed.
- Resolved an issue in Custom Patch where a string registry value always returned missing.
- Resolved an issue where database upgrade fails with uniqueness constraint violation. This only affects 7.x upgrade to 8.0.
- Resolved an issue where agents would be unable to deploy a custom patch.

8.0.3756.0

Released 11/1/2011Major New Features

- ITScripts
  - Powerful scripting capabilities just clicks away
  - Catalog of scripts including maintenance scripts, application and OS-level configuration, configuration of GPOs, monitoring and informational scripts, and more
  - Ability to import custom scripts and take advantage of the ITScript engine features to make machine discovery and credentials usage a breeze
- Credentials Manager
  - Addition of the Credentials Manager to centralize the creation and maintenance of credentials
  - User-friendly UI to allow access to your credentials anywhere in the product and specify credentials in a matter of clicks without the need to retype username and password
- Power Status Scan
  - Addition of a new scan type that allows extremely fast discovery of the power status of your machines. Discover hundreds of machines in minutes across a broad IP range or validate the power status of your machines using host name, domain, or any of the other methods available in the machine group.
  - Right-click power status scan option from Machine View for validating that a machine is online
  - Power Status Scan result located in the Results section of the Navigation Bar for historical reference to Power Status Scan results
  - Power Status Report for proof of compliance and to provide the validation that is often required by energy providers for power rebates
- Multiple Administator Support in Console
  - Support for multiple unique administrators to access the same Protect console simultaneously
  - Notification if the same account is attempting to open the console simultaneously

Minor Features and Enhancements

- Patch Scan Performance Enhancements
  - Increased scan speed
  - Reduced memory footprint
- New Operations Home Page
  - Quicker access to common operations like patch and asset scans, power status scan, ITScript runs, etc.
- Integration with Remote Desktop Protocol (RDP)
  - Initiate from Machine View against a target machine
  - Utilize existing credentials
  - Connect via hostname or IP
  - Option to connect as admin session for specific maintenance tasks that require session 0
- Integrated Deployment into Operations Monitor for Better Deployment Progress Monitoring
  - Increased visibility during deployment

        - Better progress tracking of deployments while being staged
        - Easy access to deployment results and Tracker results
    - Antivirus/Threat Protection Enhancements
        - Threat protection is now registered in Microsoft Security Center / Action Center
        - Enhanced control over the “disable” and “temporarily suspend” Active Protection features within the agent policy

Bug Fixes

- Resolved an issue the Agent could be unable to deploy a deployable SP.
- Resolved an issue where Office patches with client and full patch types download only the first patch type listed in pd5.
- Resolved an issue where the selecting Patch Download Status would not download a patch if you downloaded, deleted, then attempted to download again.
- Resolved an issue where Patch Download Status does not sort after the first time.
- Resolved an issue attempting to add a Service Pack to a patch group would result in a blank patch group.
- Resolved an issue in documentation: a mapped drive for a Download Center Path is not supported.
- Resolved an issue where agents would fail to deploy other Service Packs and Patches if errors were encountered on a Service Pack install.
- Resolved an issue where upgrading a database from 7.6 to 7.8 fails with id cannot be null.
- Resolved an issue in documentation: SQL 2008 Express and SQL 2008 R2 were not listed in the database pre-reqs.
- Resolved an issue where machine summation counts may not be accurate in Machine View.
- Resolved an issue where deleting a hosted virtual machine produces collation conflicts
- Resolved an issue where attempting to non-deploy a service pack results in Protect crash
- Resolved an issue where Patch summary report advanced filter does not properly filter by bulletin or Qnumber.
- Resolved an issue where scheduled deployments with pre install reboot run the deployment after any reboot, not the scheduled reboot.
- Resolved an issue where scheduled deployment with pre install reboot would not execute if system clock resets to a time prior to scheduling.
- Resolved an issue where the schedule dialog could change from PM to AM under certain circumstances.
- Resolved an issue where threat manifest cannot be downloaded from an http distribution server when vendor as backup is disabled.
- Resolved an issue where scan my domain does not work correctly with similar qualified domains.
- Resolved an issue where find users in the machine group domain browser would find the user by simple domain name.
- Resolved an issue where copy machine group created by a different logged in user with an ESX server setup in hosted virtual machine causes a crash.
- Resolved an issue with Protect 7.8 where Safereboot does not reboot on Windows 2000
- Resolved an issue where Agent downloads fail due to file not found error
- Resolved an issue where Deleting the last patch scan for a machine doesn't null out the patch-specific machine measures

