Shavlik Protect 9.2 Standard/Advanced Release Notes

Overview

These release notes support the current GA version of Shavlik Protect 9.2. The GA Release can be downloaded from this link: http://www.shavlik.com/downloads.

The GA build is 9.2.4988.0.

You can upgrade to Shavlik Protect 9.2 from either Shavlik Protect 9.0 or Shavlik Protect 9.1.

IMPORTANT! Shavlik recommends you create a backup of your current database before performing any upgrades. If you are using a full edition of SQL Server you should use the SQL Server Maintenance Plan Wizard to perform the backup. SQL Server Express users who do not have access to the SQL Server Maintenance Plan Wizard can use the Shavlik Protect Database Maintenance tool.

If you have any questions, please contact our Technical Support Team at http://support.shavlik.com/CaseLogging.aspx or call toll free 1-866-407-5279.

Documentation

http://www.shavlik.com/support/online-documentation/protect

System Requirements

Console

Restrictions:

- An NTFS file system is required on the console machine
- If you install the console on a domain controller that uses LDAP certificate authentication, you may need to configure the server to avoid conflict issues between the SSL certificate and the Shavlik Protect program certificate. There is no easy way to configure this on a Windows Server 2003-based domain controller and this combination is not recommended for use as a console.
- If you install the console on two or more machines that share a database, all of the console machines must have unique security identifiers (SIDs) in order to prevent user credential problems. Machines are likely to have the same SIDs if you make a copy of a virtual machine or if you ghost a machine.

Processor:

- Minimum: 2 processor cores 2 GHz or faster
- Recommended: 4 processor cores 2 GHz or faster (for 250 – 1000 seat license)
- High performance: 8 processor cores 2 GHz or faster (for 1000+ seat license)

Memory:

- Minimum: 2 GB of RAM
- Recommended: 4 GB of RAM (for 250 – 1000 seat license)
- High performance: 8 GB of RAM (for 1000+ seat license)

Video:

- 1024 x 768 screen resolution or higher (1280 x 1024 recommended)

Disk Space:

- 100 MB for application
- 2 GB minimum, 10 GB or more recommended for patch repository

Operating System (one of the following):

Note: Shavlik Protect supports 64-bit versions of the listed operating systems. 32-bit versions are not supported for the console.

- Windows Server 2012 Family R2, excluding Server Core
- Windows Server 2012 Family, excluding Server Core
- Windows Server 2008 Family R2 SP1 or later, excluding Server Core
- Windows 8.1 or later, excluding Windows RT
- Windows 7 SP1 or later, Professional, Enterprise, or Ultimate Edition

Database:

- Use of a Microsoft SQL Server database [SQL Server 2005 (Full or Express Edition) or later]. If you do not have access to a SQL Server database, the option to install SQL Server 2014 Express Edition will be provided during the prerequisite software installation process.
- Size: 1.5 GB

Prerequisite Software:

- Use of Microsoft SQL Server 2005 (Full or Express Edition) or later
- Microsoft .NET Framework 4.5.1 or later
- Windows Management Framework 4.0 (contains Windows PowerShell 4.0, which is required for the ITScripts feature). This prerequisite does not apply to Windows 8.1 and Windows Server 2012 R2 as PowerShell 4.0 is already included with these operating systems.

Windows Account Requirements:

- In order to access the full capabilities of Shavlik Protect, you must run under an account with administrator privileges

Configuration Requirements:

- When performing an asset scan of the console machine, Windows Management Instrumentation (WMI) service must be enabled and the protocol allowed to the machine.

Clients (agentless)

Operating Systems (any of the following):

- Windows XP Professional (can deploy patches to Windows XP Family SP3 or later)
- Windows XP Tablet PC Edition
- Windows XP Embedded
- Windows Server 2003, Enterprise Edition (can deploy patches to Windows Server 2003 Family SP2 or later)
- Windows Server 2003, Standard Edition
- Windows Server 2003, Web Edition
- Windows Server 2003 for Small Business Server
- Windows Server 2003, Datacenter Edition
- Windows Vista, Business Edition
- Windows Vista, Enterprise Edition
- Windows Vista, Ultimate Edition
- Windows 7, Professional Edition
- Windows 7, Enterprise Edition
- Windows 7, Ultimate Edition
- Windows Server 2008, Standard
- Windows Server 2008, Enterprise
- Windows Server 2008, Datacenter
- Windows Server 2008, Standard - Core
- Windows Server 2008, Enterprise - Core
- Windows Server 2008, Datacenter – Core
- Windows Server 2008 R2, Standard
- Windows Server 2008 R2, Enterprise
- Windows Server 2008 R2, Datacenter
- Windows Server 2008 R2, Standard - Core
- Windows Server 2008 R2, Enterprise - Core
- Windows Server 2008 R2, Datacenter – Core

