

Shavlik GA Release Notes

[Overview](#)

[Documentation](#)

[System Requirements](#)

[Major New Features](#)

[Resolved Issues](#)

Overview

These release notes support the GA version of Shavlik NetChkProtect_7.8

The GA Release can be downloaded from this link:

https://hfnetchk4.shavlik.com/downloads/NetChkProtect_7.8.1392.0.exe

The GA build is 7.8.1392.0

You can upgrade to NetChk Protect_7.8 from NetChk Protect 6.5.3 release or NetChk Protect 7.x releases.

If you are upgrading from older version than NetChk Protect 6.5.3: Please download and install NetChk Protect 6.5.3 [Download Version 6.5.3.818 - 70.9 MB \(.exe\)](#) before installing NetChk Protect 7.8.

REMEMBER: Shavlik recommends you create a backup of your current database using SQL Enterprise Manager before performing any upgrades.

If you are running SQL Express or full SQL but don't have a maintenance or backup plan in place, please read the following:

<http://supportteamblog.shavlik.com/2010/01/13/sql-database-maintenance/>

If you have any questions, please contact our US Technical Support Team at support@shavlik.com or International Technical Support Team at InternationalSE@shavlik.com or call toll free 1-866-407-5279.

Documentation

<http://forum.shavlik.com/viewtopic.php?f=70&t=17052>

System Requirements

Console

Restrictions:

- A FAT file system cannot be used on a 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 NetChk 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.

Processor:

- Minimum: Pentium 4
- Recommended: 2.0 GHz CPU (multi-core machine if more than 1000 seat license)

Memory:

- Minimum: 1 GB of RAM
- Recommended: 2 GB of RAM (4 GB if more than 1000 seat license)

Video:

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

Disk Space:

- 100 MB for application
- 2 GB or more for patch repository

Operating System (one of the following):

Note: NetChk Protect supports 32- and 64-bit versions of the listed operating systems for both console and target systems.

Minimum:

- Windows XP Professional, SP3 or later (SP2 or later if using 64-bit version)
- Windows Vista, SP1 or later, Business, Enterprise, or Ultimate Edition
- Windows 7, Professional, Enterprise, or Ultimate Edition

Recommended:

- Windows Server 2003 Family, SP2 or later
- Windows Server 2008 Family, excluding Server Core
- Windows Server 2008 Family R2, excluding Server Core

Database:

- Use of SQL Server database (SQL Server 2005, SQL Server 2005 Express Edition, SQL Server 2008, or SQL Server 2008 R2 Express Edition) is required. If you do not have access to a SQL Server database, the option to install SQL Server 2008 R2 Express will be provided during the prerequisite software installation process.

Note: SQL Server 2000 is not supported for use as a back-end database.

- Size: 1.5 GB

Prerequisite Software:

- MSXML 6.0 SP2 Hotfix (only required on console machines using Windows Vista SP1 or earlier)
- Windows Installer 4.5 or later (only required if installing SQL Server 2008 R2 Express during NetChk Protect installation)
- Use of Microsoft SQL Server 2005, SQL Server 2005 Express Edition, SQL Server 2008, or SQL Server 2008 R2 Express Edition
- SQL Native Client or SQL 2008 Native Client

- Microsoft .NET Framework 4.0 or later

Windows Account Requirements:

- In order to access the full capabilities of NetChk 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. In Windows Firewall, on Windows XP/Windows 2003 machines the service is called Remote Administration, and on Windows Vista/Windows 7/Windows Server 2008 machines the service is called Windows Management Instrumentation (WMI)/Remote Administration.

Clients (agentless)**Browser:**

- Internet Explorer 5.5 or later required to receive patch deployments

Operating Systems (any of the following):

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server
- Windows 2000 Small Business Server
- Windows XP Professional
- Windows XP Tablet PC Edition
- Windows XP Embedded
- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Standard Edition
- Windows Server 2003, Web Edition
- Windows Server 2003 for Small Business Server
- Windows Server 2003, Datacenter Edition
- Windows Vista, Home Basic Edition
- Windows Vista, Home Premium Edition
- Windows Vista, Business Edition
- Windows Vista, Enterprise Edition
- Windows Vista, Ultimate Edition
- Windows 7, Home Premium 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

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

- VMware ESX Server 3.0 or later
- VMware ESXi 3.0 or later
- VMware vCenter (formally VMware VirtualCenter) 2.0 or later
- VMware Workstation 4.0 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 (tcp139) or Direct Host (tcp445) ports must be accessible
- When deploying patches on Windows Vista or later operating systems, the Windows Update service Startup type must be set to either **Manual** or **Automatic**.
- When performing an asset scan, Windows Management Instrumentation (WMI) service must be enabled and the protocol allowed to the machine (TCP port 135). In Windows Firewall, on Windows XP/Windows 2003 machines the service is called Remote Administration, and on Windows Vista/Windows 7/Windows Server 2008 machines the service is called Windows Management Instrumentation (WMI)/Remote Administration.

Products Supported (for patch program):

- See <http://xml.shavlik.com/data/supportedproducts.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 NetPt Agent

Processor:

- 500 MHz or faster CPU

Memory:

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

Disk Space:

Note: FAT file systems are not supported on agent machines.

