Ivanti Security Controls 2018.3 Release Notes

Overview

These release notes support the General Availability (GA) version of Ivanti Security Controls 2018.3. The GA version can be downloaded from this link: https://content.ivanti.com/products/isec/v9.4/34105/IvantiSecurityControls_9.4.34105.exe

The GA build is 9.4.34015.0.

You can upgrade to Ivanti Security Controls 2018.3 from Ivanti Patch for Windows 9.3 Update 1.

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 https://www.ivanti.com/support/contact.

Documentation

The Ivanti Security Controls 2018.3 documentation is available here: https://www.ivanti.com/en-US/support/product-documentation

System Requirements

Customers upgrading from Ivanti Patch for Windows 9.3 Update 1 should note the following new console requirements:

- Memory: 16GB of RAM is now recommended for high performance systems
- Disk space: 100GB is now recommended for the patch repository
- Microsoft .NET Framework 4.7.2 or later (was 4.6.2 or later)
- Microsoft Visual C++ Redistributable for Visual Studio 2017 (was 2015)

For a complete list of requirements for the console, your agentless clients and your agent-based clients, see: https://help.ivanti.com/iv/help/en_US/isec/94/Topics/System_requirements.htm

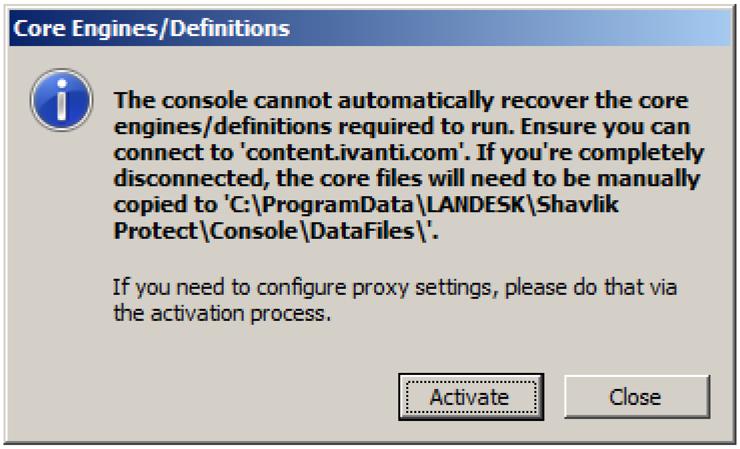
Installation Notes

- New Installation vs Upgrade:
  - If you are an existing Patch for Windows 9.3 Update 1 customer, you should perform an upgrade to Security Controls 2018.3. This will enable you to maintain your current product database and configuration data.
  - If you are (A) a new Ivanti customer, or (B) using the CTP 1 release or (C) an Ivanti Application Control customer who is migrating to the Application Control feature in Security Controls, you will be performing a new installation.

  Although the upgrade and new install processes are similar, there are differences. For example, if you perform an upgrade you will not be presented with the opportunity to create a new database or choose how users and services will connect to the database.

- Disconnected Networks: If you are installing on a disconnected console machine, in addition to manually installing any prerequisite software, you must also manually download and install the product core files BEFORE you begin the installation process.

  If you see the following dialog during installation, it means you have missed this step. Click **Close**, manually install the core files and then start the installation process again.



Core Engines/Definitions

The console cannot automatically recover the core engines/definitions required to run. Ensure you can connect to 'content.ivanti.com'. If you're completely disconnected, the core files will need to be manually copied to 'C:\ProgramData\LANDESK\Shavlik Protect\Console\DataFiles\'.

If you need to configure proxy settings, please do that via the activation process.

For information on how to manually manage your data files in a disconnected environment, refer to the following Ivanti Community post: https://community.shavlik.com/docs/DOC-24237

Major New Features

REST API

The API feature provides a simple RESTful interface with lightweight JSON-formatted responses that enables you to read and write data to/from the program. The feature allows you to automate many of your day-to-day operations, saving you considerable time and effort. The REST API allows you to fully integrate Ivanti Security Controls into your orchestration and automation systems.

The list of available functions includes:

Asset Scan Templates	Patch Downloads	Patch Deployment Templates
Credentials	Patch Groups	Patch Metadata
Distribution Servers	Patch Scans	Vendor Family Product Metadata
Machine Groups	Patch Scan Templates	Virtual Infrastructure
Operation Controller	Patch Deployments	
Patches	Patch Deployment Status	

For complete details, see: https://help.ivanti.com/iv/help/en_US/isec/API/Topics/Welcome.htm

Patch Management Support for Linux

Patch management functionality is now available for Red Hat Enterprise Linux (RHEL) systems. The scan and deployment processes are nearly identical to that used by your Windows patch agents, so you can quickly begin managing your Linux systems.

