Security Controls 2022.4

Release Notes

About this Release

Build Information

These release notes support the General Availability (GA) version of Ivanti Security Controls 2022.4.
The GA version can be downloaded from this link:

https://forums.ivanti.com/s/article/Ivanti-Security-Controls-Download

The GA build is 9.5.9353.0.

You can upgrade to Security Controls 2022.4 from Security Controls 2022.3, 2022.2, 2022.1, 2021.4, 2021.2.1 or 2019.3. 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 2022.4 documentation is available here:

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

Installation Notes

System Requirements

The following operating systems are no longer supported for use by the Security Controls console:

- Windows 7 SP1
- Windows Server 2008 family R2 SP1

IMPORTANT! Support for the Security Controls console on the Windows 8.1 operating system is scheduled to end in January 2023.

Microsoft SQL Server 2008 and 2008 R2 are no longer supported. You must be using Microsoft SQL Server 2012 or later.

A new version of the Microsoft Visual C++ Redistributable for Visual Studio 2015 – 2019 is available, so this will likely be identified as missing during the prerequisite check of the installation process.

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 Security Controls 2022.3, 2022.2, 2022.1, 2021.4, 2021.2.1 or 2019.3 customer, you should perform an upgrade to Security Controls 2022.4. 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.

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 Security Controls 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

Changes in Security Controls 2022.4

This release contains the following changes:

- A new "Automate to Compliance" REST API script is now available. The script automates the steps in the patch process (scan, deploy, reboot), repeating the steps until all patches have been deployed to the designated machines.
- The Patch Metadata function in the REST API has been enhanced to provide better sorting and pagination capabilities when viewing the query results.
- The agent client program has been updated. Much more information is now provided in the patch task logs about the patch status (downloads, installs, success, failure, error messages).
- A security enhancement has been made to the SSH server connection process. You now have the option to specify if an SSH connection can be used when the console communicates with an endpoint that supports SSH and for which SMB fails.
- More information has been added to the error codes that are displayed in the Windows deployment history tab in Machine View.
- Deprecation of Windows 8.1: Support for the Security Controls console on the Windows 8.1 operating system is scheduled to end in January 2023.

Known Issues

Deploying patches that use Red Hat Enterprise Linux 8 application streams is not supported. Detection of these patches is fully supported.

Deprecated Features

Feature That Was Removed from 2022.2

Support for Red Hat Enterprise Linux 6 has ended. This is because Red Hat has stopped providing maintenance support for Red Hat Enterprise Linux 6.

Features That Were Removed from 2021.2 Update 1

The following operating systems are no longer supported:

- The Security Controls agent is no longer supported on Windows 8 and CentOS 6 operating systems
- Agentless operations are no longer supported on Windows XP, Windows Server 2003, Windows Vista and Windows 8 operating systems.

Features That Were Removed from 2020.1

- The Security Controls console can no longer be installed on the following operating systems:
  - Windows 7 SP1
  - Windows Server 2008 family R2 SP1

  Security Controls will continue to patch these endpoints through the Custom Patch Support program.
- The ITScripts TrustedHosts list credential has been eliminated because it is not required. Machines can still be added to the list when a remote PowerShell prompt is launched from Machine View.

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 original Reporting namespace will be removed in a future release and should only be used by legacy queries. All new queries should be created using the Report2.* views. For more information about report views, see the Generating Custom Reports section in the ISeC Help.
- In the REST API, support for **servicecredentials** requests and the **sharewithservice** parameter will end in a future release. Those capabilities are contained in the new shared credentials functionality.
- In the REST API, support for the **/metadata/vendor Family.products** parameter will end in a future release. That capability is being replaced by the **Family.productVersions** parameter.

Resolved Issues

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

Problem ID	Title
905099	Resolved an issue where the console could not be activated using credentials.
961399	Resolved an issue where adding hosted VMs to a machine group via the REST API would cause an error.
966407	Resolved an issue where the Total Seats Remaining value would be negative in the Detailed License Status report.
970119	Resolved an issue where Application Control did not work when the agent download location was set to be from a distribution server using the By Agent IP Range option.
975465	Resolved an issue where, when configuring an agentless scan, the **Schedule at** option would not always change properly when toggling between a one-time scan and a recurring scan.
978618	Resolved an issue where supersedence was ignored when scanning using a patch group as a baseline.
981686	Resolved an issue where a data content issue caused the console to crash.