- Resolved an issue where At least one window within Protect causes an indefinite freeze for the entire application when a WM_SETTINGSCHANGE message is received
- Resolved an issue in Custom Patch where there would be two validation checks for each XML
- Resolved an issue in the threat engine where Ultra VNC and Remote Task Service are killed during agent Full threat scan
- Resolved an issue where Report only users are able to do more than specified
- Resolved an issue where Operations Monitor does not sort correctly by numerical order.
- Resolved an issue where a license due to expire in one day could not be activated properly.
- Resolved an issue where distribution server sync space required is multiplied by 5.
- Resolved an issue where an Error in STCore::IO::CPath::GetFullPath() causes deployment of office patches with install point to fail
- Resolved an issue where Dutch Windows 7 SP1 is not detected correctly by the prereq installer
- Resolved an issue where Software Distribution checkbox is able to be modified for Security Patch Scan Template
- Resolved an issue where Agent System Requirement documentation incorrect
- Resolved an issue where customer encountered error running machine software detail report.
- Resolved an issue where recurring jobs are deleted when they fail if credentials were invalid.
- Resolved an issue where Scheduled Task Manager could cause Window's user accounts to be locked out
- Resolved an issue which resulted in Duplicate Service Packs in the Patches Table
- Resolved an issue in documentation stating multiple consoles sharing the same DB on Domain Controllers with the same SID is not supported.
- Resolved an issue where Copy of Asset template does not store the name in the correct table
- Resolved an issue Upgrading protect overwrites st.servicehost.exe.config where we must store proxy information so the service can access the internet
- Resolved an issue when Console culture is not supported by our patch data languages, the application will crash during deployment when download is about complete.
- Resolved an issue where Running Executive summary report from a scan results has **multiple** in the machine group field.
- Resolved an issue where agents could not be deployed as a Custom Patch
- Resolved an issue where protect would crash when a required file was not in the manifest.
- Resolved an issue where Protect crashes when user attempts to open an existing template after upgrade from 7.6 to 7.8.
- Resolved an issue where an invalid distribution server credential gets an agent in an infinite check-in loop.
- Resolved an issue where Patch scan path information not being fully painted
- Resolved an issue in Power State Template where Shut Down when “Alert user, perform action when user logs off” is checked results in a reboot.
- Resolved an issue in the Deployment Detail report when using Domain as an advanced filter results in an error invalid field smachDomainName.
- Resolved an issue where Agent check-in failed due to IP Range for Primary Distribution Server being Blank.
- Resolved an issue when trying to do multiple deployments at once crashes Deployment Tracker due to a dead lock.

- Resolved an issue where deployments would reboot targets, but no patches were being deployed.
- Resolved an issue where Agent patch deployment fails when the temp dir is not on the c drive
- Resolved an issue where the Service Pack release date shows as 01/01/0001 due to UTC + 1 or higher being set.
- Resolved an issue in documentation to state the Workstation Service is required by the VMware vCenter Protect Agent
- Resolved an issue where export to CSV from machine view from Hardware Assets tab crashes the application.
- Resolved an issue where a distribution server could have an agent framework and engine mismatch.
- Resolved an issue where large numbers of agent policies cause the distribution server confirmation screen to be cut off.
- Resolved an issue where scheduled jobs that encounter an error while running are deleted and do not show up in the log or the scheduler.