Ivanti Patch for Windows® Servers 9.3 Standard/Advanced Release Notes

Overview

These release notes support the General Availability (GA) version of Ivanti Patch for Windows® Servers 9.3. The GA version can be downloaded from this link: https://content.ivanti.com/products/Protect/v9/93/4440/IvantiPatchForServers_9.3.4440.exe

The GA build is 9.3.4440.0.

You can upgrade to Ivanti Patch for Windows® Servers 9.3 from either Shavlik Protect 9.1 or Shavlik Protect 9.2.

IMPORTANT! Ivanti 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 Ivanti Patch for Windows® Servers 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

The Ivanti Patch for Windows® Servers 9.3 documentation is available here: https://www.ivanti.com/en-US/support/product-documentation

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 Ivanti Patch for Windows® Servers 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: Ivanti Patch for Windows® Servers supports 64-bit versions of the listed operating systems. 32-bit versions are not supported for the console.

- Windows Server 2016 Family, excluding Server Core and Nano Server
- Windows Server 2012 Family R2 Cumulative Update 1 or later, excluding Server Core
- Windows Server 2012 Family, excluding Server Core
- Windows Server 2008 Family R2 SP1 or later, excluding Server Core
- Windows 10 Pro, Enterprise or Education Edition
- Windows 8.1 Cumulative Update 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 2008 (Full or Express Edition) or later]. If you do not have access to a SQL Server database, the option to install either SQL Server 2016 SP1 Express Edition (if supported) or 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 2008 (Full or Express Edition) or later
- Microsoft .NET Framework 4.6.2 or later
- Microsoft Visual C++ Redistributable for Visual Studio 2015
- 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 or later and Windows Server 2012 R2 or later, as PowerShell 4.0 is already included with these operating systems.

Windows Account Requirements:

- In order to access the full capabilities of Ivanti Patch for Windows® Servers, 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
- Windows 10 Education
- Windows Server 2016, Essentials Edition
- Windows Server 2016, Standard Edition (excluding Server Core and Nano Server)
- Windows Server 2016, Datacenter Edition (excluding Server Core and Nano Server)

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
- Windows Update service must not be disabled; rather, it must be set to either **Manual** or **Automatic** in order to successfully deploy patches. In addition, the Windows Update setting on each target machine (**Control Panel > System and Security > Windows Update > Change Settings**) should be set to **Never check for updates**.
- 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 https://www.ivanti.com/en-US/support/supported-products 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 Ivanti Patch for Windows® Servers 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 Ivanti Patch for Windows® Servers Agent client
- 2 GB or more for patch repository

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

- Windows Vista Family
- Windows 7 Family
- Windows 8 Family, excluding Windows RT
- Windows 10 Family
- Windows Server 2008 Family
- Windows Server 2008 Family R2
- Windows Server 2012 Family
- Windows Server 2012 Family R2
- Windows Server 2016 Family

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

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:

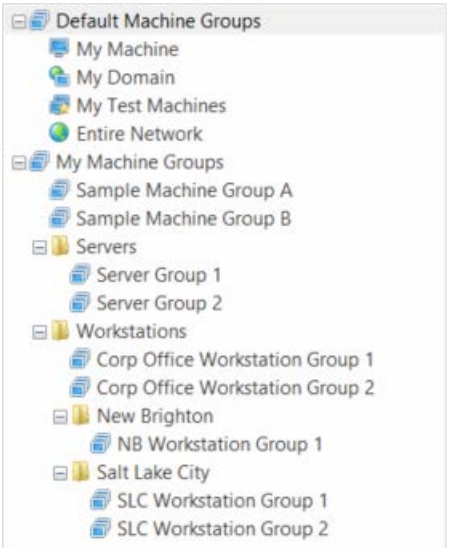
- Interact with different systems in your environment
- Script a sequence of complex events that contain dependencies
- Perform bulk operations or process list inputs from other systems
- Programmatically stage patch deployments or initiate patch downloads

For details on how to use the API feature, see the *API Quick Start Guide*.

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. Y

You can create as many folders and sub-folders as needed in the navigation pane. For example, you might choose to organize your groups based on the types of machines they contain, by location, etc.

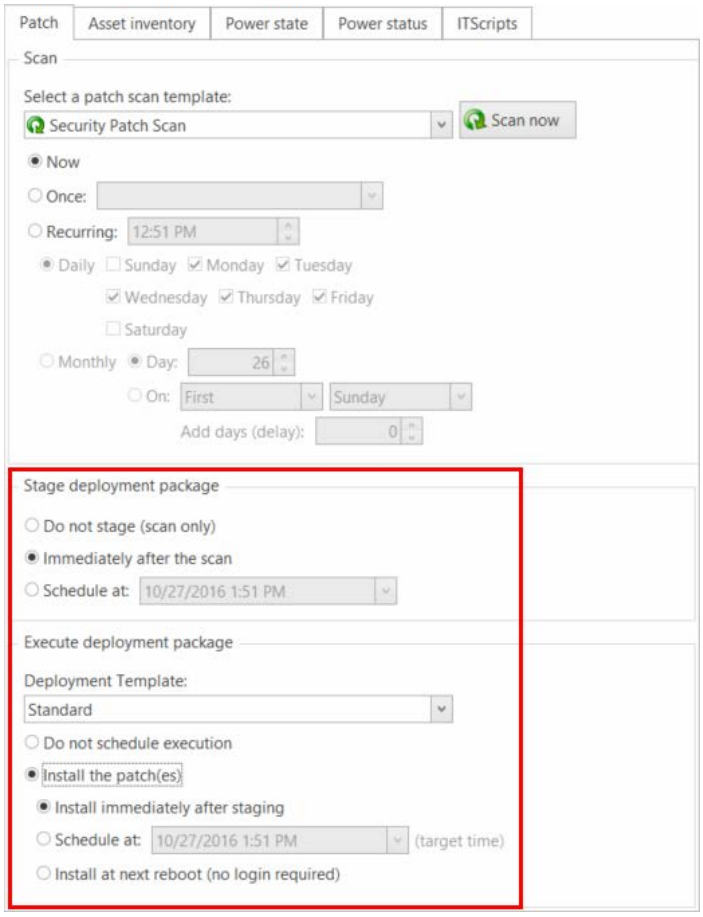


Once created, you can drag and drop items from one folder to another. You can also right-click on any level of the hierarchy and perform an operation on all items at or below that level.