- Windows 8
- Windows 8 Pro
- Windows 8 Enterprise
- Windows 8.1
- Windows 8.1 Enterprise
- Windows Server 2012, Foundation Edition
- Windows Server 2012, Essentials Edition
- Windows Server 2012, Standard Edition
- Windows Server 2012, Datacenter Edition
- Windows Server 2012 R2, Essentials Edition
- Windows Server 2012 R2, Standard Edition
- Windows Server 2012 R2, Datacenter Edition
- Windows 10 Pro
- Windows 10 Enterprise

Virtual Machines (offline virtual images created by any of the following):

- VMware ESXi 5.0 or later (VMware Tools is required on the VMs)
- VMware vCenter (formally VMware VirtualCenter) 5.0 or later (VMware Tools is required on the VMs)
- VMware Workstation 9.0 or later
- VMware Player

Configuration Requirements

- Remote Registry service must be running
- Simple File Sharing must be turned off
- Server service must be running
- NetBIOS (TCP 139) or Direct Host (TCP 445) ports must be accessible
- When deploying patches on Windows Vista or later operating systems, the Windows Update service Startup type must be set to **Manual** or **Automatic**.
- Remote Desktop connections must be allowed in order for the console to make an RDP connection with a target machine
- When performing an asset scan, Windows Management Instrumentation (WMI) service must be enabled and the protocol allowed to the machine (TCP port 135).

Products Supported (for patch program):

- See http://xml.shavlik.com/data/supportedproduct78.htm for the current list

Disk Space (for patch program):

- Free space equal to five times the size of the patches being deployed

Supported Languages (for patch program):

- Arabic, Chinese (Simplified), Chinese (Traditional), Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese (Brazil), Portuguese (Portugal), Russian, Spanish, Swedish, Thai, Turkish

Clients Running Shavlik Protect Agent

Note: An NTFS file system is required on agent machines.

Processor:

- 500 MHz or faster CPU

Memory:

- Minimum: 256 meg RAM
- Recommended: 512 meg RAM or higher

Disk Space:

- 30 MB for Shavlik Protect Agent client
- 500 MB or more for patch repository

Operating Systems (any of the following except home editions):

- Windows XP (64-bit = SP2 or later, 32-bit = SP3 or later)
- Windows Server 2003 Family SP2 or later
- Windows Vista Family
- Windows 7 Family
- Windows Server 2008 Family
- Windows Server 2008 Family R2
- Windows 8 Family, excluding Windows RT
- Windows Server 2012 Family
- Windows Server 2012 Family R2
- Windows 10 Pro and Enterprise

Prerequisite Software

- MSXML 3.0 or later

Configuration Requirements

- Workstation service must be running

Port Requirements

These are the default port requirements. The port numbers are configurable.

	Inbound Ports (Basic NAT Firewall)									
	TCP 80	**TCP 135**	**TCP 137-139 or TCP 445 (Windows file sharing/directory services)**		**TCP 443**	**TCP 3121**	**TCP 3122**	**TCP 4155**	**TCP 5120**	**TCP 5985**
Client System		X (For asset scans)	X	X				X (For listening agents)	X	X (For WinRM protocol)
Console System						X	X			
Distribution Server	X		X	X	X					

	Outbound Ports (Highly Restricted Network Environment)						
	TCP 80	**TCP 137-139 and TCP 445 (Windows file sharing/directory services)**		**TCP 443**	**TCP 3121**	**TCP 5120**	**UDP 9**
Client System	X (For agents)	X	X	X (For cloud agents)	X (For agents and Deployment Tracker)		
Console System	X	X	X	X (For cloud sync)		X	X (For WoL & error reporting)

Major 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. The report can be automatically generated once or on a recurring basis.

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.

Virtual Machine Features

Added the concept of a virtual identity for any machine that is discovered through the **Hosted Virtual Machines** tab of a machine group. The virtual identity is a combination of fields that allows the Shavlik Protect console to locate the VM in your vSphere environment at any time. This provides a seamless virtual feature experience for offline VMs, templates and snapshotting.

Support is also provided for VMware vSphere 6.0. All of Shavlik Protect's virtual inventory, scanning and deployment features can be performed on virtual machines and ESXi hypervisors created by vSphere 6.0.

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 2000 is no longer a supported operating system on client machines
- Windows 10 (Pro or Enterprise Editions) is now supported on client machines

User Interface Changes

The following user interface items have been changed:

- 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

Features That Have Been Removed in Shavlik Protect 9.2

- 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

  In response to Microsoft's strategic direction and recent end-of-life announcements, Shavlik has removed support for the above platforms on target machines.
- 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 formats are no longer supported

  The ability to export a report to these formats has been removed as they are little used and provide little value to the majority of customers. 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.
- 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 during upgrade 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.