Security Controls 2019.1

Release Notes

About this Release

Build Information

These release notes support the General Availability (GA) version of Ivanti Security Controls 2019.1.
The GA version can be downloaded from this link:

https://content.ivanti.com/products/isec/v9.4/34268/IvantiSecurityControls_9.4.34268.exe

The GA build is 9.4.34268.0.

You can upgrade to Ivanti Security Controls 2019.1 from Ivanti Patch for Windows 9.3 Update 1 or Ivanti Security Controls 2018.3 (non-AC users only). If you are currently using the Preview version of Application Control that was available in Security Controls 2018.3, you must perform a fresh installation. See the Upgrade Guide for complete details.

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 Security Controls Database Maintenance tool.

Documentation

The complete library of Ivanti Security Controls 2019.1 documentation is available here:

www.ivanti.com/en-US/support/product-documentation

Installation Notes

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 2013 (required for scanning offline VMs)
- 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 System Requirements in the Help.

New Installation vs Upgrade

If you are an existing Patch for Windows 9.3 Update 1 or Security Controls 2018.3 (non-AC) customer, you should perform an upgrade to Security Controls 2019.1. This will enable you to maintain your current product database and configuration data.

If you are a new Ivanti customer or an Ivanti Application Control customer who is migrating to the Application Control feature in Security Controls, you will be performing a new installation. If you are currently using the Application Control feature in Security Controls 2018.3, you must uninstall the program and all agents and then perform a fresh installation. See the Installation section in the Help.

Although the upgrade and new installation 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. For complete information on this process, see the Performing a New Installation topic in the Help.

For information on how to manually manage your data files in a disconnected environment, refer to the following Ivanti Community post:

https://forums.ivanti.com/s/article/How-To-Download-Content-Data-Files-and-Patches-using-the-Download-PowerShell-Script

Major New Features

Application Control (now Generally Available)

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.

In addition, the Application Control Event Viewer is being introduced in Security Controls 2019.1. This view enables you to run a large number of customizable queries that show events that have occurred during a specified time period.

Minor Features and Enhancements

Modified Home Page

The new home page design that was introduced in 2018.3 has been updated. It now has a cleaner and more graphical appearance.

Linux Deployment Results Reported to the Console

The results of Linux agent patch deployments are now reported to the console and can be found in the middle pane of Machine View. A history of prior deployments is also reported on the **Patch Deployment** tab of the **Database Maintenance** dialog.

Ability to Acknowledge Events in Event History

The Events History page now contains a new Acknowledge column that indicates whether each event has been seen and reviewed by an administrator. You can right-click an event to acknowledge it.

Review Certificate Before Connecting to a Virtual Server

The first time you connect to a vCenter Server, you may be prompted to review and verify the server's certificate. This security step ensures that you are not connecting to an untrusted server. Once the certificate is accepted, the certificate's thumbprint is stored and you will not be asked to repeat the verification process.

Agent Reboot Options Tab

A new Agent Reboot Options tab has been added to the Agent Policy Editor. This tab enables you to specify when and how an agent machine will be restarted after either an agent is upgraded or an engine component is installed or upgraded. These values have always been a part of the agent policy, but the addition of this tab enables you to finely-tune a number of reboot options.

New Import CVEs Button

A new Import CVEs button has been added to the Patch Group area of Windows Patch View. This provides a more intuitive location from which to initiate the import process.

New Database Views

A collection of new database views is now available for use in custom report queries. The new views begin with the term Reporting2.* and should be used in all new custom queries. The older collection of views, which begin with the term Reporting.*, is still available but should only be used by legacy queries.

Performance Improvements

Several performance improvements have been implemented throughout the program.

Deprecated Features

Features That Have Been Removed from 2019.1

The ITScripts WinRM Remoting target type has been removed.

Features That 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 Generating Custom Reports section in the ISeC Help.
- Support for SQL Server 2008 and SQL Server 2008 R2 will end in a future release.

Resolved Issues

The following customer support issues have been resolved in this release:

Problem ID	Title
455741	Resolved an issue where deployment progress messages for patches were prematurely marked as complete.
480165	Resolved an issue where invalid XML characters in the “InstalledBy” registry key prevented patch assessment.
482917	Resolved an issue where empty machine names returned by an Active Directory query caused a crash.
491164	Resolved an issue where agent patch scan and asset scan result identifiers were flipped when processed concurrently.
494964	Resolved an issue where Red Hat patch content metadata was missing for Red Hat 6.9 patches assessed before Dec. 28th, 2018.
496821	Resolved an issue where using the PowerShell or REST API to modify patch groups or a patch scan template did not update associated agent policies and agents.
499058	Resolved an issue where patch deployments with the “Restart and Shutdown” option would continue to reboot the system when using the Microsoft Task Scheduler.
504219	Resolved an issue where CVE Import always applied to the first patch group in the dropdown list.
506133	Resolved an issue where CVE Import incorrectly applied to software distribution.
443721	Upgraded VMware’s VDDK to address security vulnerabilities in VMware bundled open source packages.