

VMware vCenter™ Protect Essentials Plus Release Notes

[Overview](#)

[Documentation](#)

[System Requirements](#)

[Major New Features](#)

[Minor Features and Enhancements](#)

[Resolved Issues](#)

Overview

These release notes support the current GA version of VMware vCenter™ Protect Essentials Plus 8.0. The GA Release can be downloaded from this link:

https://hfnetchk4.shavlik.com/downloads/VMwareProtect_8.0.3787.0.exe

The GA build is 8.0.3787.0.

You can upgrade to VMware vCenter Protect Essentials Plus 8.0 from NetChk Protect 7.5, 7.6, or 7.8. If you are currently using a version of NetChk Protect that is older than version 7.5, you must upgrade to 7.8 before upgrading to 8.0. You can download NetChk Protect 7.8 using this link:

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

IMPORTANT! VMware Inc recommends you create a backup of your current database using SQL Server Management Studio 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 Technical Support Team at shavlik-support@vmware.com or call toll free 1-866-407-5279.

Documentation

<http://www.shavlik.com/support/onlinehelp.aspx>

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 VMware vCenter 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 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 or more for patch repository

Operating System (one of the following):

Note: VMware vCenter 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 Server 2003 Family SP2 or later
- Windows Vista SP2 or later, Business, Enterprise, or Ultimate Edition

Recommended:

- Windows Server 2008 Family SP2 or later, excluding Server Core
- Windows Server 2008 Family R2 SP1 or later, excluding Server Core
- Windows 7 SP1 or later, Professional, Enterprise, or Ultimate Edition

Database:

- Use of SQL Server database (SQL Server 2005, SQL Server 2005 Express Edition, SQL Server 2008, SQL Server 2008 Express Edition, SQL Server 2008 R2, or SQL Server 2008 R2 Express Edition SP1) is required. If you do

not have access to a SQL Server database, the option to install SQL Server 2008 R2 Express Edition SP1 will be provided during the prerequisite software installation process.

- Size: 1.5 GB

Prerequisite Software:

- Windows Installer 4.5 or later (only required if installing SQL Server 2008 R2 Express SP1 during VMware vCenter Protect installation)
- Use of Microsoft SQL Server 2005, SQL Server 2005 Express Edition, SQL Server 2008, SQL Server 2008 Express Edition, SQL Server 2008 R2, or SQL Server 2008 R2 Express Edition SP1
- Microsoft .NET Framework 4.0 or later
- Microsoft .NET Framework 2.0 SP2 (required in order to use the ITScripts feature)
- Windows PowerShell 2.0 or later (required in order to use the ITScripts feature)
- Windows Imaging Component
- Remote Desktop Connection must be allowed in order to use the RDP feature

Windows Account Requirements:

- In order to access the full capabilities of VMware vCenter 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**.
- 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). 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 VMware vCenter 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 VMware vCenter Protect Agent client
- 500 MB or more for patch repository

Operating Systems (any of the following):

- 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

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 and TCP 445 (Windows file sharing/directory services)		TCP 3121	TCP 3122	TCP 4155	TCP 5120	TCP 5985	TCP 443
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 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. 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.
2. 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
3. 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
4. Multiple Administrator 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

1. Patch Scan Performance Enhancements
 - Increased scan speed
 - Reduced memory footprint
2. New Operations Home Page
 - Quicker access to common operations like patch and asset scans, power status scan, ITScript runs, etc.
3. 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
4. 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
5. 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

Resolved Issues

- 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 the **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.

Patch 1 Resolved Issues

The following issues were resolved in Patch 1 and are included in the current GA build.

- 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.