Staged Deployments

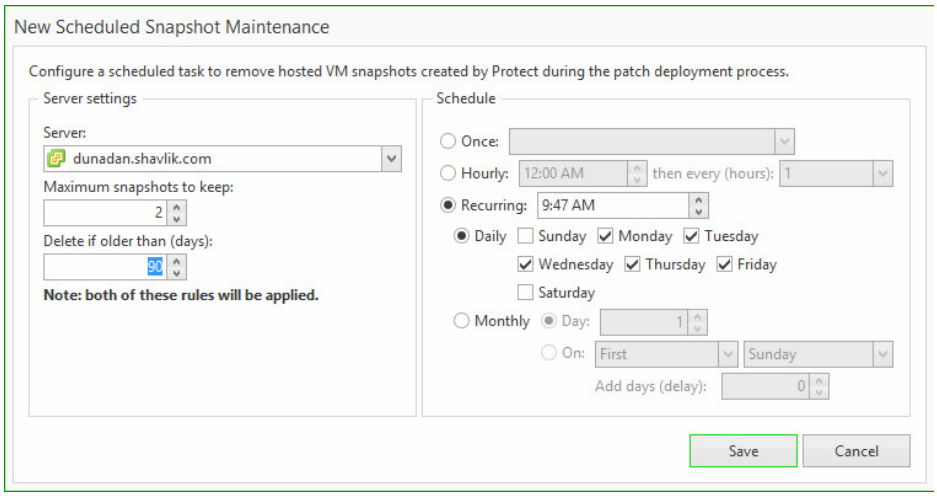
There are now four discrete schedulable points in the patch scanning and deployment process. This gives you much greater control over the entire process. You might:

- 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. To access this feature, select **Tools > Options > Snapshot Maintenance** and add a 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. For more information, in the online help system see **Administration > Utilities > Generating a Certificate from a 3rd Party CA**.

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. For example:

Use the filter menu to select which of the values currently contained in the column should be displayed.

Manual Download Method

A new **Download method** column indicates whether a patch can be downloaded automatically or if it must be downloaded manually. If the value in this column is **Automatic**, it means that Ivanti Patch for Windows® Servers can download the patch automatically. If the value is **Acquire from vendor** or some other value, it means that you must manually download the patch on your own and then move it into the patch download directory. Once the patch is there it can be deployed using the normal deployment process. If auto-deploy is used and a patch requires a manual download, the automatic deployment process will not work.

There may be a number of different reasons why a patch cannot be automatically downloadable. For example, you may have a patch that was created for a proprietary software program, or you may receive patches for a program that is no longer officially supported by the vendor.

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**. The **Tools > Operations** menu has been removed.

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; the deployment preparation process must be complete but the actual deployment cannot have started.

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.

Note: A File Downloader PowerShell script is available to assist with the file download process.

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.

New Agent Default Settings

The new default settings for the **Check-in interval** is for the check-ins to occur every eight hours, distributed over a four-hour period. In addition, the minimum check-in interval is 10 minutes. These were late changes and are not reflected in the help system.

Deprecated Features

Features That 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

  This is due to a movement in the industry to migrate from the use of SHA-1 certificates to SHA-2 certificates. Ivanti is participating in this movement and at the end of 2016 began requiring the use of SHA-2 certificates for communication between Ivanti Patch for Windows® Servers agents and the Ivanti Patch for Windows® Servers 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 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.

- Resolved an issue where a crash would occur when attempting to deploy a patch from a German-language console.
- Resolved an issue where the Migration Tool would fail when using a local SQL Server Express database.
- Resolved an issue where a patch scan would fail when opening a breadcrumb. (94387)
- Resolved an issue where scanning virtual machines and OU online machines did not properly remove duplicates, which caused a licensing error.
- Resolved an issue where opening a machine group that contained hosted machines caused a timeout error.
- Resolved an issue where the console would crash when attempting to view or cancel remote scheduled tasks.
- Resolved an issue where the Predictive patch downloads feature would fail if a patch has an empty BaseFileName.
- Resolved an issue loading the report list when attempting to create a report.
- Resolved an issue where scheduling a scan with automatic deployment would not occur if the job is opened or edited.
- Resolved an issue where a patch scan would fail and not complete rather than returning an error code.
- Resolved an issue where a space in a custom patch file name caused a problem during agent check-ins.
- Resolved an issue where scheduled console tasks were being lost if an upgrade to v9.3 failed or was cancelled.
- Resolved an issue handling cryptographic errors when applying patch data deltas.
- Resolved an issue where a scan with a cryptographic error would fail without returning an error message.
- Resolved an issue where the console was reporting an agent as active after it was uninstalled.
- Resolved an issue where superseded patches were incorrectly being reported as missing.
- Resolved an issue where, during a scan, the console would not attempt to connect to a machine using IPv4 addressing after IPv6 addressing failed.
- Resolved an issue where the CVE list in Patch View was not being refreshed.
- Resolved an issue where Event History was not providing proper details if the program attempted to download a publicly unavailable patch.