You can manage all vendor-supported Server, Workstation, Client and Computer Node variants of the following systems.

- Red Hat Enterprise Linux 6, x64 (the libicu package is required)
- Red Hat Enterprise Linux 7, x64 (the libicu package is required)

To get started using this feature, refer to the Overview of Linux Patch Management topic in the help system.

Import CVEs Into a Patch Group

The Common Vulnerabilities and Exposures (CVE) List is a public reference of known cybersecurity vulnerabilities. This list, maintained by the MITRE Corporation (mitre.org), continually changes as new vulnerabilities are detected. If your organization uses the CVE list, it can be difficult to determine exactly which patches you need to deploy to protect your machines from the threats identified in the list.

Fortunately, Security Controls simplifies this process. You simply import a list of CVEs to Security Controls and then add them to a patch group. Security Controls will automatically determine which patches are related to each CVE and it will add those patches to the patch group. You then use the patch group in your scans and deployments.

To get started using this feature, refer to the Importing CVEs topic in the help system.

Application Control (preview only)

The ability to prevent unauthorized code execution on your corporate machines, and thus protect these machines from ransomware and other malware attacks, is now available via the Application Control feature. Using techniques such as Executable Control, Privilege Management and Browser Control, Application Control reduces risk, helps achieve compliance and delivers security, all with minimal performance impact to your end users.

The Application Control feature is currently being offered as a Community Technology Preview 2 (CTP 2) release. The full General Availability (GA) release is planned for early 2019.

NOTE: If you used the CTP 1 release of Application Control and you want to use the CTP 2 release, you must uninstall CTP 1 and then perform a fresh installation of Security Controls. The CTP 1 database is not compatible with the CTP 2 database, so be sure to create a new database during the installation process.

Minor Features and Enhancements

The Product Has Been Renamed to Ivanti Security Controls

The product name has been changed from Ivanti Patch for Windows to Ivanti Security Controls. The new name reflects the addition of functionality that was previously only available in two or more separate products.

New Home Page

The home page has been totally redesigned to provide status information and statistics, quick links to many of the most popular activities and notification of any possible issues that may require your attention.

The old home page functionality, from which patch, asset, power and ITScripts tasks can be quickly and easily performed, is still available and has simply been moved to the new Agentless Operation dialog. To access this dialog, select **New > Agentless operation** or press Ctrl + N.

Reorganized Menu Bar

The New menu has been reordered and Windows and Linux tasks have been consolidated into two **New > Windows patch** and **New > Linux patch** sub-menus. Import tasks have been removed from the **New** menu and are now located in the new **Import** menu. **Manage > Items** has been renamed to **Manage > Database Maintenance** and, in addition to enabling you to view a list of all prior scans and patch deployments, it now enables you to schedule database maintenance activities that were previously configured from the **Tools > Options > Database Maintenance** tab (which has been removed).

New Sections in the Navigation Pane

The sections in the navigation pane have been renamed and reordered to provide a smarter and easier to use organization. There are also two new sections:

- Linux Patch Configurations and Groups
- Application Control Configurations

Machine View Changes

- Three news tabs have been added to the top pane to help manage the presentation of machine information.
    - Windows patch & Application Control
    - Windows asset
    - Linux patch
- Several new columns are now available, including OS type, CVSS score and CVEs.
- Information in the bottom pane has been reorganized to increase usability.

Windows Patch View

The top pane in Patch View now contains new columns that show the CVSS score and the patch file name so that you can more clearly see affected products. The bottom pane has been reorganized so that the most commonly-used content is near the top.

Tools > Options Changes

- **Display** tab: Contains a new section that is used to define program startup defaults. The **Recent errors** check box controls the date range for the new Possible Issues area on the home page. A new **Select palette** button enables you to select the color swatch you prefer to use within the program.
- **Patch** tab: This has been renamed to **Scan**. A new **Patch scan results import timeout** option enables you to specify the maximum time to wait for the console to import scan results from all target machines.
- **Downloads** tab: A new **Open directory** button provides convenient access to Windows File Explorer.
- **Database Maintenance** tab: This tab has been removed from the **Options** dialog. The database maintenance functionality is now found by selecting **Manage > Database Maintenance**.
- **API** tab: This new tab provides access to a PowerShell script that helps establish a secure connection between remote REST API clients and the console

Agent Policy Editor Changes

To accommodate the new Linux and Application Control functionality, the **Agent Policy Editor** now supports defining one or more Linux patch tasks on the **Patch** tab and it contains a new **Application Control** tab. In addition, the interface used to add, edit and delete tasks has been updated on all tabs.

