Security Controls 2022.2

Release Notes

About this Release

Build Information

These release notes support the General Availability (GA) version of Ivanti Security Controls 2022.2.
The GA version can be downloaded from this link:

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

The GA build is 9.5.9293.0.

You can upgrade to Security Controls 2022.2 from Security Controls 2022.1, 2021.4, 2021.2, 2021.1, 2020.1 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 2022.2 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

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 2022.1, 2021.4, 2021.2, 2021.1, 2020.1 or 2019.3 customer, you should perform an upgrade to Security Controls 2022.2. 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 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 2022.2

This release contains the following changes:

- An example PowerShell script has been added to the Security Controls REST API Help. This script shows how to add specific KBs to a new patch group or to existing patch groups. If you need to add an out-of-band security patch to many patch groups at once, this script simplifies the process.
- Additional options allow you to more precisely specify which language should be used within the Security Controls interface. In the **Tools > Options > Display Options** dialog, you can either select a specific language or let the console machine's operating system language setting specify which language should be used. The new language options are applied on a per user basis.
- Corrected a daylight savings time issue that sometimes caused scheduled scans to run one hour late or become disabled. The fix adds a periodic check that re-enables the scheduled scans.
- A number of known issues have been resolved.

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
889155	Resolved an issue where the ISeC agent was not able to find to the listener due to an extended patch task name.
895982	Resolved an issue where agent patch tasks were not being scheduled due to the task name length.
904592	Resolved an issue where the PowerShell module failed to load ST.Engines.Policy.dll.
907356	Resolved an issue where Linux patches would incorrectly be detected as missing because the wrong productid was being used in the patch content.
909438	Resolved an issue where custom patches did not work with the latest version of agents.
912439	Resolved an issue where the All Platforms Executive Summary report was incorrectly listed for selection when configuring the automated email settings for a machine group. This report was never intended for automatic generation. A good alternative is to use the Windows Executive Summary report.
912464	Resolved an issue where the STPatch.log would not honor the log size setting in the agent policy.
915383	Resolved an issue where the Condensed Patch Listing report no longer displayed all machines correctly in the PDF or XLS exports.
922279	Resolved an issue where Application Control did not work properly with Windows 11.
924493	Resolved an issue where patch scan results would not be sent back to the console due to an extended patch task name.
926908	Resolved an issue where, following an upgrade, the agent UI would report an unknown policy and connect to an unknown server due to an initialization error.
931204	Resolved an issue where a long agent task name would prevent the task from being scheduled.