- 30 MB for NetPt Agent client
- 500 MB or more for patch repository

Operating Systems (any of the following):

- Windows 2000 SP4 or later (with Windows Installer 3.1 or the latest version supported by Windows 2000)
- Windows XP SP2 or later
- Windows Vista Family
- Windows 7 Family
- Windows Server 2003 Family
- Windows Server 2008 Family
- Windows Server 2008 Family R2

Prerequisite Software

- MSXML 3.0 or later

Port Requirements

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

	Inbound Ports (Basic NAT Firewall)							
	TCP 80	TCP 135	TCP 139 OR TCP 445		TCP 3121	TCP 4155	TCP 5120	TCP 443
Client System		X (For asset scans)	X	X		X (For listening agents)	X	
Console System					X			
Distribution Server	X		X	X				X

	Outbound Ports (Highly Restricted Network Environment)					
	TCP 80	TCP 139 OR TCP 445		TCP 3121	TCP 5120	UDP 9
Client System	X (For agents)	X	X	X (For agents)		
Console System	X	X	X		X	X (For WoL & error reporting)
Distribution Server						

Major New Features

1. Virtual Machine Enhancements
 - a. Patching VMware templates
 - b. Disable networking while deploying to offline virtual machines
 - c. Optional pre-deployment and post-deployment snapshots
 - d. Deploy to a machine in a different state than was scanned
 - e. Scheduled deployments to offline virtual machines
2. Agent Enhancements
 - a. Deploy service packs to agents
 - b. Checkpoint/restart downloads of agent patches and service packs
3. Patch Deployment Enhancements
 - a. Deploy patches contained within archive files
 - b. Scripted Patch Detection
 - c. Uninstall multiple patches in a single deployment
4. Database Maintenance Feature
 - a. Purge old data.
 - b. Run Backups on a regular basis.
 - c. Reindex the DB.
5. Integrated with VIPRE 4.0 SDK
 - a. Engine Performance enhancements
 - b. Includes VIPRE bug fixes and enhancements
 - c. "Limit AP Scanning to only high risk file types (High Performance)" added to Agent Policy, AP tab, File Access.

Minor Features and Enhancements

1. New threat report filter: "Days to report on"
2. Left-Nav modifications and new grouping
3. New deployment template for Hosted VM deployments
4. Multi Machine Properties edit from machine view and scan view, Patch Drive Patch, Custom 1, 2, and 3.
5. New option to suppress prompts; Ex Download size dialog now has a check box to "Warn Next Time", uncheck and you will no longer be warned. Can be turned back on through tools options.

6. Power Management change; Sleep and Hibernate commands were ignored if a user was logged into the target machine. Power State Change will now enforce for those machines as well since a locked machine or idle machine with a logged in user is a prime use case for this feature.

7. Machines not scanned added to automatic email options.

Resolved Issues

- Resolved issue related to importer failure which returns 0's for scan results
- Resolved timing issue with Unable to Verify reported by Tracker
- Resolved DecryptCredentials failure
- Resolved Importer failure issue when Data is Null
- Resolved Import failure when trying to move file to bad files folder
- Resolved Importer failure when trying to access the file 'arrival file path' and it is being used by another process
- Resolved a Scans never complete. The Scanner Count does not match Import Count
- Resolved Importing Machine Groups issue where you have to click on any other Machine Group before you can import another one
- Resolved issue where you Can't set domain credentials for "My Domain" default machine group
- Resolved Importer issue where Some scan results are 'hung' in the arrivals folder - Reprocessing Bad Files
- Resolved issue where Protect incorrectly exports machine role details that are utilized by SSI
- Resolved issue where Operations monitor show incorrect data
- Resolved issue with Machines By Patch Report
- Resolved issue with Unconventional Bulletin ID in custom patch
- Resolved issue with install agent using example command script
- Resolved Deployment with custom dialog failure
- Resolved issue to cancel jobs using stscheduleview
- Resolved issue when Attempting to "Deploy all missing" for a scan that includes at least one non-downloadable patch (which does NOT exist in the patch repository)
- Resolved issue with Non English Language OS fail to download
- Resolved issue if same user logs on to another console and connected to same DB, then going to tools > option > defaults creds > setting them will not work
- Resolved database upgrades failure when converting SoftwareAssetScans converting the language field
- Resolved issue when Selecting vendor severity in Deployment Detail report advanced criteria generates an error
- Resolved issue with deploying Q931125/MSRC-001 patch displays as Uninstall Succeeded
- Resolved issue where Patch scan template XML file location has no effect

- Resolved issue with machine context menu slow to display when the user has many machine groups
- Resolved issue with & in shavlik comment forum links not displayed
- Resolved issue with Agent upgrade can break agent's ability to update patch and threat data
- Resolved issue with having LangID of 0
- Resolved issue with Scheduled scans do not get proxy credentials
- Resolved issue with refresh files
- Resolved issue where User is able to delete system deployment templates
- Resolved Error 13 - Scanning SQL Server 2005 Unable to access registry key Error [87]
- Resolved issue where user is Unable to set "Minutes between sending console results:" for data rollup > 1000
- Resolved issue with Deployment Status by Machine: Report Gallery's "Deployment to report on" or Advanced Report Settings's Deployment Names time is in GMT not local time
- Resolved issue with Threat Definition Version not updated when Threat Scan rolls up from Agent