The CHM Help File is Now Only Available as a Separate Download

The CHM version of the help system is no longer included with the installation package. If you access the help system using the CHM file that is used when you choose the Local help viewer option, you will need to follow the instructions for downloading the file and configuring the system. This is a one-time process.

If you access the help system on the web, you are not affected.

Service Pack Groups are Now Called Product Levels

The term Product Level better reflects the terminology used by Microsoft Corporation to identify different versions or updates of their products, such as Windows 10. Some products may still use the older service pack terminology, and for these products you will still see the term SP1, SP2, etc. in the Product level column within Machine View and other areas of the product.

Manage > Items

This has been renamed to **Manage > Database Maintenance**. In addition to viewing and managing the list of prior scans, script executions and patch deployments, this dialog now contains the database maintenance functionality that was previously available on the old **Tools > Options > Database Maintenance** tab.

Help > About Dialog

The Version Info / App Info button has removed. This information is now presented on the new **Application** and **File versions** tabs. The columns on the **File versions** tab are now sortable. And the dialog now contains a link to a web page that shows the list of Ivanti patents that protect Ivanti software and cloud services.

Performance Improvements

Many performance improvements have been implemented throughout the product.

Deprecated Features

Features Will be Removed in Future Releases

- A new set of database views has been created and is organized using the Reporting2 namespace. The Reporting2 namespace now includes a view for CVSS scores. The Reporting namespace will be removed in a future release. For more information about report views, see the *Report Views Guide* available from the Patch for Windows section on the Ivanti Product Documentation page.
- Support for SQL Server 2008 and SQL Server 2008 R2 will end in a future release.

Resolved Issues

- Resolved an issue where performing a scan with an empty patch group would result in a scan for all security patches.
- Resolved an issue where the program would crash if an invalid version of VMware Tools is installed.
- Resolved an issue where agent deployments were not included in Scheduled Deployment Status by Machine reports.
- Resolved an issue where generating reports could cause the program to crash due to an issue with Windows 10 1803 default fonts.
- Resolved an issue where trace logging was insufficient to diagnose agent communication issues
- Resolved an issue where an Asset Scan report was not selectable from the Reports dialog.
- Resolved an issue where the deploy service packs right-click option was not available.
- Resolved an issue where Machine View did not contain a target machine’s last known IP address when using cloud agents.
- Resolved an issue where attempting to download a patch from Patch View incorrectly caused the “None of the selected patches need to be downloaded” message to appear.
- Resolved an issue where Patch View did not display the correct patches when selecting Server OS filters.
- Resolved an issue where previously deleted deployment templates were being shown in the Deployment Template list in an agent policy.
- Resolved an issue where email notifications of scheduled staged deployments were being sent early.
- Resolved an issue where cancelling a deployment did not delete the scheduled deployment from online hosted VMs.
- Resolved an issue where executing multiple scans and deployments caused Deployment Tracker to incorrectly show deployment results.
- Resolved an issue where deployments would hang during the deployment initialization and file download phases.
- Resolved an issue where a race condition caused the console to crash.
- Resolved an issue where Office patches were not deploying because they were incorrectly shown as already installed.
- Resolved an issue where the Affected Machines tab in Patch View was not properly updating.
- Resolved an issue where scanning a Windows 10 target machine failed due to a problem with SPN target name validation.
- Resolved an issue where an exception occurred mapping a virtual machine.
- Resolved an issue where the Installed On date was not inserted into the database in the correct format when the date/time format was not English.
- Resolved an issue where an agentless asset scan failed when the admin share on the target machine was disabled.
- Resolved an issue where a scan result could not be deleted from the navigation pane.
- Resolved an issue where a message was not displayed if a scan result could not be deleted from the navigation pane.

- Resolved an issue where a patch deployment failed when specifying a deployment template that used a distribution server.
- Resolved an issue where error messages where not displayed or written to the ErrorVariable file when performing a patch deployment from the PowerShell API.
- Resolved an issue where the Effectively Installed icon was not being displayed in a Condensed Patch Listing report.